Sound management of risks related to money laundering and financing of terrorism

I. Introduction

1. Being aware of the risks incurred by banks of being used, intentionally or unintentionally, for criminal activities, the Basel Committee on Banking Supervision is issuing these guidelines to describe how banks should include money laundering (ML) and financing of terrorism (FT) risks within their overall risk management.

2. The Committee has a long-standing commitment to promote the implementation of sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures that are critical in protecting the safety and soundness of banks and the integrity of the international financial system. Following an initial statement in 1988,[1] it has published several documents in support of this commitment. In September 2012, the Committee reaffirmed its stance by publishing the revised version of the *Core principles for effective banking supervision*, in which a dedicated principle (BCP 29) deals with the abuse of financial services.

3. The Committee supports the adoption of the standards issued by the Financial Action Task Force (FATF).[2] In February 2012, the FATF released a revised version of the *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (the FATF standards), to which the Committee provided input.[3] In March 2013, the FATF also issued *Financial Inclusion Guidance*, which has also been considered by the Committee in drafting these guidelines. The Committee's intention in issuing this paper is to support national implementation of the FATF standards by exploring complementary areas and leveraging the expertise of both organisations. These guidelines embody both the FATF standards and the Basel Core Principles for banks operating across borders and fits into the overall framework of banking supervision. Therefore, these guidelines are intended to be consistent with and to supplement the goals and objectives of the FATF standards, and in no way should they be interpreted as modifying the FATF standards, either by strengthening or weakening them.

5. The Committee's commitment to combating money laundering and the financing of terrorism is fully aligned with its mandate "to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability".[4] Sound ML/FT risk management has particular relevance to the overall safety and soundness of banks and of the banking system, the primary objective for banking supervision, in that:

- it helps protect the reputation of both banks and national banking systems by preventing and deterring the use of banks to launder illicit proceeds or to raise or move funds in support of terrorism; and
- it preserves the integrity of the international financial system as well as the work of governments in addressing corruption and in combating the financing of terrorism.

6 The inadequacy or absence of sound ML/FT risk management exposes banks to serious risks, especially reputational, operational, compliance and concentration risks. Recent developments, including robust enforcement actions taken by regulators and the corresponding direct and indirect costs incurred by banks due to their lack of diligence in applying appropriate risk management policies, procedures and controls, have highlighted those risks. These costs and damage could probably have been avoided had the banks maintained effective risk-based AML/CFT policies and procedures.

7. It is worth noting that all these risks are interrelated. However, in addition to incurring fines and sanctions by regulators, any one of them could result in significant financial costs to banks (eg through the termination of wholesale funding and facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the diversion of limited and valuable management time and operational resources to resolve problems.

1. Assessment, understanding, management and mitigation of risks

(a) Assessment and understanding of risks

15. Sound risk management[16] requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country,[17] sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied. The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations (product and service offered) will then have to take into account the risk assessment and the bank's resulting risk profile. A bank should have appropriate mechanisms to document and provide risk assessment information to competent authorities such as supervisors.

16. A bank should develop a thorough understanding of the inherent ML/FT risks present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business. This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information such as national risk assessments and country reports from international organisations. Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control those identified inherent risks. Any resulting residual risk should be managed in line with the bank's risk profile established through its risk assessment. This assessment and understanding should be able to be demonstrated as required by, and should be acceptable to, the bank's supervisor.

(b) Proper governance arrangements

17. Effective ML/FT risk management requires proper governance arrangements as described in relevant previous publications of the Committee.[18] In particular, the requirement for the board of directors to approve and oversee the policies for risk, risk management and compliance is fully relevant in the context of ML/FT risk. The board of directors should have a clear understanding of ML/FT risks. Information about ML/FT risk assessment should be communicated to the board in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions.

18. Explicit responsibility should be allocated by the board of directors effectively taking into consideration the governance structure of the bank for ensuring that the bank's policies and procedures are managed effectively. The board of directors and senior management should appoint an appropriately qualified chief AML/CFT officer to have overall responsibility for the AML/CFT function with the stature and the necessary authority within the bank such that issues raised by this senior officer receive the necessary attention from the board, senior management and business lines.

(c) The three lines of defence

19. As a general rule and in the context of AML/CFT, the business units (eg front office, customer-facing activity) are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. The second line of defence includes the chief officer in charge of AML/CFT, the compliance function but also human resources or technology. The third line of defence is ensured by the internal audit function.

20. As part of **the first line of defence**, policies and procedures should be clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the bank in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions.

21. A bank should have adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards. All banks should implement ongoing employee training programmes so that bank staff are adequately trained to implement the bank's AML/CFT policies and procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank according to their needs and the bank's risk profile. Training needs will vary depending on staff functions and job responsibilities and length of service with the bank. Training course organisation and materials should be tailored to an employee's specific responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement the bank's AML/CFT policies and procedures. New employees should be required to attend training as soon as possible after being hired, for the same reasons. Refresher training should be provided to ensure that staff are reminded of their obligations and their knowledge and expertise are kept up to date. The scope and frequency of such training should be tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the bank.

22. As part of **the second line of defence**, the chief officer in charge of AML/CFT should have the responsibility for ongoing monitoring of the fulfilment of all AML/CFT duties by the bank. This implies sample testing of compliance and review of exception reports to alert senior management or the board of directors if it is believed management is failing to address AML/CFT procedures in a responsible manner. The chief AML/CFT officer should be the contact point regarding all AML/CFT issues for internal and external authorities, including supervisory authorities or financial intelligence units (FIUs).

23. The business interests of a bank should in no way be opposed to the effective discharge of the above-mentioned responsibilities of the chief AML/CFT officer. Regardless of the bank's size or its management structure, potential conflicts of interest should be avoided. Therefore, to enable unbiased judgments and facilitate impartial advice to management, the chief AML/CFT officer should, for example, not have business line responsibilities and should not be entrusted with responsibilities in the context of data protection or the function of internal audit. Where any conflicts between business lines and the responsibilities of the chief AML/CFT officer arise, procedures should be in place to ensure AML/CFT concerns are objectively considered at the highest level.

24. The chief AML/CFT officer may also perform the function of the chief risk officer or the chief compliance officer or equivalent. He/she should have a direct reporting line to senior management or the board. In case of a separation of duties the relationship between the aforementioned chief officers and their respective roles must be clearly defined and understood.

25. The chief AML/CFT officer should also have the responsibility for reporting suspicious transactions. The chief AML/CFT officer should be provided with sufficient resources to execute all responsibilities effectively and play a central and proactive role in the bank's AML/CFT regime. In order to do so, he/she must be fully conversant with the bank's AML/CFT regime, its statutory and regulatory requirements and the ML/FT risks arising from the business.

26. **Internal audit, the third line of defence,** plays an important role in independently evaluating the risk management and controls, and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures. A bank should establish policies for conducting audits of (i) the adequacy of the bank's AML/CFT policies and procedures in addressing identified risks, (ii) the effectiveness of bank staff in implementing the bank's policies and procedures; (iii) the effectiveness of compliance oversight and quality control including parameters of criteria for automatic alerts; and (iv) the effectiveness of the bank's training of relevant personnel. Senior management should ensure that audit functions are allocated staff that are knowledgeable and have the appropriate expertise to conduct such audits. Management should also ensure that the audit scope and methodology are appropriate for the bank's risk profile and that the frequency of such audits is also based on risk. Periodically, internal auditors should conduct AML/CFT audits on a bank-wide basis. In addition, internal auditors should be proactive in following up their findings and recommendations.[19] As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT measures.

(d) Adequate transaction monitoring system

28 A bank should have a monitoring system in place that is adequate with respect to its size, its activities and complexity as well as the risks present in the bank. For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process. When a bank has the opinion that an IT monitoring system is not necessary in its specific situation, it should document its decision and be able to demonstrate to its supervisor or external auditors that it has in place an effective alternative. When an IT system is used, it should cover all accounts of the bank's customers and transactions for the benefit of, or by order of, those customers. It must enable the bank to undergo trend analysis of transaction activity and to identify unusual business relationships and transactions in order to prevent ML or FT.

29. In particular, this system should be able to provide accurate information for senior management relating to several key aspects, including changes in the transactional profile of customers. In compiling the customer's profile, the bank should incorporate the updated, comprehensive and accurate CDD information provided to it by the customer. The IT system should allow the bank, and where appropriate the group, to gain a centralised knowledge of information (ie organised by customer, product, across group entities, transactions carried out during a certain timeframe etc). Without being requested to have a unique customer file, banks should be able to risk-rate customers and manage alerts with all the relevant information at their disposal. An IT monitoring system must use adequate parameters based on the national and international experience on the methods and the prevention of ML or FT. A bank may make use of the standard parameters provided by the developer of the IT monitoring system; however, the parameters used must reflect and take into account the bank's own risk situation.

30. The IT monitoring system should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report (STR) or taking other steps in order to minimise the risk. The chief AML/CFT officer should have access to and benefit from the IT system as far as it is relevant for his/her function (even if operated or used by other business lines). Parameters of the IT system should allow for generation of alerts of unusual transactions and should then be subject to further assessment by the chief AML/CFT officer. Any risk criteria used in this context should be adequate with regard to the risk assessment of the bank.

31. Internal audit should also evaluate the IT system to ensure that it is appropriate and used effectively by the first and second lines of defence.

2. Customer acceptance policy

32. A bank should develop and implement clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment.[20] When assessing risk, a bank should consider the factors relevant to the situation, such as a customer's background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence (when different), products used, nature and purpose of accounts, linked accounts, business activities and other customer-oriented risk indicators in determining what is the level of overall risk and the appropriate measures to be applied to manage those risks.

33. Such policies and procedures should require basic due diligence for all customers and commensurate due diligence as the level of risk associated with the customer varies. For proven lower risk situations, simplified measures may be permitted, if this is allowed by law. For example, the application of basic account-opening procedures may be appropriate for an individual who expects to maintain a small account balance and use it to conduct routine retail banking transactions. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. The FATF *Financial Inclusion Guidance*[21] provides useful guidelines on designing AML/CFT procedures that are not overly restrictive to the financially or socially disadvantaged.

34. Where the risks are higher, banks should take enhanced measures to mitigate and manage those risks. Enhanced due diligence may be essential for an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or an individual who is a politically exposed person (PEP). In particular, such enhanced due diligence is required for foreign PEPs. Decisions to enter into or pursue business relationships with higher-risk customers should require the application of enhanced due diligence measures, such as approval to enter into or continue such relationships, being taken by senior management. The bank's customer acceptance policy should also define circumstances under which the bank would not accept a new business relationship or would terminate an existing one.

3. Customer and beneficial owner identification, verification and risk profiling

35. For the purposes of this guidance, a customer refers, in accordance with the FATF Recommendation 10, to any person[22] who enters into a business relationship or carries out an occasional financial transaction with the bank. The customer due diligence should be applied not only to customers but also to persons acting on their behalf and beneficial owners.[23] In accordance with the FATF standards, banks should identify customers and verify their identity.[24]

36. A bank should establish a systematic procedure for identifying and verifying its customers and, where applicable, any person acting on their behalf and any beneficial owner(s). Generally, a bank should not establish a banking relationship, or carry out any transactions, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. Consistent with BCP 29[25] and the FATF standards, the procedures should also include the taking of reasonable measures to verify the identity of the beneficial owner. A bank should also verify that any person acting on behalf of the customer is so authorised, and should verify the identity of that person.

37. The identity of customers, beneficial owners, as well as persons acting on their behalf, should be verified by using reliable, independent source documents, data or information. When relying on documents, a bank should be aware that the best documents for the verification of identity are those most difficult to obtain illicitly or to counterfeit. When relying on other sources than documents, the bank must ensure that the methods (which may include checking references with other financial institutions and obtaining financial statements) and sources of information are appropriate, and in accordance with the bank's policies and procedures and risk profile of the customer. A bank may require customers to complete a written declaration of the identity and details of the beneficial owner, although the bank should not rely solely on such declarations. As for all elements of the CDD process, a bank should also consider the nature and level of risk presented by a customer when determining the extent of the applicable due diligence measures.[26] In no case should a bank disregard its customer identification and verification procedures just because the customer is unable to be present for an interview (non-face-to-face customer); the bank should also take into account risk factors such as why the customer has chosen to open an account far away from its seat/office, in particular in a foreign jurisdiction. It would also be important to take into account the relevant risks associated with customers from jurisdictions that are known to have AML/CFT strategic deficiencies and apply enhanced due diligence when this is called for by the FATF, other international bodies or national authorities.

38. While the customer identification and verification process is applicable at the outset of the relationship or before an occasional banking transaction is carried out, a bank should use this information to build an understanding of the customer's profile and behaviour. The purpose of the relationship or the occasional banking transaction, the level of assets or the size of transactions of the customer, and the regularity or duration of the relationship are examples of information typically collected. Therefore, a bank

should also have policies and procedures in place to conduct due diligence on its customers sufficient to develop customer risk profiles either for particular customers or categories of customers. The information collected for this purpose should be determined by the level of risk associated with the customer's business model and activities as well as the financial products or services requested by the customer. These risk profiles will facilitate the identification of any account activity that deviates from activity or behaviour that would be considered "normal" for the particular customer or customer category and could be considered as unusual, or even suspicious. Customer risk profiles will assist the bank in further determining if the customer or customer category is higher-risk and requires the application of enhanced CDD measures and controls. The profiles should also reflect the bank's understanding of the intended purpose and nature of the business relationship/occasional banking transaction, expected level of activity, type of transactions, and, where necessary, sources of customer funds, income or wealth as well as other similar considerations. Any significant information collected on customer activity or behaviour should be used in updating the bank's risk assessment of the customer.

39. A bank should obtain customer identification papers as well as any information and documentation obtained as a result of CDD conducted on the customer. This could include copies of or records of official documents (eg passports, identity cards, driving licences), account files (eg financial transaction records) and business correspondence, including the results of any analysis undertaken such as the risk assessment and inquiries to establish the background and purpose of the relationships and activities.

40. A bank should also obtain all the information necessary to establish to its full satisfaction the identity of their customer and the identity of any person acting on behalf of the customer and of beneficial owners. While a bank is required to both identify its customers and verify their identities, the nature and extent of the information required for verification will depend on risk assessment, including the type of applicant (personal, corporate etc), and the expected size and use of the account. The specific requirements involved in ascertaining the identity of natural persons are usually prescribed in national legislation. Higher-risk customers will require the application of enhanced due diligence to verify customer identity. If the relationship is complex, or if the size of the account is significant, additional identification measures may be advisable, and these should be determined based on the level of overall risk.

41. When a bank is unable to complete CDD measures, it should not open the account, commence business relations or perform the transaction. However, there may be circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business. In such circumstances, the bank should adopt adequate risk management procedures with respect to the conditions and restrictions under which a customer may utilise the banking relationship prior to verification. In situations where an account has been opened but problems of verification arise during the course of the establishment of the banking relationship that cannot be resolved, the bank should close or otherwise block access to the account. In any event, the bank should consider filing a STR in cases where there are problems with completion of the CDD measures.[27] Additionally, where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/FT, banks should not voluntarily agree to open accounts with such customers. In such situations, banks should file an STR with the relevant authorities accordingly and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

42. A bank should have in place procedures and material capacity enabling front office, customer-facing activities to identify any designated entities or individuals (eg terrorists, terrorist organisations) in accordance with their national legislation and the relevant United Nations Security Council Resolutions (UNSCRs).

43. While the transfer of funds from an account in the customer's name in another bank subject to the same CDD standard as the initial deposit may provide some comfort, a bank should nevertheless conduct its own due diligence and consider the possibility that the previous account manager may have asked for the account to be closed because of a concern about illicit activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant has been refused banking facilities by another bank due to concerns over illicit activities of the customer, it should consider classifying that applicant as higher-risk and apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

44. A bank should not open an account or conduct ongoing business with a customer who insists on anonymity or who gives an obviously fictitious name. Nor should confidential numbered[28] accounts function as anonymous accounts but they should be subject to exactly the same CDD procedures as all other customers' accounts, even if the procedures are carried out by selected staff. While a numbered account can offer additional confidentiality for the account-holder, the identity of the latter must be verified by the bank and known to a sufficient number of staff to facilitate the conduct of effective due diligence, especially if other risk factors indicate that the customer is higher-risk. A bank should ensure that its internal control, compliance, audit and other oversight functions, in particular the chief AML/CFT officer, and the bank's supervisors, have full access to this information as needed.

4. Ongoing monitoring

45. Ongoing monitoring is an essential aspect of effective and sound ML/FT risk management. A bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity. Without such knowledge, the bank is likely to fail in its obligations to identify and report suspicious transactions to the appropriate authorities. Ongoing monitoring should be conducted in relation to all business relationships and transactions, but the extent of the monitoring should be based on risk as identified in the bank risk assessment and its CDD efforts. Enhanced monitoring should be adopted for higher-risk customers or transactions. A bank should not only monitor its customers and their transactions, but should also carry out cross-sectional product/service monitoring in order to identify and mitigate emerging risk patterns.

46. All banks should have systems in place to detect unusual or suspicious transactions or patterns of activity. In establishing scenarios for identifying such activity, a bank should consider the customer's risk profile developed as a result of the bank's risk assessment, information collected during its CDD efforts, and other information obtained from law enforcement and other authorities in its jurisdiction. For example, a bank may be aware of particular schemes or arrangements to launder proceeds of crime that may have been identified by authorities as occurring within its jurisdiction. As part of its risk assessment process, it will have assessed the risk that activity associated with such schemes or arrangements may be occurring within the bank through a category of customers, group of accounts, transaction pattern or product usage. Based on this knowledge, the bank should design and apply appropriate monitoring tools and controls to identify such activity. These could be through alert scenarios for computerised monitoring systems or setting limits for a particular class or category of activity, for instance.

47. Using CDD information, a bank should be able to identify transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer's normal and expected transactions.

48. A bank should have established enhanced due diligence policies and procedures for customers who have been identified as higher-risk by the bank. In addition to established policies and procedures relating to approvals for account opening, a bank should also have specific policies regarding the extent and nature of required CDD, frequency of ongoing account monitoring and updating of CDD information and other records. The ability of the bank to effectively monitor and identify suspicious activity would require access to updated, comprehensive and accurate customer profiles and records.

49. A bank should ensure that they have appropriate integrated management information systems, commensurate with its size, organisational structure or complexity, based on materiality and risks, to provide both business units (eg relationship managers) and risk and compliance officers (including investigating staff) with timely information needed to identify, analyse and effectively monitor customer accounts. The systems used and the information available should support the monitoring of such customer relationships across lines of business and include all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer's behaviour or business profile and transactions made through a customer account that are unusual.

50. The bank should screen its customer database(s) whenever there are changes to sanction lists. The bank should also screen its customer database(s) periodically to detect foreign PEPs and other higher-risk accounts and subject them to enhanced due diligence.

RBI Guidelines

2. Guidelines

2.1 General

i) Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account.

ii) Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

iii) Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 1976, as amended from time to time, wherever applicable are strictly adhered to.

2.2 KYC Policy

Banks should frame their KYC policies incorporating the following four key elements:

a)Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and
d) Risk Management.

2.3 Customer Acceptance Policy (CAP)

a) Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.

(i) No account is opened in anonymous or fictitious/ benami name(s);

(ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;

(iii) 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 instructions/guidelines issued by Reserve Bank from time to time;

(iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank 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. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

(v) 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 is opened by an intermediary in fiduciary capacity and

(vi) 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 organisations etc.

b) Banks 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. 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 is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

c) 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 and 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 should be categorised 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 should 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 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.

d) It is important to bear in mind 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.

2.4 Customer Identification Procedure (CIP)

a) The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank 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. Banks 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 bank 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 banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in paragraph 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank 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.

b) It has been observed that some close relatives, e.g. wife, son, daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, banks can 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) wanting to open an account is a relative and is staying with him/her. Banks can 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, banks should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

c) Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should 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.

d) An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annex-I to this Master Circular. It is clarified that permanent correct address, as referred to in Annex-I, means 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 bank for verification of the address of the customer.

e) It has been brought to our notice that the said indicative list furnished in Annex – I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

2.5 Customer Identification Requirements – Indicative Guidelines

i) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks should 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 settlors 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.

ii) Accounts of companies and firms

Banks need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with banks. Banks 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.

iii) Client accounts opened by professional intermediaries

When the bank 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. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks 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 bank 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 bank, the bank should still look through to the beneficial owners. Where the banks 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 bank.

iv) 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. Banks 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. Banks should verify the identity 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 a PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

v) 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 case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

2.6 Small Deposit Accounts

(i) Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I of this master circular, banks should open an account for him, subject to:

Introduction from another account holder who has been subjected to full KYC procedure. The introducer’s account with the bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer,

or

any other evidence as to the identity and address of the customer to the satisfaction of the bank.

ii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs.

80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

2.7 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Banks 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. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks 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. Every 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. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

2.8 Closure of accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should 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 need to be taken at a reasonably senior level.

2.9 Risk Management

a) The Board of Directors of the bank should ensure that an effective KYC programme is 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. Banks should, in consultation with their boards, 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 banking/business relationship.

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

2.10 Introduction of New Technologies – Credit cards/debit cards/ smart cards/gift card

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Further, marketing of these cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.11 Combating financing of terrorism

a) In terms of PMLA Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to 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.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Banks are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, banks should 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 should immediately be intimated to RBI and FIU-IND.

Content credits:

https://m.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?Id=4354&Mode=0#:~:text=For%20customers%20that%20are%20legal,of%20that%20person%3B%20(iii)

https://www.bis.org/bcbs/publ/d505.pdf