BANK SUPERVISION SECTOR

27 February 2012

CIRCULAR NO. 1/2012

TO ALL BANKS OPERATING IN THE REPUBLIC

The General Manager/Regional Manager

……. Bank

REGULATIONS AND GUIDELINES FOR BANKS RELATED TO COMBATING MONEY LAUNDERING AND TERRORISM FINANCING

According to the subject in above and pursuant to the directives of the Governor and in compliance with the provisions of Law No. 1/2010 related to Combating Money Laundering and Terrorism Financing and its executive regulation, the rules in this circular should be complied with and taken into consideration.

A. Aim of these Guidelines

- The purpose of these guidelines is to make sure that banks comply with the terms of Law No. 1/2010 on Combating Money Laundering and Terrorism Financing and its executive regulation.
- To protect the banking sector from transactions arising from money laundering and terrorism financing through the banks complying with the policies, regulations, procedures, controls, and principles, which ensure the prevention and detection of money laundering and terrorism financing activities and reporting on them in accordance with international standards.

- To protect banks from illicit transactions and prevent their being exploited as channels for transmitting illegal transactions involving money laundering, terrorism financing, or other illicit activities.
- To enhance the soundness of the banking sector and protect its reputation and integrity thereby protecting its customers.

B. Circular's Application Scope

All banks operating in the Republic of Yemen.

C. Definitions

Without prejudice to the definitions given under Law No. 1/2010 on Combating Money Laundering and Terrorism Financing and the definitions laid down in its Executive regulation, the following words and terms in this Circular will have the meaning assigned against each of them unless the context indicates otherwise.

- **The Law**: Law No. 1/2010 on Combating Money Laundering and Terrorism Financing.
- **Executive regulation**: Executive regulation of Law No. 1/2010 on Combating Money Laundering and Terrorism Financing.
- **The Committee**: The National Committee for Combating Money Laundering and Terrorism Financing.
- **FIU**: Financial Information Unit.
- Funds: Any assets material or otherwise, electronic, transferable or fixed including all types of currencies foreign or domestic, securities, title deeds and documents and derivatives thereof.
- **Money Laundering**: The act defined in Article 3 of the Law.
- **Terrorism Financing**: The act defined in Article 4 of the Law.
- **The Real Beneficiary**: The natural person who owns or who is in actual control of the customer or for whose account the transaction is effected or in his favor or according to his will.
- **Politically exposed persons (PEPs)** by reason of the Office They Hold: Persons who occupy or have occupied high public office in a foreign state such as head of state or government or a distinguished politician, judge, high ranking army officer or government official or a distinguished personality in a political party, including their family members to the third degree.

- **Due Diligence**: The efforts made to know the identity of the customer and the real beneficiary and follow up the transactions carried out in a continuous relationship in addition to understanding the nature and objective of the future relationship between the customer and the financial or non financial institution or the specified professions.
- **Occasional Customer**: A customer who is not in a continuous relationship with the bank.
- **A permanent Relationship**: A financial or banking relationship arising between the bank and the customer which is expected at the outset to last for quite a period of time, involve various transactions and an activity as defined in "financial and nonfinancial institutions" and is related to the services and activities offered by the bank to its customers where the bank expects the relationship will be a lasting one.
- **Shell Bank**: is a bank that has no physical presence in the jurisdiction in which it is incorporated and licensed and is not affiliated to a regulated financial institution group that is subject to effective consolidated supervision.
- **Physical Presence**: A bank has physical presence if:

a. It has fixed premises to receive its customers and to actually conduct its business. It is not enough just to have a local agent or low-level employees.
b. The presence of effective management.
c. Record keeping of transactions.
d. Subject to inspection by the supervision authority either in the country where it was incorporated or where it conducts its activities.

- **Correspondent Banking**: Banking services offered by one bank to another.
- **Non-profit Organization**: Any legal person incorporated in accordance with the provisions of the Law with the main objective of offering social or charitable services without aiming to make a profit from its activities or distributing it or realizing a personal benefit but raising and distributing funds for charitable, religious, cultural, educational or social purposes.
- **Non-Resident Customer**: Natural or legal person residing outside the Republic or someone who has resided in the Republic for less than a year irrespective of the nationality of this person, except those who have permanent economic activities and residences in the Republic of Yemen even though they only stay in Yemen on an intermittent basis.

D. Key Principles for Combating Money Laundering and Terrorism Financing

1st principle Responsibility of the Board of Directors: The Board of Directors and higher executive management of the bank should ensure that its policies, procedures, systems and controls appropriately and adequately address and meet the procedures of AML/CFT Law and these guidelines.

2nd principle Risk - Based Approach: Banks should adopt a risk-based approach in their dealing with customers in accordance with the procedures of the Law, its executive regulation and these guidelines.

3rd principle Know Your Customer: Banks should know each of their customers to the extent appropriate to the customer's risk profile.

4th principle Record Keeping: Banks should keep records of the customers data in accordance with the Law, its executive regulation for the period specified therein.

5th principle Reporting: Banks should have measures in place to ensure internal and external reporting whenever money laundering or terrorism financing is known or suspected.

6th principle High standard examination and continuous training: Banks should have adequate screening procedures to ensure high standards when appointing or hiring officers or employees and also should have an appropriate ongoing AML/CFT training programs for their officers and employees.

E. General AML/CFT Responsibilities

1. Board of Directors' Responsibilities

The Board of directors should be primarily responsible for implementing the following procedures:

1.1. Establishing internal written policies, procedures and controls which are appropriate for the sound application of the Law, its executive regulation and guidelines issued by the Central Bank related to AML/CFT operations.

1.2. The Board of Directors should be primarily responsible for the effectiveness of the internal policies, procedures, systems and controls related to AML/CFT.
1.3. Adequate screening procedures to ensure high standards when appointing or employing officers or employees in the bank.
1.4. Appropriate ongoing training programs for the officers and employees on AML/CFT systems and techniques.
1.5. Establishing an AML/CFT Compliance Unit at the bank head office as well as branches.
1.6. Appointing the officer in charge of the AML/CFT Compliance Unit and his deputy in the bank and granting him the required powers and full independence.
1.7. Establishing an independent internal auditing function with adequate resources to test the extent of compliance with the policies, procedures, regulations and controls related to AML/CFT.
1.8. Establishing specific methodology for risk management in the bank related to AML/CFT.
1.9. Documentation of the policies and methodologies in respect of risk management.
1.10. Necessary steps should be taken to ensure that money laundering and terrorism financing risks are taken into consideration in the daily operations or when new products are developed or new customers accepted.
1.11. Examining AML/CFT procedures related to existent customers.

2. AML/CFT Internal Regulations

2.1. The bank should establish internal rules, policies and procedures which are appropriate for the sound application of the Law, its executive regulation and guidelines issued by the Central Bank pertaining to AML/CFT operations, while periodically examining these policies and procedures to measure the extent of compliance and discover weaknesses and shortcomings and taking necessary action to avoid or remedy them in accordance with the control procedures of money laundering operations.
2.2. The bank should ensure that the actions taken are consistent with the AML/CFT risks and the volume, nature and complexity of its activities.

2.3. The bank should establish a written clear AML/CFT policy endorsed by the board of directors for the application safety of the Law, the executive regulation and guidelines and controls issued in this respect while taking into consideration updating them on a continuous basis.

2.4. Establishing written detailed AML/CFT procedures taking into account the accurate spelling out of duties and responsibilities in consistence with the approved relevant policy in addition to putting in place the necessary arrangements for the carrying out of those policies, procedures, systems and controls for ensuring the prevention of money laundering operations.

2.5. The bank should put in place suitable arrangements for the compliance unit, with the officer in charge of the department to be of high administrative caliber and enabling him and other concerned employees to have access at a suitable time to a customer's identification data and other information related to due diligence Procedures, transaction records and AML/CFT operations.

2.6. The bank should put in place suitable screening procedures to ensure the application of the highest standards in appointing or employing officers and employees.

2.7. The bank should put in place suitable procedures to test integrity and honesty on appointing officers and employees including the compliance officer and his deputy.

2.8. The bank should keep its staff abreast of developments related to AML/CFT techniques, systems and trends and explaining to them clearly all aspects of the Law, the executive regulations and the procedures arising there from and the guidelines particularly those related to due diligence and notification reports on suspicious transactions.

2.9. The bank should set up an ongoing suitable training program for officers and employees.

2.10. The bank should set up arrangements to enable the internal audit function to test the systems established to ascertain their efficiency and effectiveness in AML/CFT and suggest remedies for any deficiency, updates or development required. The audit function should be independent and adequately resourced to test compliance including random sample testing and evaluate the extent of the compliance with

AML/CFT policies, procedures, regulations and controls and preparing reports thereon.

2.11. The bank must ascertain the ability of the internal systems and the policies and procedures adopted to discover unusual transactions or those which are carried out with suspicious customers and referring them to the compliance officer.

3. AML/CFT Compliance Officer and his Deputy

3.1. Appointment

3.1.1. The bank should establish a compliance unit at head office as well as at the branches pursuant to the provisions of Article 27 Paragraph 3 of the executive regulation.

3.1.2. The bank should appoint a compliance officer pursuant to the provisions of Article 27 Paragraph 4 of the executive regulation who will be responsible for AML/CFT in the bank. A deputy should be appointed to carry on his duties during his absence with notification to the Financial Information Unit and the Bank Supervision Sector of their names, titles and also in the event of their replacement.

3.2. Criteria for the appointment of compliance officer and his Deputy

The AML/CFT compliance officer must fulfill the following conditions:

3.2.1. Must be employed a high management level.

3.2.2. Should have suitable academic qualifications and adequate expertise.

3.2.3. Should be a person of integrity, honesty and good reputation.

3.3 General Responsibilities and Authority of the Compliance Officers

The compliance officer must be independent in exercising his duties and must be provided with the essential means to perform these duties in a manner that will achieve the intended objectives. The following matters must be taken into consideration:

3.3.1. Not to entrust him with work that is in contradiction with his duties as the officer in charge of AML/CFT procedures.

3.3.2. He should have the essential authority for carrying out his responsibilities in an independent way.

3.3.3. He should have the authority to report directly to higher management or the board of directors of the bank in order to enhance the efficiency and effectiveness of AML/CFT systems and the compliance of the staff assigned to them.

3.3.4. He should have the power to supervise and monitor the application of AML/CFT policies, procedures, regulations and controls in the bank including the risk based approach to money laundering and terrorism financing risks.

3.3.5. Ascertain that suitable policies, procedures and systems are in place in the bank, develop and preserve them with the aim of monitoring compliance in the daily operations of the bank with the Law and its executive regulation, guidelines, policies, procedures, systems and controls and evaluate them regularly regarding their effectiveness in preventing money laundering and terrorism financing activities.

3.3.6. He has the right to obtain all data and see all records or documents which he deems essential for carrying out his duties in examining the reports of unusual transactions and suspicious reports presented to him. He also has the right to get in touch with relevant staff in the bank for executing his duties and have unrestricted access to all data related to the customers' transactions in the bank at a convenient time with the aim of pinpointing analyzing and monitoring suspicious transactions in an effective manner.

3.3.7. Should insure complete confidentiality and secrecy for all procedures of receiving reports about the unusual operations and suspicion reports , and what is done in examining them and reporting to the FIU.

3.3.8. He should be fully empowered to report to and notify the FIU on transactions which he suspects of involving money laundering or terrorism financing pursuant to the Law and its executive regulation.

3.4. Duties and Responsibilities of the Compliance Officer and his deputy

The compliance officer is in charge of the following:

3.4.1. Receive internal reports on suspicious transactions in the bank, investigate and evaluate them.

3.4.2. Examine the unusual transactions which the bank's internal systems make available to him and the suspicious transactions referred to him by bank staff supported with relevant reasons or those sent to him by any other party.

3.4.3. Prepare the reports on transactions suspected of involving money laundering or terrorism financing on the standard forms designated for this purpose and send them to the FIU in the Central Bank of Yemen.

3.4.4. File transactions in respect of which he finds no grounds for suspicion with the reasons for the action taken.

3.4.5. Ensure prompt response to an inquiry or request for information by the FIU and the Bank Supervision Sector to obtain data related to AML/CFT issues.

3.4.6. Acting as a focal or central point of contact between the bank, FIU, Bank Supervision Sector and other national authorities in connection with AML/CFT issues.

3.4.7. Suggest what is necessary by way of developing and updating the bank policy in the area of AML/CFT as well as the systems and procedures adopted by the bank in this field with the aim of enhancing their effectiveness and efficiency and keeping abreast of local and international developments.

3.4.8. Monitor the accounts and transactions of the bank customers at head office and all the branches in the Republic and abroad.

3.4.9. Overall onsite and offsite inspection on the compliance of all bank branches and the concerned staff at head office and branches with the legal provisions, controls and internal regulations related to AML/CFT as well as completing the "know your customer" form.

3.4.10. Cooperate and coordinate with the department concerned in the bank related to the setting up of bank staff training plans in the area of

AML/CFT, suggest the training programs necessary to implement these plans and follow up implementation.

3.4.11. Ensure that the Compliance Deputy Officer is well informed of the significant developments in AML/CFT.

3.4.12. The Compliance Deputy Officer acts on behalf of the officer in his absence or when the post is vacant and is subject to the same rules that apply to the Officer related to his responsibilities.

3.4.13. Prepare periodic reports at least once every year on AML and FFT activities in the bank and present them to the board of directors to study them within a fixed time frame for pointing out suggestions and deciding on actions to be taken related to them. These reports should be sent to the FIU together with the board of Directors' relevant remarks and decisions.

3.5. Compliance Officer's Annual Report

3.5.1. The report should assess the adequacy and effectiveness of the bank's AML/CFT policies, procedures, systems and controls.

3.5.2. The minimum procedures of the Annual Report that should be submitted to the Board of Directors for each fiscal year should include the following details:

a. The efforts made during the period covered by the report in respect of unusual and suspicious transactions and action taken related to them.

b. The number and types of internal suspicious transaction reports made to the Compliance Officer.

c. The number of reports advised to the FIU and those not advised and reasons thereof.

d. Outcome of the periodic audit of the AML/CFT systems and procedures in the bank, weaknesses revealed and suggestions to avoid them, including the reports produced by the bank's internal systems regarding unusual transactions.

e. Amendments made to policies, internal systems or procedures in the bank in the area of AML/CFT during the period covered by the report.

f. Summary of the extent of compliance with implementation of plans set up during the period covered by the report for the general onsite and offsite inspection of the various bank branches to ascertain the extent of compliance in applying the provisions of the Law and its executive regulation, the guidelines, controls and internal systems related to AML/CFT.

g. Present the plan established for onsite and offsite inspection of the bank branches during the next period.

h. Detailed memo of the training programs held for the bank officers and employees in the area of AML/CFT during the period in question.

i. Items to be improved in training programs and suggestions to implement required improvements and the training program for the following year.

j. Number and types of bank customers classified in the high risk category.

3.6. **Responsibilities of Branches in the Republic**

3.6.1. The bank should ensure that branch employees are in compliance with the Law, its executive regulation and AML/CFT guidelines and controls as well as completing the “Know Your Customer” form.

3.6.2. The Bank should appoint liaison officers in its branches to carry out the duties of the Compliance Officer in the branches.

3.6.3. Set up systems, procedures and internal controls to monitor money transactions and transfers and any other account related transactions especially those made through ATMs and all electronic devices.

3.6.4. Policies and procedures should compel employees to present reports to the compliance officer on any suspicious transactions

and the extent of compliance on the part of the branch with the required procedures.

3.7. **Responsibilities of Branches and Affiliates Abroad**

3.7.1. The bank should ensure that officers and employees in its branches and affiliates abroad are in compliance with the Law, its executive regulation, guidelines, policies, procedures and systems and their application in the host country to the extent permitted by the local laws and regulations in that country.

3.7.2. Policies, procedures, systems and controls should compel officers and employees in branches and affiliates abroad to present reports to the Compliance Officer at the bank's head office in the Republic of Yemen on suspicious transactions.

3.7.3. Branches and affiliates abroad may apply requirements that impose higher standards in respect of AML/CFT policies, procedures, systems and controls in so far as customers, whose operations extend to a number of other countries, are concerned.

3.7.4. If the laws and systems in the host country prevent the application of the provisions of the Law, its executive regulation and guidelines related to compliance with AML/CFT procedures on branches and affiliates, the officers and employees thereof must immediately inform the Compliance Officer at head office and FIU regarding this matter.

3.7.5. The bank should give special attention to procedures in affiliated branches and affiliates in countries that do not apply or inadequately apply the FATF recommendations.

F. Risk Based Approach

- The bank should develop a risk-based approach for monitoring as appropriate its business, number of customers and types of transactions.
- The bank should classify its customers and products according to the degree of money laundering and terrorism financing risk.

- The bank should pay special care in dealing with cases representing high degree of risk.
- The bank should put in place the necessary procedures for dealing with these risks in accordance with their level of seriousness.
- The bank should classify risks into two categories: high and low.
- The bank should revise the classification of customers according to degree of risk at least once every two years or during that period if changing circumstances necessitate such a revision.
- The bank on classifying customer risk should ascertain that the system put in place for risk management includes policies and procedures based on identifying, evaluating, monitoring and reporting risks and that the system deals with all areas of risk.
- The bank on classifying customer risk should as a minimum consider the following four risk elements (customer risks, product risks, transmission channel risks and geographic risks)as the following:

1. Customers Risks

1.1. The bank should assess and document the risks of money laundering, terrorism financing and other illicit activities posed by different types of customers. The intensity of customer due diligence measures and ongoing monitoring required for a particular type of customer should be proportionate to the perceived or potential level of risk posed by the relationship with the customer. The bank should also have the policies and essential procedures for tackling and dealing with these risks.

1.2. The bank should have in place enhanced customer due diligence and ongoing monitoring procedures if it suspects that a customer is an individual, charity or non-profit organization that is associated with, or involved in, terrorism acts or terrorism financing or a terrorism organization per se or when an individual or legal person is subject to sanctions or listed in the circulars sent to banks or exposed to risks because of his position or connection to AML/CFT issues.

1.3. The bank should not enter into a business relationship with non-profit organizations or customers who require enhanced due

diligence except with the approval of top management and after completing the enhanced due diligence measures. Following are some factors for guidance in determining the above mentioned risks:

1.3.1. Risks related to customer

- Customers in whose case it is difficult to identify the real beneficiary of their activities, for example as a result of the complexity of ownership in the case of legal persons.
- Customers with dubious reputation and unsatisfactory records.
- Nonresident customers.
- High risk customers because of their public office (politically exposed persons (PEPs) or those connected to them or foreign customers.

1.3.2. Risks related to Customers' transactions

- Transactions not proportionate to the declared purpose of the relationship.
- Services required incompatible with the nature of the customers' activities.
- Conducting complex or huge transactions without clear justification.
- Dealing with an institution at a location far away from the residence of the customer or place of business without clear justification.
- Holding numerous accounts at the bank and conducting various transactions by the customer or more than one firm located in the same area without a clear reason.
- Dealing in large amounts of cash despite the fact that the activity of the customer does not warrant the use of a lot of cash.
- A clear change takes place in the pattern of relationship of the customer with the bank for no clear reason or it is reported to the bank that the customer is involved in illegal activities.
- Unjustified use of intermediaries in dealing with the bank.
- Customer asks that some transactions be shrouded in utmost secrecy.
- Indirect transactions and those effected through modern electronic means.

1.3.3. Risks related to customers' activities

- Activities characterized by extensive dealing in cash including financial services such as money transfer and foreign exchange companies.
- Charities and other entities that are non-profit organization.

- Traders in precious metals and stones, masterpieces and works of art and real estate agents and companies.

2. Risks Related to Product

2.1. The bank should assess and document the risks of money laundering, terrorism financing and other illicit activities posed by the products it offers or proposes to offer to its customers. Such products may include the saving accounts, financial transfers, payable through accounts, wire transfers etc. The bank should also have a methodology on the basis of which business relationship with customers will be classified based on different types of products it offers or proposes to offer.

2.2. Product related risks include those that may be exploited in money laundering or terrorism financing comprising the new products and services and innovations whether offered by the bank or is a party to them. Of these services are those that do not require a lot of information on their users or those that are of an international nature such as bank services presented through the internet, prepaid cards and international electronic transfers.

3. Delivery Channel Risks

3.1. The bank should assess and document the risk of money laundering, terrorism financing and other illicit activities posed by the mechanisms, electronic banking operations, other operations undertaken electronically through which business relationships are started, conducted and maintained. The intensity of the customer due diligence measures and ongoing monitoring in relation to particular interface must be appropriate and proportionate to the perceived and potential level that may be posed by that interface.

3.2. The bank should have policies, procedures, systems and controls to address specific risks of money laundering and terrorism financing or other illicit activities posed by the different types of interface and technological developments through which business relationships are started, conducted and maintained. The policies, procedures, systems and controls should include measures to prevent misuse of technological developments in money

laundering and terrorism financing schemes and manage specific risks associated with non-face-to-face business relationship or transactions.

3.3. The bank should include in its methodology of procedures how the customers will be classified in relation to the interface through which the business relationship is started, conducted and maintained.

4. Risks related to geographical regions

4.1. The bank should assess and document the risks of involvement in money laundering, terrorism financing and other illicit activities posed by different jurisdictions with which its customers are associated or may become associated. Such association can be where the customer lives, or the business incorporated or otherwise established in a foreign jurisdiction. In identifying high risk jurisdictions, the bank may use the following guidelines:

4.1.1. Jurisdictions subject to sanctions, boycott or other similar measures by the United Nations.

4.1.2. Jurisdictions that lack AML/CFT laws and systems or do not apply the FATF Recommendations or apply them inadequately.

4.1.3. Jurisdictions that finance or support terrorism activities.

4.1.4. Jurisdictions renowned for widespread corruption or other illegal activities such as growing and dealing in narcotics and trafficking and smuggling of weapons etc.

4.2. The bank should have policies, procedures, systems and controls to address the specific risks of money laundering, terrorism financing and other illicit activities posed by different jurisdictions, with which the bank's customers are or may be associated.

4.3. In order to evaluate the effectiveness of AML/CFT regimes in different jurisdictions the bank should consider as a minimum the following three factors:

4.3.1. The legal framework in these jurisdictions.

4.3.2. Sanctions and inspection imposed.

4.3.3. International cooperation.

G. Due Diligence Procedures

1. Customer Acceptance Policy

1.1. The banks should develop clear policies and procedures for the conditions of customer acceptance taking into consideration all factors related to customers, their activities, nationalities and the transactions and accounts with which they are connected and any other indicators associated with customer risk. These policies should include a detailed description for every customer according to risk degree and the basis on which the customer relationship should be classified. Furthermore, the following points should be taken into account in respect of high risk customers:

1.1.1. Special care should be taken in applying the identification procedures related to these customers and their legal status.

1.1.2. The policies and procedures should include a description of these customers.

1.2. These policies and procedures should be laid down in writing and sanctioned by the board of directors of the bank.

2. Customer Due Diligence Basic Procedures

2.1. The bank should not establish a business relationship with the customer, unless this customer and relevant parties to the business relationship, including any beneficial owner, have been identified and verified.

2.2. The bank should not offer services and products or continue to deal with persons without ascertaining their documents and keeping copies thereof. Furthermore, the bank should not enter into a business relationship with anonymous persons or fictitious names.

2.3. The regular business undertaken by the customer should be assessed at regular intervals against the expected pattern of his activity. Any deviation from the norm should be examined in order to determine whether any suspicion arises related to money laundering and terrorism financing. In order to assess unexpected activities, the bank should obtain and keep record of information related to:

2.3.1 Nature of business likely to be undertaken,

2.3.2 Pattern of transactions,

2.3.3 Purpose of the relationship or establishing the account

2.3.4 Nature of the activity.

2.3.5 Signatories to the account and persons having the right to act on the customer's behalf.

2.4. In case the bank has not obtained satisfactory evidence of identity before establishment of the business relationship, it should consider the possibility of sending a report on the suspicious transactions to FIU.

2.5. The bank should establish special systems to identify customers and their legal status and the real beneficiaries whether natural persons or legal persons in the following cases:

2.5.1 On establishment of a continuous business relationship whether on opening the account or the beginning of the relationship in any way.

2.5.2 When suspicion arises at any stage of the relationship with the customer or real beneficiary provided the examination should include in all circumstances an assessment of the aspects of the activities of the customer and the real beneficiary.

2.5.3 When an occasional transaction is undertaken (including numerous transactions which appear to be connected to each other) if its value exceeds one million Yemeni Rials or the equivalent in other currencies.

2.5.4 When an occasional transaction is undertaken in the form of a cable transfers exceeding two hundred thousand Yemeni Rials in value or the equivalent in other currencies the same measures should be applied to the beneficiaries of the transfer taking into account that in all circumstances the complete data required are obtained.

2.5.5 When suspicion or doubt arises of the commitment of money laundering or terrorism financing.

2.5.6 When there is a doubt about the genuineness, accuracy or adequacy of any customer identification data obtained earlier.

2.6. In determining the identification of the real beneficiary the bank should act as follows:

2.6.1 The identification of the customer and real beneficiary should be verified and determined irrespective of whether the customer is an individual or legal person in accordance with the specimen form designated by the bank, provided it contains the minimum level of data required pursuant to Article 8 of the executive regulation.

2.6.2 For all customers, the bank should determine whether the customer is acting on behalf of another person. The bank should also take all necessary steps to obtain sufficient identification data to verify the identity of that other person.

2.6.3 For customers that are legal persons the bank should take steps to:

- Understand the ownership and control structure of the customer,
- Determine the natural person (s) who ultimately own or control the customer.

2.7. The bank should obtain information related to the purpose and nature of the business relationship.

2.8. The bank should determine the extent to which the customer due diligence measures should be applied on the basis of risk sensitivity.

2.9. The bank should be able to prove to the Bank Supervision Sector that the customer due diligence measures in place are convenient and proportionate to the money laundering and terrorism financing risks.

2.10 The bank should not accept from the agent such as a solicitor, accountant, financial broker or persons of similar professions the pretext of professional secrecy on providing the required identification data.

2.11 The bank that is a part of a financial group should take into consideration the activities of the customer with the various branches of the group on applying customer due diligence measures in determining the identification of customers.

2.12 The bank should apply the customer due diligence measures in respect of its present customers on the basis of the strength of material evidence and risks and apply them at the appropriate time of the existing business relationship. Examples of the appropriate time to apply these measures are the following:

2.12.1. When a large transaction is undertaken.

2.12.2. When a considerable change in the customer's documents takes place.

2.12.3. When a material change occurs in the way the business is run and accounts are managed.

2.12.4. Transactions are undertaken that are unusual or in contradiction to the ordinary norm of operations of the customer according to the data available on him at the bank.

2.12.5. A present customer requests a new relationship to be established or a material change effected in the nature of the existing relationship.

2.12.6. When the bank realizes that it does not have sufficient data on an existing customer.

2.13. The customer's identification should be verified by reference to the identification documents and his signature which are kept in the bank's records. If any essential items are missing the customer should be asked to provide them. The identification of existing customers should be verified particularly in the following cases:

2.13.1. On opening all types of accounts whether credit or debit.

2.13.2. Loans and credit facilities of all types.

2.13.3. All types of letters of guarantee.

2.13.4. Financial leasing contracts.

2.13.5. Credit and debit card contracts.

Reliance on a Third Party

1. When the bank decides to seek assistance from another bank, financial institution or intermediary in completing the identification procedures of a customer, either to obtain the necessary data or verify data presented, the ultimate responsibility for meeting the procedures of customer due diligence rests with the bank concerned and not the third party.
2. A bank should only accept customers introduced to it by other financial institutions or intermediaries who have been subjected themselves to FATF equivalent customer due diligence measures.
3. Whenever a bank relies on third parties to perform some of the elements of the CDD process, the bank should obtain the necessary information and documentation concerning the aspects of CDD process from the third party and take adequate steps to make sure that the identification data and other required documents related to CDD process are pursuant to customer identification measures.
4. The bank should ascertain that the third party is subject to control and inspection and has adequate procedures related to the procedures of determining customer identification and record keeping.

5. In case the third party whose assistance is sought is in another country or where the bank has branches or subsidiaries in a foreign jurisdiction, the bank should take into account in which jurisdictions it can rely on third parties for introductions, based on the information available whether these countries apply FATF recommendations adequately.
6. A bank should rely on a third party for introduction only after taking a written confirmation from the introducer that all customer due diligence measures required by FATF Recommendations have been followed and that the identity has been established and verified.
7. The bank should create a direct communication channel with the customer after seeking the documents, data and recommendations from the third party.
8. The bank should be furnished with details of third parties on whom it relies for purposes of customer due diligence measures and notify the Bank Supervision Sector thereof.
9. Whenever the bank is not satisfied that the introducer is in compliance with the procedures of the FATF Recommendations, the bank must conduct itself its CDD process related to customer identification. The bank may also not accept any subsequent introductions from the introducer and consider ceasing to depend on this introducer regarding the application of the CDD process.

a. Failure to Complete the CDD Procedures as Required

When a bank is unable to complete the CDD procedures and verify the identity of the customer, it should act as follows:

1. Not to open an account for the customer or establish any business relationship with him.
2. Where necessary report the matter to FIU.

b. Completing CDD Procedures After Establishing Business Relationship

1. The bank may complete customer and real beneficiary identity verification for CDD process purposes after establishing a business relationship with the customer provided:

- There is little risk of money laundering or terrorism financing and these risks are effectively managed.

- The CDD process is completed as soon as practicable during a period not exceeding fifteen days.

2. If the customer and real beneficiary identity verification is not completed within the period specified in paragraph 1, the bank should act as follows:

- Not to open an account for the customer, establish any business relationship with him or undertake any transaction on his behalf.
- Immediately notify FIU thereof.
- Monitor risk management related to such customers.

3. CDD Measures to Determine Customer Identity

The bank should not maintain accounts in the names of anonymous or fictitious persons and comply with the CDD process in determining and verifying the identity of natural persons and legal persons as well as the relevant real beneficiaries. The bank should obtain the following documents and data:

3.1 Individuals: The bank should as a minimum comply with the following steps to identify a customer:

3.1.1 The bank should ensure that the customer completes the specimen form for opening any type of account provided the forms are standard at the head office as well as the branches and should include as a minimum all the data mentioned in Art 8(1) of the Executive regulations, in addition to signing the form in the presence of the employee concerned.

3.1.2 The bank should obtain the following documents:

- A copy of the personal or family identification card or passport, while in the case of non Yemenis a copy of the passport containing valid residence for the Republic of Yemen.
- Names and details of the persons authorized to have access to the account and their nationalities as well as copies of the documents proving the genuineness of the data provided.
- Names and addresses of the legal representatives of minors and those unable to act on their own as well as copies of the documents proving the genuineness of the data provided.
- Any other documents not mentioned but which the bank may consider necessary.

- The bank should ascertain that the employee concerned has examined the original documents and signed the copies obtained as proof that they are authentic copies of the originals.

3.1.3 Obtain accurate information on the person applying for the opening of the account, his profession and the activities he pursues.

3.1.4 Reasonable steps should be taken to ascertain the beneficial owner of the account.

3.1.5 Reasonable steps should be taken to ascertain if the customer is a high risk person as a result of holding public office.

3.1.6 Obtain an undertaking from the customer to update the details of his record immediately any change occurs to them or when the bank asks for such an update.

3.1.7 The bank should ascertain the genuineness of the data available on the customer by examining the originals of the documents presented by him.

3.1.8 Obtain any other data not mentioned but which the bank may consider necessary.

3.2 <u>Legal persons:</u> If the customer is a legal person, the bank should obtain the details and documents evidencing the nature of the legal person, its legal status, name, nationality, composition of its capital and aspects of its activities. The bank should also obtain the details of the persons officially authorized to have access to the account as well as the names and addresses of the principal shareholders of the legal person and members of its board of directors. Furthermore and as a minimum the following steps should be taken:

3.2.1 The bank should ensure that the customer completes the specimen form for opening any type of account provided the forms are standard at the head office as well as the branches and should include as a minimum all the data mentioned in Art 8(2) of the Executive regulations, in addition to signing the form in the presence of the concerned employee.

3.2.2 The bank should obtain the following documents:

- Authentic copies of the originals of the articles of association, memorandum of association, articles of agreement and license.
- Authentic copy of the original trade registration certificate.

- Name and address of the owner and names and addresses of partners or shareholders the ownership of each of whom exceeds 10% of the capital of the firm or company.
- Names and addresses of the managers authorized to sign on behalf of the firm or company.
- Specimen signatures of the persons authorized to have access to the account
- A written declaration from the customer specifying the identity of the beneficial owner of the account or the beneficiary of the transaction to be undertaken, including his full name, title, place of residence and information on his financial position.
- Resolution of the chairman of the board of directors of the company to open the account including the persons who are authorized to have access to the account and made his and their acquaintance.
- Copy of the personal or family identity card or passport of the proprietor of the firm, the collective (active) partners or the shareholders the ownership of each of whom exceeds 10% of the capital of the company and the authorized signatories on behalf of the company.
- The documents evidencing the authorization by the firm or company to the natural person(s) who represent it.
- Any other documents not mentioned but which the bank may consider necessary.
- The bank should ascertain that the employee concerned has examined the original documents and signed the copies obtained as proof that they are authentic copies of the originals.

3.2.3 Purpose of opening the account and establishment of the business relationship.

3.2.4 In addition to obtaining the documents and procedures mentioned above, the bank must, in the case of limited liability companies, obtain the names and addresses of the chairman of the board of directors, the general manager and the financial manager.

3.2.5 Reasonable steps should be taken to ascertain the beneficial owner of the account.

3.2.6 Reasonable steps should be taken to ascertain if the customer is a high risk person as a result of holding public office.

3.2.7 The bank should pay special attention to legal persons and ascertain their physical existence by means of obtaining a copy of the latest financial report of the company or its financial statements or through any other sources available.

3.2.8 Obtain an undertaking from the customer to update the details of his record immediately any change occurs to them or when the bank asks for such an update.

3.2.9 The bank should ascertain the genuineness of the data available on the customer by examining the originals of the documents presented by him.

3.2.10 Obtain any other data not mentioned but which the bank may consider necessary.

3.3 <u>Non-profit Organizations:</u> The bank should not open any accounts for non-profit organizations without obtaining the following documents and data:

3.3.1 A letter issued by the Ministry of Social affairs and Labor confirming the organization's personality and permission to open bank accounts.

3.3.2 Authentic copy of the original articles of association.

3.3.3 Authentic copy of the original license.

3.3.4 Name of the organization and its legal form.

3.3.5 Addresses of head office and branches.

3.3.6 Telephone and fax numbers.

3.3.7 Purpose of the relationship, sources and uses of its funds and any other information required by the authorities concerned.

3.3.8 Authorized signatories on behalf of the organization and their addresses.

3.3.9 Specimen signatures of persons authorized to have access to the account in accordance with the instructions of the Ministry of Social Affairs and Labor, in addition to the necessity of determining the identity of those authorized to have access to the account in accordance with the above mentioned customer identification process.

3.3.10 The bank should ensure the completion of the bank specimen form containing data related to customer identity verification for non-profit institutions on opening all types of accounts.

3.3.11 The bank should pay special attention in the case of non-profit organizations and societies ascertaining their physical existence and that

the applicants for opening the accounts are really those responsible for the organization or society.

3.3.12 The bank should ascertain the authenticity of the data available on the customer by means of examining the original documents presented and obtaining copies thereof. The concerned employee should sign each copy of the documents as proof that they are authentic copies of the originals.

3.4 Where the person dealing with the bank is acting on behalf of the customer irrespective of whether the customer is a natural person or a legal person, the bank should ensure the existence of a power of attorney issued by the concerned authorities. This document or an authentic copy thereof should be kept by the bank. It is also essential to determine the identities of the customer and agent verifying them according to the above mentioned customer identification process.

4 CDD process to Determine the Identity Related to Correspondent Banks and Financial Institutions

When a bank begins a business relationship with a correspondent bank or financial institution, it should apply the above mentioned CDD measures for determining a customer's identity related to legal persons, in addition to what follows:

4.1 Obtaining the approval of top management of the bank prior to establishing a relationship with correspondent banks.

4.2 Collecting sufficient information on the correspondent bank and its ownership and management structures in order to fully understand the nature of its business. The bank should, through published data, determine the reputation of the correspondent bank and the type of supervision to which it is subjected. The bank should also inquire whether the correspondent bank , any of its board members or controlling shareholders have been under investigation related to money laundering or terrorism financing offences, penalized or administrative measures issued against them.

4.3 Obtaining information on the position of the correspondent bank in respect of its compliance with the local legislations and controls and CDD criteria applied to its customers and its efforts in the area of AML/CFT. The bank

should also ascertain the extent of availability of effective internal policies and procedures at the correspondent bank in this respect by means of some questionnaire which correspondent banks and financial institutions are obliged to complete clarifying their compliance with the local legislations and controls and the criteria and procedures of determining and verifying the identities of their customers and the efforts they make in AML/CFT as well as the availability of effective internal policies and procedures in these banks.

4.4 Determining in writing the responsibility of the correspondent bank or financial institution in respect of AML/CFT.

4.5 Ascertaining that the correspondent bank or financial institution is subject to effective control by the authorities concerned.

4.6 Documentation of all information, documents and agreements signed with the correspondent bank or financial institution and making them available to the concerned authorities when necessary.

4.7 The bank should ensure that the correspondent banks and financial institutions which maintain the payment accounts apply the CDD measures on their customers who have right of access to those accounts. The correspondent bank should also be able to provide the documents and data related to the CDD process and continuous monitoring on request within an acceptable time frame or without delay.

4.8 Periodic examination of the transactions undertaken on the account of the correspondent bank to ascertain that those transactions are compatible with the purpose of opening the account.

4.9 The bank, on applying the CDD process to determine the identity of the correspondent bank, should ascertain the level of risk posed by reference to the data available, of which what follows:

4.9.1 The existence of any control reservations on the bank's AML/CFT and risk management systems.

4.9.2 Whether the location of the correspondent bank's head office is in a high or low risk country.

4.9.3 The extent of private banking services offered by the correspondent bank.

4.9.4 The extent of accounts maintained by the correspondent bank for customers who are considered to be politically exposed persons (PEPs).

4.10 Not to establish correspondent relationship with fictitious banks/financial institutions or with institutions offering correspondent services to fictitious banks.

H. Information Updating

The bank should update the information, data and documents related to the cases mentioned in Article 7 of the Law particularly high risk customers in accordance with the following conditions:

1. The bank should update the information, data and documents mentioned in Article 8 of the Executive regulations every five years but taking into account reducing this period related to high risk customers or where suspicion arises regarding the authenticity or genuineness of the data or information in the bank's records, or regarding the customer himself at any stage of the relationship with him.
2. While taking into consideration the provisions of paragraph 1 above, the updating of documents should take place as follows:

2.1. In the case of accounts opened for natural persons by use of the personal or family identity card or passport the updating should take place every five years if their validity exceeds this period otherwise three months before their expiry.

2.2. In the case of the accounts opened for legal persons in accordance with a profession license or trade registration certificate the updating should take place on the expiry of the license or registration.

2.3. In the case of accounts opened in accordance with official letters or memos from the concerned authority related to non-profit organizations such as associations, charities and others, the updating should take place at least every five years or on the expiry of the specified period in the relevant laws regulating these organizations.

3. In the case of correspondent banks, the updating of information and records should take place regularly every three years as a maximum or on the happening of any changes or suspicions arising in respect of the correspondent bank at any stage of the relationship.
4. If suspicion arises regarding the authenticity of data or identification documents, the bank should verify their genuineness by all means available,

including the contacting of the authorities concerned with registering or issuing these documents and records such as Ministry of Trade and Industry, the General Investment Authority, the Free Zones Authority, Civil Status Authority and Land Registry Authority etc.

5. Where the bank requires any other data on the customer.

I. Continuous Monitoring of the Transactions

1. The bank should put in place an internal system to monitor on a continuous basis the transactions of customers to ensure they are compatible with the customers' records available at the bank and the nature of their activities. The degree of follow up should be proportionate to the level of risk posed by the customer and the nature and volume of his activities, his nationality and his connections with the outside world.
2. Periodic examination, or when needed, of the existing records particularly of customers posing a high risk profile or on the happening of an event requiring an update of the records.
3. The bank should give special attention to all complex transactions or unusually large ones and out of the norm transactions which have no apparent economic or legal objective such as large transactions not compatible with the business relationship with the customer. The bank should also pay special attention to transactions that exceed certain limits and entries in the customer's account that are incompatible with the size of the balance or transactions that are out of the usual norm of the account activity. The background and purpose of those transactions should be examined as far as possible, while documenting all the results reached in writing and made them available to the supervision authorities and external auditors for a period of at least five years.
4. The bank should pay special attention to the internal reports on large complex suspicious transactions and establish a comprehensive system to determine the mechanism of these reports and those responsible for their preparation and the way they are analyzed under guidance of the Compliance Officer and on a daily basis.

Intensive CDD Process for High Risk Customers Transactions and Financial Services

1. The bank should take intensive CDD measures and strengthen its continuous surveillance on realizing the existence of a high degree of money laundering and terrorism financing risks. These measures should be considered over and above the usual CDD Process applied to all customers who is mentioned above.

2. The bank should put in place on enhanced measures for the following high risk persons:

a. Nonresident customers whether legal persons or natural persons are those who have no permanent residence or address in the Republic of Yemen. The following steps should be taken in conducting the identification measures related to these customers and their legal status.
   i. The bank should know the purpose of the relationship.
   ii. Validity of residence in the Republic of Yemen at the outset of the relationship.
   iii. Obtain copy of passport.
   iv. Obtain memo of association in the case of a legal person sanctioned by the authorities concerned in the mother country or its embassy in the Republic of Yemen.
   v. Obtain copy of the license to carry on the business or the trade registration certificate from the mother country signed and stamped by the concerned authority in that country and sanctioned by its embassy in the Republic of Yemen.

b. The bank should take the following steps in the case of politically exposed persons (PEPs) because of their public office:

2.2.1 The bank should in addition to the CDD process mentioned in these guidelines establish risk management systems to determine if the future customer or beneficial owner is a high risk person as a result of his public office such as obtaining information from the customer or by looking up data available to the public or electronic commercial databases on politically exposed persons (PEPs) by way of their public office.

2.2.2 Obtain the approval of top management before establishing a business relationship.

2.2.3 Obtain the approval of top management to continue the business relationship when it becomes known that an existing customer is a politically exposed persons (PEPs) as a result of his public office.

2.2.4 Reasonable measures should be taken to find out the source of wealth and funds of customers and beneficial owners designated as politically exposed persons (PEPs) because of their public office.

2.2.5 The bank should monitor intensively and continuously the business relationship with a customer who is politically exposed persons (PEPs)as a result of his public office.

2.2.6 The bank should keep in a private record all the above measures and precautions related to the customer who is politically exposed persons (PEPs) as a result of his public office.

2.2.7 Periodic examination of the risk management policies and procedures pertaining to this type of customers and corrective measures taken when necessary.

2.2.8 The bank should apply these rules on customers who are politically exposed persons (PEPs) as a result of their public office and their relatives to the third degree.

c. <u>Customers who belong to countries that apply FATF Recommendations inadequately</u>

The bank should take suitable measures to pay special attention to transactions undertaken with persons who belong to countries that do not apply the FATF Recommendations or do not apply them as required, including legal persons and other financial institutions taking strong measures in this respect. Following are examples of the measures:

i. Careful monitoring of the transactions of these customers and finding out their purpose and notifying FIU where a clear economic purpose is lacking or any suspicion arises thereof.

ii. Business relationship or financial transactions should not be undertaken with the above mentioned countries or persons belonging to or are located in them.

d. <u>Non-face-to-face business relationships and new technologies</u>

2.4.1 The bank should put in place policies, procedures and internal systems necessary to avoid risks related to the misuse of technological

developments in the area of money laundering and terrorism financing. Such types of relationship would include transactions concluded over electronic web sites or other means such as the email and internet services as well as ATMs, phone banking , fax and POS services and use of prepaid and debit cards. Examples of policies and arrangements to be established include the verification of documents presented and the request for additional documents related to indirect customers, the establishment of independent contact with the customer, reliance on the intermediation of a third party and made it a condition that the first installment be paid through an account in the name of the customer at another bank subject to the same CDD process. For more details reference should be made to the Basle Committee Report published in July 2003 "Principles of Risk Management Related to Electronic Bank Operations".

2.4.2 The bank should have effective CDD process applied to non-face-to-face customers and establish necessary measures to ascertain the identity of the customer and that the address obtained is his actual address. Such measures may include calling the customer on telephone numbers obtained from him previously belonging to his home, job or work place. His employer may also be contacted with the prior consent of the customer in order to obtain officially details of his salary and other available means such as telephone and electricity bills to verify the address of the customer.

2.4.3 The bank that allows the carrying out of payment transactions through electronic website services should ascertain that the system for monitoring these transactions is the same as the one applied to the other services offered. The bank should also have a risk-based approach to evaluate money laundering and terrorism financing risks arising from such services.

e. <u>Private bank services</u>

i. The bank that provides private bank services should establish policies and systems compatible with determining and evaluating the risks arising from offering these services , taking into consideration the nature of these services including:

- Determining the purpose of the private bank services including the size and type of services to be offered to the customer and the probable activity of the customer's account.
- Development of the business relationship between the bank and the customer utilizing private bank services.

ii. Private bank services represent the provision of personal services to large customers through a central contact officer who liaises between the customer and the bank. This officer facilitates the use by the customer of the private services and products offered by the bank, including:

- Transactions carried out on the various types of accounts.
- Funds transfer.
- Asset management and offering consultant services.
- Lending (including credit cards and personal loans).
- Opening of letters of credit, issue of letters of guarantee and documentary collection processing.
- Safe custody including safe keeping of securities for customers.
- Various other services provided to the customers whether financial or otherwise.

f. <u>Other cases</u>

2.6.1 Products under fictitious names numerical or forged or without a name.

2.6.2 Correspondent bank relationship: on applying for facilities against deposits or hiring safe deposit boxes.

2.6.3 Correspondent payment accounts. On opening a correspondent account it is necessary to obtain a recommendation or signature verification from a known bank.

2.6.4 Agents: On depositing amounts in cash or traveler cheques through a person(s) who do not represent the account holder by means of power of attorney or authorization the bank should subject the agent and the principal to CDD process before undertaking any transaction involving agency. The bank should consider both the principal and agent as its customers.

2.6.5 Bearer negotiable instruments: The bank should have policies, procedures, systems and controls ensuring CDD for AML/CFT risks related to the use of bearer negotiable instruments in so far as the bank is concerned. Before the bank undertakes a transaction involving the

transformation of a bearer negotiable instrument into a registered specimen for dividend or capital payment purposes, the bank should apply the enhanced CDD process on the bearer of the instrument or the beneficial owner and consider both of them as its customers.

Wire Transfers

The bank should apply the CDD process to determine customer identity where the transfer exceeds two hundred thousand Yemeni Rials or the equivalent in other currencies, meanwhile taking into consideration what follows:

1. Outgoing transfers

1.1 The bank that issues the transfer whether its destination is in Yemen or overseas should include all required details and data related to the originator of the transfer that should accompany electronic funds transfer affected by the bank on behalf of its customers.

1.2 The bank should apply due diligence measures to identify the originator of the transfer be he a natural person, legal person or non-profit institution, verify the accuracy of the identity, keep a record thereof and register it in full in the specimen form used for the transfer. The minimum data that should be obtained from the originator of the transfer are as follows:

1.2.1. Name of originator.

1.2.2. Account number or reference number in the absence of an account.

1.2.3. Address of originator.

1.2.4. Purpose of the transfer.

1.2.5. Information of the beneficiary (name, address, account number, if any)

In case the originator has no account, the bank should obtain his personal data and keep an authentic copy of his personal ID or passport.

1.3. The bank should verify the genuineness of all data according to the required measures before initiating any transfer. In the case of bulk transfers the bank should register the originator's account number or reference number in the absence of an account. The bank should also act as follow:

1.3.1. The bank should keep a record of all the data related to the originator.

1.3.2. The bank should be able to provide the necessary data to the receiving bank during a period of three business days from the date of receipt of such a request.

1.3.3. The bank should be able to respond immediately to any order issued by the official authorities for examination of these data.

1.4. The bank should ensure that non-routine transfers should not be batched as batching could increase the money laundering and terrorism financing risks. Such batching obligations do not apply to transfers made by a bank acting as principal, e.g. in the case of spot foreign exchange transactions.

2. <u>Incoming transfers</u>

2.1. The bank should draw up effective procedures and systems to detect transfers unaccompanied by sufficient information on the originator and deal with them appropriately. This may be considered as an element in evaluating the extent of suspicion in the transfer or the transactions connected with it and thereafter FIU should be notified of the suspicion.

2.2. The bank should request the party originating the transfer to submit all missing information and in the event the originating party fails to do so, the bank should take appropriate action based on the risk rating assessment including the refusal of the transfer.

2.3. In case the beneficiary has no account, the bank should obtain his personal data and keep an authentic copy of his personal or family ID or passport.

3. <u>Cases where bank acts as intermediary in the chain of payment</u>

3.1. Where the bank acts as intermediary in the execution of the transfer, it should keep all the information attached to the electronic transfer specimen form.

3.2. If the bank fails to obtain the information attached to the transfer for technical reasons, it should keep all the other information available whether they are complete or not for a period of five years.

3.3. If the intermediary bank receives incomplete information about the originator, it should relay the transfer data to the receiving bank, which should refuse receiving the transfer if it does not contain complete data on the originator.

4. <u>Circumstances where the above procedures do not apply</u>

4.1. When the transaction is executed through the use of a debit or credit card, provided the card number is attached to all transfers arising out of the

transactions and the card is not used as a payment instrument for a financial transfer.

4.2. When the transfer transaction is effected from a bank to another and both originator and beneficiary are banks acting for their own accounts.

J. Simplified CDD Measures

1. The bank may apply simplified CDD measures in circumstances where money laundering and terrorism financing risks are low.
2. The bank may apply simplified CDD measures related to the customers, transactions or products where the risks are low, as follows:

2.1. Ministries, authorities and government institutions.

2.2. Financial institutions that are in compliance with AML/CFT procedures as provided in the Law, the Executive regulations, these guidelines and FATF Recommendations. They should also be supervised to ensure their continuous compliance with these procedures.

2.3. In the event of a one-off or occasional transaction is undertaken where the amount is less than one million Yemeni Rials or the equivalent in other currencies, it may be sufficient to obtain the name and contact details of the customer.

2.4. In the event of occasional transactions for an occasional customer in the form of wire transfers amounting to less than two hundred thousand Yemeni Rials or the equivalent in other currencies, it may be sufficient to obtain the name and contact details of the customer.

2.5. The bank wishing to apply simplified CDD measures on the above customers must retain documentary evidence in support of its categorization of the customer.

2.6. Simplified CDD process should not be applied when the bank knows, suspects or has reason to suspect that the customer is engaged in money laundering or terrorism financing or the transaction is carried out on behalf of another person involved in money laundering or terrorism financing activities.

2.7. Simplified CDD process should not be applied when the bank knows , suspects or has reason to suspect that the transactions are linked and intended to circumvent the threshold specified in the above two paragraphs.

STRs Requirements

1. The bank should draw up effective policies, procedures and controls for reporting to FIU all transactions suspected of involving money laundering or terrorism financing including attempts to execute those transactions regardless of the size of the transaction. These policies and procedures should enable the bank to comply with the Law, its Executive regulations and these guidelines in respect of preparing reports on suspicious transactions and sending them expeditiously to FIU in addition to effective cooperation with FIU and the authorities implementing the Law.
2. The STR should include details of the reasons on which the bank relied in its report that the transaction is a suspicious one as well as the facts and circumstances on which the bank based its suspicion.
3. Reporting should be completed on the specimen form prepared by FIU and distributed to banks together with instructions on how it should be completed. All data and copies of documents related to the suspicious transaction should be attached to the report, taking into consideration compliance with the instructions in completing the form.
4. The bank should ascertain that it has effective policies and procedures related to internal reporting on all money laundering and terrorism financing suspicious transactions. These policies and procedures should enable the bank to comply with the Law, its Executive regulations and these guidelines and make it possible to present the internal reports on suspicious transactions expeditiously to the Compliance Officer.
5. The bank should ensure that all officers and employees have direct access to the bank's Compliance Officer and that the reporting hierarchy between the employees and Officer is short. All officers and employees of the bank are obliged to report when they have reasonable grounds to doubt or suspect that funds channeled through the bank are proceeds of criminal activities or related to terrorism financing or linked to or are to be used for terrorism or by a terrorism organization.
6. The officers and employees of the bank should promptly make an internal report on the suspicious transaction to the Compliance Officer. They should also promptly report all subsequent transaction details on the customer to the Compliance Officer. The latter must properly and appropriately document

the report and furnish a written acknowledgement to the officer or employee, together with a reminder of the provisions related to tipping off. The Compliance Officer should also consider the internal report in the light of all relevant information available to the bank and decide whether the transaction is suspicious and furnish a written notice to the employee in this respect.

7. Tipping off the customer, beneficiary or anyone else except the pertinent authorities and parties is prohibited pursuant to the provisions of the Law and the Executive regulations, on any item of the report related to a suspicious financial transaction that it involves money laundering or terrorism financing or data related to it.
8. Bank staff should be trained on indicators of suspicion related to transactions that may involve money laundering or terrorism financing, including the basic suspicion indicators in respect of money laundering and terrorism financing contained in Circular No. 2/2012.

K. AML/CFT Training

1. The bank should put in place appropriate ongoing AML/CFT training plans and programs for its officers and employees on an annual basis as a minimum.
2. The bank training program should be an ongoing one to ensure that officers and employees maintain their knowledge, skills and capabilities with the aim of enhancing their efficiency in complying accurately with the regulations and systems prescribed for AML/CFT and their understanding and keeping abreast of new developments pertaining to general methods and trends of money laundering and terrorism financing and systems for combating them and local and international new events in this field.
3. The Bank should carry out a review of training needs at regular intervals, examining the issues of existing experience, skills and capabilities as well as required posts and roles. The bank should also look into its size and its risk rating, the results of previous training and future needs, while the board of directors should take into account the results of every review.
4. These programs should be planned and carried out in coordination with FIU at CBY and AML/CFT National Committee, meanwhile taking into consideration the following:

4.1. Training should cover all the units of the bank and all its officers and employees.

4.2. In carrying out training programs assistance should be sought from the Banking Studies Institute and specialized institutes to be established for this purpose or where AML/CFT training is part of their curriculum, whether inside the country or outside, while benefiting from local and international experience in this respect.

4.3. Coordination should be made with the Compliance Officer regarding the selection of staff to attend training programs in this area.

4.4. The Bank Supervision Sector and FIU in CBY should be informed of all the details of the programs mentioned above.

L. Records and Documents Keeping

1. The bank should comply with the provisions of Art. 24 of the Executive regulations related to the keeping of records, data, documents and information for a period of five years or longer if requested by the pertinent authority, in addition to keeping the documents of the following items:

1.1. The required records related to domestic or international transactions after the execution of the transaction regardless of whether the account or business relationship is ongoing or has been terminated.

1.2. The documents and records related to accounts opened for natural persons and legal persons or banks and other financial institutions as from the date of closing the account.

1.3. The documents and records related to transactions undertaken for persons who do not maintain an account with the bank (occasional customers).

1.4. The documents and records related to unusual or suspicious transactions which should include copies of the reports on the transactions sent to FIU and relevant data and documents until a judicial verdict or final decision related to the transaction is issued whichever is later.

1.5. The records related to wire transfers containing incomplete data on the applicant.

1.6. The documents and records of training programs including all programs offered to the officers and employees in the bank on AML/CFT, as well

as the names of trainees and sections and departments where they work, contents and duration of the training program and the institute which conducted the training whether in Yemen or abroad, as from the date of termination of the training program.

1.7. The records and documents related to transactions undertaken with customers provided they contain sufficient data to understand the details of each transaction separately.

1.8. The records and documents of reports which the Compliance Officer has taken a decision to save and keep on record, as from the date the decision has been taken.

2. The bank should keep all records, documents and reports in a safe way, besides keeping additional copies thereof in another place.

3. The system of keeping and retaining records and documents should enable their retrieval easily and promptly, in such a way that any data or information required can be retrieved and made available in adequate form and without delay.

M. General Provisions

1. These guidelines are compulsory on all banks operating in the Republic of Yemen and are part and parcel of their regulations and procedures aiming at controlling, detecting and preventing AML/CFT activities.

2. The banks should comply with the following:

2.1. Put in place a manual for AML/CFT procedures which defines the policies and procedures for identifying a customer and the departments responsible for AML/CFT in the bank, in compliance with these guidelines and AML/CFT procedures, while the bank carries on its business and the system of continuous monitoring of the customers' transactions and accounts and money laundering and terrorism financing indicators.

2.2. Every bank should provide and make available an electronic data base containing the names of all persons reported by CBY or those with suspicious accounts and reported to the bank by FIU or the ones under suspicion by the bank itself, in order to enable the employees in charge of opening accounts and dealing directly with the customer at the very beginning of establishing the business relationship to detect the persons

whose names are included in the database, when they attempt to open accounts at the bank whether in person or through an agent or when executing any occasional transaction with any of them. The FIU should be informed immediately when any of those names is detected.

2.3. Training employees on a continuous basis. Those in charge of training programs and concerned staff should participate in training courses, seminars and workshops related to this matter with the objective of always understanding and appreciating AML/CFT issues.

2.4. Introducing employees to the provisions of the AML/CFT Law, its Executive regulations and the pertinent guidelines issued by CBY.

3. Any officer or employee of a bank is prohibited from running an account as an agent on behalf of a customer with the exception of a husband, a wife or relatives of the first degree and after obtaining the approval of top management.
4. In connection with occasional transactions for those who have no accounts and which do not exceed one million Yemeni Rials or the equivalent in other currencies or a number of transactions which appear to be connected to each other, a special register should be set up, manual or electronic, to input all data required on the customer.
5. If the account is opened or various banking or occasional transactions are effected through correspondence, the applicant is required to verify his signature on the dispatched documents, if he resides abroad, through a correspondent bank, affiliate, representative office of the bank, a branch or another bank. In addition to the verified signature, it is also required the dispatch and receipt of a sanctioned copy of the applicant's passport, ID or residence card, pursuant to the guidelines related to dealing with a third party.
6. The contract concluded between the bank and external auditor should provide for obliging the latter to ascertain that the bank is in compliance with the AML/CFT Law, its Executive regulations and these guidelines. The external auditor should also express an opinion on the adequacy of the bank's policies and procedures in this respect in the report he submits to bank management. It is essential that he informs CBY immediately he discovers any violation of these guidelines.

7. The bank should put in place a charter of honor or code of conduct for its employees containing bank business ethics. The staff of the internal auditor's department should be trained to test these ethics or norms of behavior and report noncompliance with them, the high cost of living of the bank employees which is inconsistent with the salaries they obtain and the employees who use their personal accounts for purposes that do not concern them or at the service of bank customers or other persons.
8. In applying this circular the nature of microfinance banks and the bank activities they are allowed to pursue should be taken into consideration.
9. In case of violation of any of these guidelines, the bank shall be liable to a penalty or proceeding tougher than those imposed by the Banking Law No. 38 for 1998 or the provisions of the Law and its Executive regulations.

These guidelines come into force on the date of their issue.

Mohamed Saad Al Rowdhi

Sub Governor

Bank Supervision Sector

Central Bank of Yemen

27/02/2012