



BANQUE D'INVESTISSEMENT ET DE DÉVELOPPEMENT DE LA CEDEAO  
ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT  
BANCO DE INVESTIMENTO E DE DESENVOLVIMENTO DA CEDEAO

**PROCEDURES FOR THE  
APPLICATION OF THE  
FRAMEWORK  
DOCUMENT ON ANTI-MONEY  
LAUNDERING AND  
COUNTERING THE FINANCING  
OF TERRORISM AND  
PROLIFERATION OF WEAPONS  
OF MASS DESTRUCTION**

**April 2023**

## PREAMBULE

**Considering** Decision A/Dec.3/06/06 of 14 June 2006 relating to the Reorganization of the ECOWAS Bank for Investment (EBID);

**Considering** Articles 24, 25, 26 and 27 of EBID's Articles of Association on the composition, powers, meetings and decision-making procedures of the Board of Directors;

**Considering** Resolution n° RES.24/08/07/BIDC/EBID/CA/BD/18 of 21 August 2007 relating to the EBID Risk and Credit Committee;

Upon recommendation of the Risk and Credit Committee during the 37th meeting of the Committee held on march 29th 2023 ;

The Board of Directors, by Resolution N°17/04/23/BIDC/EBID/CA/BD/83 of April 3, 2023, approves the Procedures for the application of the framework document on anti-money laundering and countering the financing of terrorism and proliferation of weapons of mass destruction as follows:



BANQUE D'INVESTISSEMENT ET DE DÉVELOPPEMENT DE LA CEDEAO  
ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT  
BANCO DE INVESTIMENTO E DE DESENVOLVIMENTO DA CEDEAO

## ACRONYMS

**BCEAO:** Central Bank of West African States

**EBID:** ECOWAS Bank for Investment and Development

**ECOWAS:** Economic Community of West African States

**FIU:** Financial Intelligence Unit

**IMF:** International Monetary Fund

**FATF:** Financial Action Task Force FATF

**GIABA:** Financial Action Group. Inter-Governmental Action Group against Money Laundering.

**KYC:** Know Your Customer

**AML/CFT:** refers to Anti-Money Laundering Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction

**OECD:** Organization for Economic Cooperation and Development

**UNO:** United Nations Organization

**PEP:** Politically Exposed Person

**WAEMU:** West African Economic and Monetary Union

## CONTENTS

### Table of Contents

<b>PREAMBULE</b> .....	<b>2</b>
<b>ACRONYMS</b> .....	<b>3</b>
<b>INTRODUCTION</b> .....	<b>6</b>
1. <b>PROCEDURE N° 1: AML/CFT Compliance Function</b> .....	<b>7</b>
2. <b>PROCEDURE N° 2: AML/CFT Mechanism</b> .....	<b>8</b>
3. <b>PROCEDURE N° 3: Responsibilities of the AML/CFT Compliance function</b> .....	<b>8</b>
4. <b>PROCEDURE N° 4 : Money Laundering Risk Mapping</b> .....	<b>9</b>
5. <b>PROCEDURE N° 5 : Measures Relating to the Identification of Promoters and Other Business Relationships – Customer Due Diligence or Know Your Client (KYC)</b> .....	<b>11</b>
6. <b>PROCEDURE N° 6: Identification of Beneficial Owners</b> .....	<b>14</b>
7. <b>PROCEDURE N° 7: Provisions applicable to Trusts</b> .....	<b>15</b>
8. <b>PROCEDURE N° 8: Identification of other business relationships and other information requirements</b> .....	<b>15</b>
9. <b>PROCEDURE N° 9: Enhanced due diligence with regards to identifying and knowing business relationships</b> .....	<b>16</b>
10. <b>PROCEDURE N° 10: Enhanced due diligence in relation to Politically Exposed Persons and Non-profit Organizations</b> .....	<b>18</b>
11. <b>PROCEDURE N° 11 : Enhanced due diligence over country risks</b> .....	<b>19</b>
12. <b>PROCEDURE N° 12: Due diligence with regard to the means of payment and new technologies</b> .....	<b>20</b>
13. <b>PROCEDURE N° 13 : Closer examination of certain transactions to be recorded in the confidential register</b> .....	<b>21</b>
14. <b>PROCEDURE N° 14: Reporting suspicious transactions</b> .....	<b>21</b>
15. <b>PROCEDURE N° 15 : Combating the financing of terrorism and the proliferation of weapons of mass destruction and implementing the international financial sanctions</b> .....	<b>23</b>
16. <b>PROCEDURE 16 : Training and awareness</b> .....	<b>25</b>
17. <b>PROCEDURE N° 17 : Data protection and Archiving of documents</b> .....	<b>25</b>
18. <b>PROCEDURE N° 18 : Professional secrecy – Prohibition of disclosure</b> .....	<b>26</b>
19. <b>PROCEDURE N° 19 : Responsibility of Executives and Staff – Legal Protection</b> .....	<b>27</b>
20. <b>PROCEDURE N° 20 : AML/CFT monitoring and internal reporting</b> .....	<b>28</b>
<b>ANNEXES</b> .....	<b>30</b>
<b>ANNEX 1: AML/CFT Bank Questionnaire for Correspondent Banks</b> .....	<b>30</b>
<b>ANNEX 2: Alert report</b> .....	<b>30</b>
<b>ANNEX 3: Monitoring Chart for Anti-Money Laundering Activities</b> .....	<b>30</b>
<b>ANNEX 4: Questionnaire non-bank AML/CFT and KYC</b> .....	<b>30</b>



## INTRODUCTION

This document contains the Procedures for the Application of the Framework Document on Anti-Money Laundering and Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction. These procedures are key for the effective implementation of the Bank's policy on anti-money laundering, countering the financing of terrorism policy and countering the proliferation of weapons of mass destruction and aim at providing the EBID staff with detailed information on the requirements to fully implement the Bank's AML/CFT framework.

The present procedures are in conformity with the latest update of the 40 FATF Recommendations and GIABA recommendations. The procedures are also based on relevant International Conventions of the United Nations, the African Union and international good practices, standards and legislation.

By virtue of their contents, the procedures are for Senior Executives of EBID, officers in charge of the anti-money laundering mechanism, and persons in charge of client relations and other business relationships including persons in charge of support duties.

These procedures apply to all operations of EBID, including direct loans, syndicated loans, equity participation, guarantees, resource mobilization, and financial investments.

## **1. PROCEDURE N° 1: AML/CFT Compliance Function**

- 1.1. The Board in its supervisory function takes the responsibility for setting, approving and overseeing the implementation of an adequate and effective internal governance and internal control framework to ensure compliance with applicable requirements in the context of the prevention of money laundering and financing terrorism.
- 1.2. EBID's person in charge of compliance, shall be appointed by the President of the Bank, to be in charge of the day-to-day operation of the Banks's anti-money laundering and countering the financing of terrorism (AML/CFT) policies, procedures.
- 1.3. The Bank shall provide the compliance function with adequate resources, including staff and technology, for the discharge of its obligations, and shall ensure that the powers to propose any measures necessary to ensure the effectiveness of the Bank's internal policies, controls and procedures are granted to the persons responsible for those functions.
- 1.4. Compliance staff shall not be placed in a position where there is a possible conflict between their compliance responsibilities and any other responsibilities they may have.
- 1.5. AML/CFT compliance staff may enter all areas of the Bank and have access to any documents and records considered necessary for the performance of responsibilities set out in these procedures and for the correct implementation of the AML/CFT Policy.
- 1.6. The person in charge of AML/CFT compliance shall have the right to require all members of Management and staff promptly to supply such information and explanations as may be needed.
- 1.7. The person in charge of AML/CFT compliance shall keep abreast of sound compliance practices and in particular take into account the recommendations of the FATF, GIABA and other relevant standard setters and international standards and legislation on AML/CFT compliance-related issues.
- 1.8. The person in charge of AML/CFT compliance shall submit once a year, or more frequently where appropriate, to the Board of Directors a report on the implementation of its internal policies, controls and procedures, and shall keep the Board of Directors informed of the outcome of any reviews.
- 1.9. The Board of Directors will take the necessary actions to remedy any deficiencies identified in a timely manner.
- 1.10. The compliance function shall be further detailed in a Compliance Charter approved by the Board of Directors.

## **2. PROCEDURE N° 2: AML/CFT Mechanism**

- 2.1. The Banks' AML/CFT mechanism for anti-money laundering, countering the financing of terrorism and weapons of mass destruction shall be implemented in accordance with the related AML/CFT Policy document, these procedures, the AML/CFT Compliance Charter and any other document related with AML/CFT, approved by EBID.
- 2.2. Each Head of Department shall appoint one person as AML/CFT correspondent to serve as relay and provide assistance on AML/CFT within the Department.
- 2.3. The Bank's AML/CFT procedures shall be set out in writing.
- 2.4. The person in charge of AML/CFT compliance shall be responsible for the implementation of the Bank's AML/CFT Mechanism.

## **3. PROCEDURE N° 3: Responsibilities of the AML/CFT Compliance function**

- 3.1. The EBID's AML/CFT Compliance Function shall have responsibilities in the following areas:
  - a) Preparation of a risk assessment framework;
  - b) Preparation and implementation of the Banks's policies, controls and procedures and receiving information on significant or material weaknesses in such policies, controls and procedures.
  - c) Preparation of policies and procedures and to provide advice in relation to customer due diligence, including high-risk customers, sectors, among others.
  - d) Monitoring the Bank's compliance with the AML/CFT mechanism;
  - e) Reporting to the Board on measures to be taken to ensure compliance with applicable standards and international legislation, and provide an assessment of the possible impact of any changes in the international standards and legislation on the Banks's activities and compliance framework;
  - f) Reporting suspicious transaction to the FIUs;
  - g) Planning and implementation of training and awareness activities to the EBID staff on AML/CFT;
  - h) Others as may be determined by the Board or defined in the AML/CFT Charter of Compliance.

3.2. The Charter of Compliance shall clearly set out the competencies of the person in charge of AML/CFT compliance.

#### **4. PROCEDURE N° 4 : Money Laundering Risk Mapping**

4.1. The objective of the AML/CFT risk assessment is to identify and assess the risks of money laundering and terrorism financing, taking into account risk factors including those relating to customers, countries or geographies areas, products, services, transactions or delivery channels.

4.2. The following shall guide the risk-based approach applied by EBID:

- a) The assessment of the money laundering and terrorism financing risk profile of EBID, including the risks of non-compliance, shall be reviewed both periodically and when there are major events or developments in its management and operations;
- b) EBID shall also set up a monitoring system to detect atypical transactions that might raise money laundering or terrorist financing suspicions;
- c) To ensure the effectiveness of the transaction monitoring, the Banks's monitoring activity should in principle cover all services and products offered to customers and all transactions which are carried out on behalf of the customer or offered to the customer by the Bank;
- d) Notwithstanding the above, not all transactions need to be scrutinized individually;
- e) The intensity of the monitoring shall respect the risk-based approach and shall be designed around precise and relevant criteria, taking account, in particular, of the characteristics of the customers and the risk level associated with them, the products and services offered, and the countries or geographical areas concerned;
- f) Due diligence measures should match the level of risk associated with the type of client or business relationship (public sector, private sector, banks, other), type of country concerned, type of product (direct loan, syndicated loan, guarantee, equity participation, letter of credit, other). The analysis should be formalized in a scale of risk mapping designed specifically for money laundering risks;
- g) Identify, where appropriate, sectors or areas where enhanced measures are to be applied, and, where appropriate, specifying measures to be taken. With regard to high-risk categories, enhanced due diligence should be applied during the identification and know your client phase on the one hand, and the monitoring of transactions on the other hand;
- h) Identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorism financing;
- i) Use the identification process above in the allocation and prioritization of resources to combat money laundering and terrorism financing and to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorism financing;

- j) Make information available promptly to the competent departments to facilitate the carrying out of the Banks's money laundering and financing terrorism risk assessments;
- k) On the basis of proven cases that may have been reported to the person in charge of AML/CFT compliance and potential risks that could occur, the person in charge of AML-CFT compliance shall prepare plans of action aimed at reducing such risks e.g. may urge the Departments of Operations to enhance knowledge of clients and partners in order to curb counterpart risks and the risk of money laundering.
- l) The AML/CFT compliance function must update the money laundering risk mapping system once a year. The process shall take, at least, the following into consideration:
  - i. type of events that led to suspicions of money laundering;
  - ii. primary underlying offenses revealed in the dossiers forwarded to FIUs;
  - iii. type of offenses described in FIU, FATF and GIABA reports;
  - iv. List of countries mentioned by FATF where inadequate legislation or practices hinder anti-money laundering efforts.

4.3. The risk mapping involves differentiating low and high risks for each category of client, country and operations. The approach is presented, as an example, in the form of a table, below:

	Low Risk	Normal Risk	High Risk
<b><i>Client and other relationships</i></b>			
Regulated banks <sup>1</sup> FATF listed countries			XXXXXXXX
Regulated banks Countries not listed		XXXXXXX	
Countries with an efficient AML/CFT mechanism	XXXXXXXX		
Countries under UN sanctions			XXXXXXXX
Public Sector Borrowers			XXXXXXXX
Private Sector Borrowers		XXXXXXX	
Defaulting borrowers Non-performing loans & files for			XXXXXXXXXX

litigation			
Politically exposed persons			XXXXXXXX
<b><i>Economic sectors</i></b>			
Building and public works			XXXXXXXX
Mining and oil sectors			XXXXXXXX
Import – export			XXXXXXXX
Other economic sectors		XXXXXXX	
<b>Transaction (Means of payment)</b>			
Project financing			XXXXXXXX
Equity participation			XXXXXXXX
Cash			No cash
Cheques			XXXXXXXX
Wire transfers		XXXXXXX	

**5. PROCEDURE N° 5 : Measures Relating to the Identification of Promoters and Other Business Relationships – Customer Due Diligence or Know Your Client (KYC)**

- 5.1. In relation to Customer Due Diligence and identification of banks, lending institutions, guarantee funds, other financial institutions and borrowers, EBID shall apply customer due diligence measures:
- a) when establishing a business relationship;
  - b) when there is a suspicion of money laundering or terrorism financing; or
  - c) when there are doubts about the veracity or adequacy of previously obtained customer identification data.
- 5.2. The following rules shall apply in relation with identification of customers or “Know Your Client”:
- a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

- b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the Bank is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
  - c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
  - d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.
- 5.3. Notwithstanding the above rules, the following shall specifically apply for Know Your Client measures:
- a) With regard to financial institutions, accreditation by regulatory authority (Central Bank);
  - b) With regard to banks and business enterprises, extract from the Trade, Companies and Mortgage Register, current status, most recent audited accounts and External Auditor's Report;
  - c) With regard to representatives of corporate bodies (banks and business concerns):
    - i. Valid identity card or any similar document (passport) including a photograph;
    - ii. Confirmation of address (i.e electricity bills, water bills, telephone bills including the address of the representative of corporate bodies);
    - iii. Substantiation of powers.
- 5.4. When performing the identification of the client, EBID staff shall also verify that any person purporting to act on behalf of the customer is so authorized and identify and verify the identity of that person.
- 5.5. EBID shall prohibit:
- a) any new relationship when prior identification is obviously impossible or unsatisfactory (prospective client's refusal to forward identification documents from reliable and independent sources, forged documents, and other similar situations);
  - b) to make payments on anonymous accounts or anonymous passbooks or accounts with fictitious names. EBID shall, in any event, require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.
- 5.6. Where the business relationship proves to be unsatisfactory, project examination and/or any other transaction must be suspended.
- 5.7. Legal contract documentation should make provision for the likelihood of early loan

reimbursement and termination of business relationship where the identification data forwarded proves to be false or extremely inaccurate.

- 5.8. When performing the identification measures EBID staff shall take into account at least the following variables when assessing the risks of money laundering and terrorist financing:
- a) the purpose of an account or business relationship;
  - b) activities of the company and its promoters
  - c) company's balance sheet and assets of natural persons and origin;
  - d) the level of assets to be deposited by a customer or the size of transactions undertaken;
  - e) the regularity or duration of the business relationship.
- 5.9. Simplified customer due diligence measures may be applied when the Bank ascertains that the business relationship or the transaction presents a lower degree of risk.
- 5.10. The Bank shall ensure sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.
- 5.11. When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, the Bank shall take into account at least the following factors of potentially lower risk situations:
- a) Customer risk factors:
    - i. public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
    - ii. public administrations or enterprises;
    - iii. customers that are resident in geographical areas of lower risk as set out in point (c) below;
  - b) Product, service, transaction or delivery channel risk factors:
    - i. financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
    - ii. products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).
  - c) Geographical risk factors:
    - i. Member States;
    - ii. third countries having effective AML/CFT systems;
    - iii. third countries identified by credible sources as having a low level of corruption or other criminal activity;
    - iv. third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised GIABA and FATF Recommendations and effectively implement those requirements.

5.12. The questionnaire to be used for the purpose of non-bank AML/CFT and KYC is in the Annex to these procedures.

## **6. PROCEDURE N° 6: Identification of Beneficial Owners**

6.1. For the purpose of this procedure, beneficial ownership shall mean any natural person who ultimately owns or controls a legal entity or express trust or similar legal arrangement, as well as any natural person on whose behalf or for the benefit of whom a transaction or activity is being conducted.

6.2. The following shall apply in relation with beneficial ownership:

- a) EBID will ensure that corporate and other legal entities with which performs its business have obtained and hold adequate, accurate and current information on its beneficial ownership, including the details of the beneficial interests held.
- b) Those entities shall be required to provide, in addition to information about their legal owner, information on the beneficial owner when the Bank is taking customer due diligence measures in accordance with the previous sections. This information will be accessible in a timely manner by the Bank's compliance function and shall be kept in a central register which is adequate, accurate and current.
- c) For the purpose of this procedures, control through an ownership interest' shall mean an ownership of 25% plus one of the shares or voting rights or other direct or indirect ownership interest in the corporate entity, including through bearer shareholdings, on every level of ownership.
- d) For the purpose of this procedure, 'control via other means' shall include at least one of the following:
  - i. the right to appoint or remove more than half of the members of the board or similar officers of the corporate entity;
  - ii. the ability to exert a significant influence on the decisions taken by the corporate entity, including veto rights, decision rights and any decisions regarding profit distributions or leading to a shift in assets;
  - iii. control, whether shared or not, through formal or informal agreements with owners, members or the corporate entities, provisions in the articles of association, partnership agreements, syndication agreements, or equivalent documents depending on the specific characteristics of the legal entity, as well as voting arrangements;
  - iv. links with family members of managers or directors/those owning or controlling the corporate entity;
  - v. use of formal or informal nominee arrangements.
- e) For the purpose of this procedure, beneficial ownership information shall be adequate, accurate, and current and include the following:

- i. the first name and surname, full place and date of birth, residential address, country of residence and nationality or nationalities of the beneficial owner, national identification number and source of it, such as passport or national identity document, and, where applicable, the tax identification number or other equivalent number assigned to the person by his or her country of usual residence;
  - ii. the nature and extent of the beneficial interest held in the legal entity or legal arrangement, whether through ownership interest or control via other means, as well as the date of acquisition of the beneficial interest held;
  - iii. information on the legal entity or legal arrangement of which the natural person is the beneficial owner, as well as the description of the control and ownership structure.
- f) Beneficial ownership information shall be obtained within 14 calendar days from the creation of legal arrangements. It shall be updated promptly, and in any case no later than 14 calendar days following any change of the beneficial owner(s), and on an annual basis.

## **7. PROCEDURE N° 7: Provisions applicable to Trusts**

- 7.1. The Bank shall assess if trustees have obtained and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust.
- 7.2. The information mentioned above shall include the identity of:
  - a) the settlor;
  - b) the trustee(s);
  - c) the protector (if any);
  - d) the beneficiaries or class of beneficiaries; and
  - e) any other natural person exercising effective control over the trust.
- 7.3. In their relations with the Bank, trustees shall disclose their status and provide the information referred above, to the Bank, in a timely manner where, as a trustee, the trustee forms a business relationship relevant for the legal arrangements in place with the Bank.
- 7.4. Where EBID is unable to identify one or the other beneficial owners it shall desist from establishing any relationship and report the situation to the FIU concerned.

## **8. PROCEDURE N° 8: Identification of other business relationships and other information requirements**

- 8.1. The same amount of due diligence shall be applicable to all other EBID business relationships.
- 8.2. The identification data of borrowers and other business relationships including their address

shall be kept in special files within a centralized information system.

- 8.3. The various departments and divisions shall enter and update the data for their respective activities.
- 8.4. The data shall be accessed through an enabling system managed by the Department responsible for Information Technology under the supervision of the Department responsible for Risk Management and subject to periodic internal audit.
- 8.5. The files holding data on borrowers and other business relationships must be updated continuously.
- 8.6. Any information collected in respect of developments in the political life of borrowers and data collected on the borrowers should be entered in the business relations file: change in Management, representatives, attainment of Politically Exposed Persons' status, address, etc.
- 8.7. Data collected and KYC dossiers shall be updated during the periodic review of portfolios.

**9. PROCEDURE N° 9: Enhanced due diligence with regards to identifying and knowing business relationships**

- 9.1. When dealing with natural persons or legal entities established in the third countries identified as high-risk third countries, as well as in other cases of high risk that are identified by the Bank, the Bank shall apply enhanced customer due diligence measures to manage and mitigate those risk appropriately.
- 9.2. The bank shall use a risk-based approach in relation to all entities and branches or majority owned subsidiaries located in high-risk countries.
- 9.3. The Bank shall examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions and all unusual patterns of transactions, which have no apparent economic or lawful purpose and shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.
- 9.4. The following high-risk situations shall be taken into account when assessing the risk of money laundering and terrorism financing:
  - a) Customer risk factors:
    - i. the business relationship is conducted in unusual circumstances;
    - ii. customers that are resident in geographical areas of higher risk as set out in point (c);
    - iii. legal persons or arrangements that are personal asset-holding vehicles;
    - iv. companies that have nominee shareholders or shares in bearer form;
    - v. businesses that are cash-intensive;
    - vi. the ownership structure of the company appears unusual or excessively complex

given the nature of the company's business.

- b) Product, service, transaction or delivery channel risk factors:
  - i. private banking;
  - ii. products or transactions that might favor anonymity;
  - iii. non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
  - iv. payment received from unknown or unassociated third parties;
  - v. new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.
- c) Geographical risk factors:
  - i. countries identified by credible sources, such as mutual evaluations of FATF or GIABA, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
  - ii. countries identified by credible sources as having significant levels of corruption or other criminal activity;
  - iii. countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
  - iv. countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

9.5. The following shall apply specifically as enhanced measures relating to relationships with cross-border Correspondent Banks and other businesses:

- a) collect sufficient information in order to understand the type of activities, and evaluate the bank's reputation and the quality of supervision;
- b) verify if the correspondent bank has been under investigation or subjected to measures from AML/CFT regulatory authorities,
- c) evaluate the quality of control put in place,
- d) obtain authorization from the Executive Committee and the President prior to establishing new relationships with correspondent banks,
- e) ensure that the correspondent bank applies monitoring measures in conformity with FATF recommendations.

9.6. EBID shall not establish a relationship with a correspondent bank (shell bank) which does not have any material resource in its host country.

9.7. EBID shall ensure that its correspondent banks do not deal with fictitious banks.

9.8. Bank staff should be required to ask prospective correspondent banks to respond to a

questionnaire on the anti-money laundering measures it has taken.

- 9.9. Annex I to these procedures contains AML/CFT questionnaire for correspondent banks and other businesses.

**10. PROCEDURE N° 10: Enhanced due diligence in relation to Politically Exposed Persons and Non-profit Organizations**

- 10.1. A politically exposed person means a natural person who is or who has been entrusted with prominent public functions and includes (no public function below shall be understood as covering middle-ranking or more junior officials):
- a) Heads of State, heads of government, ministers and deputy or assistant ministers;
  - b) Members of Parliament or of similar legislative bodies;
  - c) Members of governing bodies of political parties;
  - d) Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
  - e) Members of courts of auditors or of the boards of central banks;
  - f) Ambassadors, *chargé d'affaires* and high-ranking officers in the armed forces;
  - g) Members of the administrative, management or supervisory bodies of State-owned enterprises;
  - h) Directors, deputy directors and members of the board or equivalent function of an international organization.
- 10.2. The measures applied to politically exposed persons are to be applied also to family members or persons known to be close associates of politically exposed persons.
- 10.3. For the purpose of the politically exposed person definition, family includes: the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; the parents of a politically exposed person.
- 10.4. When the name of a politically exposed person appears in any transaction such as loan, guarantee, equity participation, person (s) in charge of the dossier must state this in the dossier summary file and record the observation in the Credit Appraisal Report and EBID Relationships Reference File. Prior to presenting the dossier to the Credit Committee, a special memo should be forwarded to the President or Vice-President for information and decision concerning the politically exposed person, regardless of the outcome of the

dossier itself.

- 10.5. The following are methods to determining the Status of a Politically Exposed Person:
- a) Common knowledge facts in EBID;
  - b) Credible sources, data base query, search engines or specialized external data bases.
- 10.6. The collection of information relating to Politically Exposed Persons, include, but is not limited to:
- a) activities;
  - b) income;
  - c) asset and origin.
- 10.7. The Bank staff shall apply the following measures in case of business relationship with politically exposed persons:
- a) Obtain senior management approval for establishing or continuing business relationships with such persons;
  - b) Take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transaction with such persons;
  - c) Conduct enhanced, ongoing monitoring of those business relationships.
- 10.8. When a politically exposed person is no longer entrusted with a prominent public function relevant to the operations of EBID (in a member State or an international or regional organization) the Bank's staff shall ensure that for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.
- 10.9. Enhanced due diligence measures shall be also applied during the identification of the official and unofficial officers of the non-profit organizations through the rules defined for beneficial owners' identification and enhanced due diligence set out in these procedures.

## **11. PROCEDURE N° 11 : Enhanced due diligence over country risks**

- 11.1. The Bank shall identify high-risk countries and jurisdictions and duly evaluate if there are strategic deficiencies that might endanger its operations.
- 11.2. More specifically, the Bank shall be in a position to identify if the legal and institutional framework of the countries with which it does business, contains:
- a) Criminalization of money laundering and terrorism financing;
  - b) Measures relating to customer due diligence;

- c) Requirements relating to record keeping; and
  - d) Requirements to report suspicious transactions.
- 11.3. For the identification of the high-risk third countries the Bank shall follow the information produced by FATF, which publishes the results of assessments by FATF and those conducted by other institutions (World Bank, IMF, GIABA) about country compliance with FATF Recommendations, in two documents namely:
- a) FATF public statement on jurisdictions with strategic anti-money laundering and combatting the financing of terrorism (AML/CFT) deficiencies,
  - b) A list of countries with strategic (AML/CFT) deficiencies for which they have developed a plan of action with FATF.
- 11.4. The FATF list of countries with anti-money laundering deficiencies on the FATF web site: [www.fatf-gafi.org](http://www.fatf-gafi.org) shall be taken in consideration for the purpose of this procedure.
- 11.5. The OECD grey list is available on the OECD web site: [www.oecd.org](http://www.oecd.org) shall be taken in consideration for the purpose of this procedure.
- 11.6. Analysis of money laundering risks must take into consideration the links that business relationships can have with any of the countries identified by the FATF as posing a risk to the international financial system.
- 11.7. The Bank shall also evaluate if the jurisdictions of the projects have authorities that are competent and equipped with enough powers and procedures to effectively combating money laundering and terrorism financing as well as the effectiveness of the AML/CFT system in addressing money laundering and terrorism financing risks.
- 11.8. Prohibitions for projects involving jurisdictions identified as high-risk countries shall be applied by EBID.

## **12. PROCEDURE N° 12: Due diligence with regard to the means of payment and new technologies**

- 12.1. The Bank shall exercise constant due diligence especially, with regard to transactions made on the means for settling loan disbursements, maturities and financial products.
- 12.2. Constant due diligence should also be extended to all EBID treasury transactions.
- 12.3. The following shall apply in relation to cash transactions:
- a) In principle, cash transactions shall be prohibited in the procedures of the Bank including payments and receipts with the exception of minor expenses made in respect of general services;
  - b) Where a cash payment has been received in respect of a commercial transaction by way of exception, the transaction shall be examined thoroughly, and the report forwarded to the person responsible for AML/CFT compliance for recording in the confidential register.
- 12.4. The following shall apply with regard to transactions by cheque:

- a) Thorough examination of the issuer, beneficiary and bank or non-bank endorser;
  - b) An uncrossed cheque with several non-bank endorsers must be subjected to special scrutiny to justify the intervention of several beneficiaries. A crossed bearing more than one non-bank endorsement is an irregular cheque.
  - c) Cheques issued or originating from countries classified under risk of money laundering or terrorism financing, should be subjected to close scrutiny.
  - d) Cashed bank cheques present a high risk of money laundering as the name of the payer and debited account are not indicated in the payment document.
- 12.5. The following shall apply with regard to transfer of funds:
- a) All wire transfers made shall bear the name of the issuer, the name and address of the beneficiary;
  - b) EBID shall ensure that wire transfers received contain the same information;
  - c) The Loan Administration Division and Treasury shall point out wire transfers that do not include the name and address of the issuer or where they are not written in full;
  - d) Missing information shall be demanded from the originator's bank;
  - e) Anomalies observed should be submitted to the person responsible for AML/CFT compliance to record the outcome of close scrutiny.
- 12.6. New business practices (long distance business relationships, request for third parties), new products, involve additional risks that have to be controlled through enhanced due diligence.

### **13. PRODEDURE N° 13 : Closer examination of certain transactions to be recorded in the confidential register**

- 13.1. Any important and complex transaction that does not seem to have an economic justification must be subjected to close scrutiny and the results recorded in the "Confidential Register" kept by the AML/CFT supervisor, in digital format together with scanned copies of documents attached.
- 13.2. Where the outcome of the close examination nullifies any doubt and suspicion over the transaction, only the elements collected shall be recorded in the register.
- 13.3. Notwithstanding the above, where there continues to be doubts or suspicion, the transaction shall be reported to the FIU concerned.
- 13.4. Information to be recorded in the confidential Register shall be as follows:
- a) the origin and the destination of the funds,
  - b) context and purpose of the transaction,
  - c) identity of the persons benefiting from the transaction.

### **14. PROCEDURE N° 14: Reporting suspicious transactions**

- 14.1. In regard to reporting suspicious transactions, the Bank compliance function shall:
- a) Inform the concerned FIU, including by filing a report, on its own initiative, where the Bank knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist

- financing, and by promptly responding to requests by the FIU for additional information in such cases; and
- b) provide the concerned FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.
- 14.2. More specifically, the following transactions shall be reported to the concerned FIU:
- a) sums of money in the books and all other goods which could have resulted from an infringement (crime or offence);
  - b) assets-related transactions where the assets may have resulted from money laundering;
  - c) amounts of money or any other assets suspected to be earmarked for the financing of terrorism;
  - d) sums of money or any other assets suspected to be earmarked for the financing of weapons of mass destruction;
  - e) any transaction in which doubts remain over the originator or beneficiaries regardless of the due diligence implemented;
  - f) any transaction made with trust funds or any other instrument for the management of special-purpose assets (trusts, affiliated trusts, foundations, Anstalt, others) that the identity of the settlors and beneficiaries are not known.
- 14.3. The Bank shall put special attention to the source of funds:
- a) injections of capital (self-financing) in loan transactions;
  - b) destination funds disbursed under loan disbursements;
  - c) destination of funds disbursed under equity participation;
  - d) source of funds collected under loan reimbursements agreements.
- 14.4. All suspicious transactions, including attempted transactions, shall be reported.
- 14.5. As soon as there is doubt over identity, or suspicion of money laundering, the staff member shall prepare an alert form for the attention of the person in charge of AML/CFT compliance.
- 14.6. The information shall remain strictly confidential and shall not be divulged to anyone within or outside the Bank, who is not expected to have knowledge of the transaction concerned.
- 14.7. The reporting to the person in charge of compliance shall be done through submission of the Alert Form approved in Annex II of these procedures.
- 14.8. The compliance function shall transmit the information referred to in this procedure to the concerned FIU.
- 14.9. Where there is suspicion of money laundering and financing of terrorism, the report shall be forwarded to the FIU of the State where the primary offence is supposed to have been committed. Where asset freezing shall be the sanction to be applied, the matter shall be referred to the FIU of the country of resident of the natural person (s) or corporate body or bodies concerned.
- 14.10. The reports may come under four categories namely:
- a) reports relating to the identification of borrowers, promoters and other business relations, where it was not possible to identify the beneficial owners (natural person stakeholders) or real beneficiaries,

- b) reports of suspected money laundering, financing of terrorism and the proliferation of weapons of mass destruction,
- c) additional reports forwarded spontaneously to the FIU concerned to confirm or invalidate an already reported suspicion,
- d) responses to requests for information made by an FIU in respect of a transaction involving EBID;
- e) Other as may be determined by the person in charge of compliance in accordance with the AML/CFT Charter of Compliance.

14.11. The following shall apply in terms of timing and format for the preparation of the reports:

- a) Reports shall be prepared as soon as there is suspicion regarding a transaction even when it is in respect of an already completed transaction;
- b) Where the transaction has not yet been completed, the person in charge of AML/CFT compliance shall indicate the expected deadline for the completion of the transaction to the FIU;
- c) The report may be prepared through whatever means. Verbal reports shall be confirmed in writing not later than 48 hours.
- d) It is prohibited to inform owners of amounts that gave rise to suspicion about the existence of the report.

14.12. The following shall be applied to follow to reports:

- a) The FIU shall acknowledge receipt of reports. The FIU may ask for additional information.
- b) Where the transaction has not yet been completed, the FIU may object to it exceptionally, for 48 hours beyond which the objection must be confirmed by a judge. Where the facts are liable to constitute an offense, the FIU shall forward the dossier to the Attorney-General without including the report of suspicion that gave rise to the dossier. The declarant shall be informed at the appropriate time.

## **15. PROCEDURE N° 15 : Combating the financing of terrorism and the proliferation of weapons of mass destruction and implementing the international financial sanctions**

15.1. The following shall be applied by the Bank in relation to asset freezing:

- a) The person in charge of AML/CFT compliance shall obtain updated lists of entities (natural persons and corporate bodies) targeted by asset-freezing measures, and forward the lists to staff concerned in all departments of EBID;

- b) Prior to establishing any kind of business relationship, persons in charge of the relationship (analysts and others concerned) shall verify that the names of EBID business relationships, clients, borrowers, promoters, banks and other financial institutions including any of EBID's natural person or corporate business relationships are not on the sanctions list;
- c) Regarding corporate entities, the names of managers, executive directors and any other representatives should not be on the sanctions list;
- d) The due diligence required for politically exposed persons shall be extended to their associates;
- e) The lists of sanctions decided by the United Nations Security Council, lists from ECOWAS Member States and where necessary, lists from UEMOA;
- f) Other lists to be consulted include lists from OFAC (USA), lists from the European Union, United Kingdom (UK) and France;
- g) The analyst or any other person in charge of a business relationship who notices that the name of a natural person or corporate business relationship is on any of the above-mentioned list shall inform his supervisor promptly and forward a filled-out alert form to the person in charge of AML/CFT compliance.
- h) After analysing the situation, the person in charge of AML/CFT compliance shall inform the FIU concerned and wait to receive a response from them before taking another action.

15.2. The following shall be considered by the Bank in relation to embargos:

- a) An embargo is an administrative or military sanction prohibiting the free movement of goods or articles.
- b) Embargoes are imposed either by the UN Security Council, a State or a group of States.
- c) Ignorance of embargoes and non-compliance is an operational risk that could lead to counterpart risk.
- d) Embargoes are applicable to all economic operators including companies and not only banks and financial institutions. Economic embargoes may be imposed for political reasons. They are often imposed against the supply of arms to belligerent countries.
- e) Embargoes may be imposed on countries that do not comply with the Treaty on the Non-Proliferation of Weapons of Mass destruction. Therefore, financial flows corresponding to payment or withdrawal of funds for goods under embargo shall be prohibited on the same basis as the transportation of the goods.
- f) The person in charge of AML/CFT compliance shall update a list of countries under embargo and make it available to all staff concerned.
- g) Whenever a citizen or a transaction from one of these countries is involved in activities, the person who is in charge of treating operations shall inform his superior and the person in charge of AML/CFT compliance.

## **16. PROCEDURE 16 : Training and awareness**

- 16.1. The person in charge of AML/CFT compliance in collaboration with the department responsible for Human Resources shall prepare an AML/CFT training plan and ensure that staff concerned receive training and awareness raising measures.
- 16.2. The training shall focus on procedures and shall highlight transactions that should be subjected to greater scrutiny as a result of the risks identified through the classification of risks mapping.
- 16.3. Each Head of Department shall appoint an AML/CFT correspondent who shall receive extensive training relating to anti-money laundering obligations, the modalities for detecting suspicious operations including the use of alert forms, in order to offer appropriate contributions to activities of the Department.
- 16.4. Training and awareness raising sessions must be organized in accordance with the training plan, but in any case, at least once a year for staff concerned.
- 16.5. Staff attendance of AML/CFT trainings events shall be compulsory.
- 16.6. Training programmes shall be duly documented.
- 16.7. The AML/CFT training should be given to newly hired staff as soon as they are hired and on an ongoing risk-sensitive basis to existing staff.
- 16.8. The awareness raising initiative shall be extended to all staff, including the members of the Board as well as any temporary or seconded employees.

## **17. PROCEDURE N° 17 : Data protection and Archiving of documents**

- 17.1. To the extent that it is strictly necessary for the purposes of preventing money laundering and terrorist financing, the Bank may process special categories of personal data and personal data relating to criminal convictions and offences subject to the safeguards provided below.
- 17.2. For the purpose of this procedure, personal data shall be processed by the Bank on the basis of the applicable framework only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes.
- 17.3. The Protection of Personal Data technical and organizational measures at EBID shall be in accordance with the policies and procedures approved for that purpose.
- 17.4. The Bank shall retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:
  - a) a copy of the documents and information obtained in the performance of customer due diligence, including information obtained through electronic identification means, and

- the results of the analyses undertaken for the purpose of reporting suspicious transactions;
- b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions.
- 17.5. By way of derogation from the defined above, the Bank may decide to replace the retention of copies of the information by a retention of the references to such information, provided that the nature and method of retention of such information ensure that the Bank can provide immediately to competent authorities the information and that the information cannot be modified or altered.
- 17.6. The Bank making use of the derogation referred to, above in this procedure, shall define the categories of information for which it will retain a reference instead of a copy or original, as well as the procedures for retrieving the information so that it can be provided to competent authorities upon request.
- 17.7. All the documents relating to anti-money laundering and countering the financing of terrorism shall be preserved for 5 years.
- 17.8. The archiving of data in both paper form and digital form must comply with safety and confidentiality rules in force at EBID.
- 17.9. The count down to the five -year deadline shall commence when the business relationship is closed.
- 17.10. The documents concerned also include background information and documents relating to operations or transactions for which the count down to the 5-year deadline shall commence at the end of the year in which the operations or transactions were made.

## **18. PROCEDURE N° 18 : Professional secrecy – Prohibition of disclosure**

- 18.1. Professional secrecy shall be basic rule. All information relating to anti-money laundering shall be strictly confidential.
- 18.2. The Bank shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with the suspicious transactions reporting procedures or that a money laundering or terrorist financing analysis is being, or may be, carried out.
- 18.3. The above shall not apply to disclosures to competent authorities and to self- regulatory bodies where they perform supervisory functions, or to disclosure for the purposes of investigating and prosecuting money laundering, terrorist financing and other criminal activity.
- 18.4. By way of derogation to the above, disclosure may take place within any Bank office or branch, established in third countries, provided that those branches or offices fully comply with the Bank's policies and procedures, including procedures for sharing information

within Bank.

- 18.5. By way of derogation from the above, in certain circumstances, disclosure may take place between the Bank and entities from third countries which impose requirements equivalent to those imposed by the Bank.
- 18.6. By way of derogation from the above, disclosure may take place between the Bank and other entities which imposes requirements equivalent to those approved by the Bank, and that they are from the same category of business and are subject to professional secrecy and personal data protection requirements.
- 18.7. Professional secrecy may not be invoked as a justification for withholding information from certain entities or authorities, especially a Judge, within the framework of an investigation relating to money laundering, the financing of terrorism or proliferation of weapons of mass destruction.

## **19. PROCEDURE N° 19 : Responsibility of Executives and Staff – Legal Protection**

- 19.1. Due diligence and reporting obligations are incumbent on EBID, the Executives and staff members.
- 19.2. The following shall be applied in relation to exemption to liability for reports of suspicion forwarded in good faith:
  - a) There shall be total exemption to liability for reports forwarded in good faith;
  - b) There shall be an exemption from responsibilities in the case of suspicion report written in good faith that is, without malicious intent;
  - c) No vicarious or criminal liability action whatsoever or disciplinary action from the office shall be levelled against staff members even where no conviction resulted from the suspicious transactions reported;
  - d) The States concerned shall be liable for any possible damages to persons as a result of reporting a suspicion in good faith.
- 19.3. The following shall be applied in relation to exemption to liability from making some transactions:
  - a) Where a suspicious transaction has been made and there has been no fraudulent collusion with the perpetrators of underlying primary offenses, no criminal proceedings whatsoever shall be instituted against the EBID's person in charge of compliance, the Executives or staff of the institution, provided the suspicious transaction was reported in good faith.

## **20. PROCEDURE N° 20 : AML/CFT monitoring and internal reporting**

- 20.1. The person in charge of AML/CFT compliance should have the responsibility for ongoing monitoring of the implementation of the measures, policies, controls and procedures adopted to ensure the Bank's compliance with its AML/CFT obligations.
- 20.2. The person in charge of AML/CFT compliance shall report to and advise the Board on measures to be taken to ensure compliance with applicable standards and international legislation, and should provide an assessment of the possible impact of any changes in the international standards and legislation on the Banks's activities and compliance framework.
- 20.3. The AML/CFT reporting shall take place, at least on annual basis.
- 20.4. Notwithstanding other reporting obligations deriving from the AML/CFT Charter of Compliance, the person in charge of AML/CFT compliance shall prepare a monitoring chart comprising the main indicators proving the actual operation of the mechanism and containing at least information on:
  - a) Money laundering and terrorism financing risk assessment;
  - b) Resources regarding AML/CFT;
  - c) Policies and procedures.
- 20.5. The detailed procedures and the identification of the elements to be reported in relation to the three main groups of information required under the previous paragraph shall be set out in the AML/CFT Charter of Compliance.
- 20.6. The EBID' department responsible for Internal Audit shall include the audit of the AML/CFT mechanism in its audit mission schedule:
  - a) it shall ensure that there is a bona fide person in charge of AML/CFT in EBID to report suspicious transactions.
  - b) verify the relevance of procedures and their updating.
  - c) ensure that staff receive training on a regular basis and that the sessions can be tracked;
  - d) Control the use of alert forms that track doubts or suspicion regarding the identity of business relationships, implemented and envisaged transactions, by all staff concerned.
  - e) evaluate the relevance of analyses that are the bases for recording alerts in the confidential register or reporting suspected money laundering to FIUs.
  - f) verify that documents relating to AML/CFT are put in the archive in conformity with the procedure in force.
  - g) Make recommendations that it shall consider appropriate for rectifying any deficiencies that may have been observed or that may be capable of improving the operations of the mechanism.

20.7. The relation between the Compliance function and other EBID departments for the purpose of AML/CFT shall be set out in the Charter of Compliance.

## **ANNEX**

**ANNEX 1: AML/CFT Bank Questionnaire for Correspondent Banks**

**ANNEX 2: Alert Form for the Supervisor of the AML/CFT Mechanism**

**ANNEX 3: Monitoring Chart for Anti-Money Laundering Activities**

**ANNEX 4: Questionnaire non-bank AML/CFT and KYC**