



Policies and Procedures for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Countering the Proliferation of Weapons of Mass Destruction (CPWMD).

BIR Bank, S.A



BIR Bank

Policies and Procedures for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Countering the Proliferation of Weapons of Mass Destruction (CPWMD).

Document Details

Title:	Anti-Money Laundering and Counter-Terrorist Financing Policies and Procedures
File:	DCOM.002.2015_Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation of Weapons of Mass Destruction Policies and Procedures

Document Revision

Date:	Version	Responsible	Reason for intervention
12-2022	V4	DCOMP	Update
12-2022	V4	DORG	Formatting
** -2022	V4	IC	Validation

Approved by:

Date:	Version	Name	Signature
_-2022	V4	Management Board	



BIR Bank

Policies and Procedures for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Countering the Proliferation of Weapons of Mass Destruction (CPWMD).

Sub-Process Updates:

Version	Date of entry into force	Adjustments
V1	01-12-2015	Establishment (CA.OS.MP.006.2015)
V2	09-09-2019	Update (CA.OS.007.2019)
V3	08-12-2020	Update (CA.OS.007.2020)
V4	15-05-2023	Update (CA.OS.005.2023)

Legislation/Regulation to support the Sub-Process:

Diploma	Date of entry into force	Subject
Law No 5/2020	June 27	Anti-Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction Act.
Notice No 14/2020	June 22	Rules to Prevent and Combat Money Laundering, Terrorist Financing.
Regulation No 5/2021	November 8	Prevention of and Fight against Money Laundering, Terrorist Financing.
Law No 1/2012	January 12	Designation and Implementation of International Legal Acts.
Presidential Decree No 2/18 of 11 January	January 11	It establishes the organization and functioning of the Financial Intelligence Unit (FIU), providing the obligation for financial institutions to report transactions of a certain type of transaction.
Presidential Decree No 214/13	December 13	Regulation of the Law on the Designation and Execution of International Legal Acts.
Law No 5/20 of 27 January	January 27	Law on the Prevention and Combating of Money Laundering, Financing of Terrorism, and Proliferation of Weapons of Mass Destruction, which establishes preventive and punitive measures for the prevention of Money Laundering/Financing of Terrorism. It also establishes the applicable sanctioning regime in case of non-compliance.
Law No 38/20	November 11	Law approving the Angolan Criminal Code
Law No 19/17	August 25	Law on Prevention and Combating Terrorism, establishes preventive, repressive, investigative, and special procedural measures, support, and protection for victims of terrorism, the occurrence of the phenomenon of terrorism, acts committed on Angolan territory by national or foreign citizens, as well as acts committed abroad.
Instruction No 09/CMC/12-21	December 20	Designated Persons Identification Declaration Form
Instruction No 10/CMC/12-21,	December 20	Suspicious Operation Declaration Form



BIR Bank

Policies and Procedures for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Countering the Proliferation of Weapons of Mass Destruction (CPWMD).

Instruction No 13/CMC/12-21,	December 20	Freezing of Funds and Economic Resources
FATF Recommendations - Financial Action Task Force	2022	Version 2022
Instruction No 20/2020	December 09	Definition of the model for the Anti-Money Laundering and Counter-Terrorist Financing Prevention Report, as well as the implementation of risk validation
Instruction No. 13/2018	September 19	Definition of the criteria for Anti-Money Laundering and Counter-Terrorist Financing Prevention in International Trade Operations.

Abbreviations:

UN - United Nations

OFAC - U.S. Foreign Assets Control Agency

EU - European Union

BIR - Rural Investment Bank

FIU - Financial Intelligence Unit

INDEX

CHAPTER I - SCOPE OF APPLICATION AND OBJECTIVES....	Error! Bookmark not defined.
1.1. Scope.....	Error! Bookmark not defined.
1.2. Objectives.....	Error! Bookmark not defined.
CHAPTER II - FRAMEWORK.....	Error! Bookmark not defined.
2.1. Applicable Legislation and Regulation.....	Error! Bookmark not defined.
2.2. Concept of Money Laundering and Terrorist Financing.....	Error! Bookmark not defined.
CHAPTER III - ML/TF RISK PREVENTION PROGRAM.....	Error! Bookmark not defined.
3.1. AML/TF Risk Management System.....	Error! Bookmark not defined.
CHAPTER IV - GENERAL AML/TF PREVENTION POLICIES....	Error! Bookmark not defined.
4.1. AML/TF Risk Management Policy	Error! Bookmark not defined.
4.2. Customer Acceptance Policy	Error! Bookmark not defined.
4.2.1. Prohibited Customers	Error! Bookmark not defined.
4.3. Acceptance of Customers Subject to Prior Authorization	Error! Bookmark not defined.
4.4. Governance Model	Error! Bookmark not defined.
4.5. Management Information	Error! Bookmark not defined.
CHAPTER V - AML/TF PREVENTION PRINCIPLES AND PROCEDURES.....	Error! Bookmark not defined.
5.1. Duty of Identification	Error! Bookmark not defined.
5.2. Duty of Diligence	Error! Bookmark not defined.
5.3. Adaptation to the risk level.....	Error! Bookmark not defined.
5.4. Enhanced Due Diligence	Error! Bookmark not defined.
5.5. Continuous Monitoring Obligation	Error! Bookmark not defined.
5.6. Obligation to Refuse	Error! Bookmark not defined.
5.7. Obligation to Abstain.....	Error! Bookmark not defined.
5.8. Examination Duty.....	Error! Bookmark not defined.
5.9. Obligation to report operations to competent authorities	Error! Bookmark not defined.
5.10. Internal procedure for reporting suspicious transactions	Error! Bookmark not defined.
5.11. Notification of Designated Persons and Entities	Error! Bookmark not defined.
5.12. Reporting of Cash Transactions.....	Error! Bookmark not defined.
5.13. Duty to Retain Documents	Error! Bookmark not defined.
5.14. Duty of Cooperation.....	Error! Bookmark not defined.
5.15. Duty of Secrecy	Error! Bookmark not defined.
5.16. Duty of Control.....	Error! Bookmark not defined.
5.17. Training Obligation.....	Error! Bookmark not defined.
CHAPTER VI - IDENTIFICATION / DETECTION OF OPERATIONS AND MONITORING	Error! Bookmark not defined.

- 6.1. Identification and Detection of Suspicious Operations and Monitoring **Error! Bookmark not defined.**
- 6.2. Identification and Detection of Suspicious Operations by the *Compliance* Directorate
Error! Bookmark not defined.
- 6.3. Identification and Detection of suspicious operations by the Commercial Structure
(*front-office*) and other Business Units..... **Error! Bookmark not defined.**
- 6.4. Monitoring of Entities (high risk, PEPs, entities referenced by competent authorities)
Error! Bookmark not defined.
- 6.5. Investigation of Operations by the *Compliance* Directorate.....**Error! Bookmark not defined.**

CHAPTER VII - CONTROL OF ENTITIES SUBJECT TO FINANCIAL COUNTERMEASURES **Error! Bookmark not defined.**

- 7.1. Filtering Entities and Transactions **Error! Bookmark not defined.**
- 7.2. Filtering Entities **Error! Bookmark not defined.**
- 7.3. Transaction Filtering and Blocking **Error! Bookmark not defined.**
- 7.4. Freezing of Funds and Economic Resources **Error! Bookmark not defined.**

CHAPTER VIII - ANNEXES **Error! Bookmark not defined.**

ANNEX I - "Incidence Report" *Template*..... **Error! Bookmark not defined.**

ANNEX II -Typology of Suspicious Operations **Error! Bookmark not defined.**

ANNEX III - List on the set of categories of crimes underlying the crime of money laundering
(listed in the glossary of the 40 FATF Recommendations complemented by Law No. 38/20 of
November 11th, Law that approves the Angolan Criminal Code).**Error! Bookmark not defined.**

CHAPTER I - SCOPE OF APPLICATION AND OBJECTIVES

1.1. Scope

The "Manual of Policies and Procedures for the Prevention and Combating of Money Laundering, Financing of Terrorism, and Proliferation of Weapons of Mass Destruction" (hereinafter referred to as the "Manual") applies to all business units of Banco de Investimento Rural, S.A. (hereinafter referred to as "BIR" or "BIR Bank").

The rules set forth in this Manual, adopted by BIR Bank, correspond to the implementation of international principles and guidelines on the Prevention of Money Laundering and Combating the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (ML/CFT-P), as well as current legal requirements, regulatory demands established by the National Bank of Angola (hereinafter referred to as "BNA"), and guidelines from the Financial Information Unit of Angola (hereinafter referred to as "UIF").

1.2. Objectives

This Manual defines the internal policies and procedures of BIR on Prevention and Combat of ML/TF-P, having as its main objectives:

- ensure the implementation of an efficient system for preventing and combating the crime of money laundering and terrorist financing, and the proliferation of weapons of mass destruction, with a risk-based approach;
- ensure that the BIR Bank knows its customers ("*Know Your Customer*"), its business and its transactions ("*Know Your Transactions*"-"*Know Your Transactions/Payments*");
- Establish adequate internal policies and procedures for the fulfillment of the legal and regulatory obligations to which the Bank is subject;
- to raise awareness of and hold accountable the Bank's staff of compliance with the rules on preventing and combating money laundering and terrorist financing in the event of non-compliance with those rules;
- ensure that operations and transactions relating to international trade comply with enhanced due diligence procedures as they represent a high risk of money laundering, terrorist financing and underlying offenses;

- establish appropriate controls to mitigate the identified risks;
- Establish mechanisms to ensure the effective detection of suspicious transactions and their reporting to competent authorities, including the Financial Intelligence Unit.

The *Compliance Directorate (DCOMP)* is responsible for this Handbook and is subject to formal approval by the BIR Board of Directors (BD).

Adjustments/updates to this Manual must be approved by the Management Board on a proposal from the *Directorate of Compliance (DCOMP)* and with the knowledge of the Directorate for Internal Audit (DIA) and the Directorate for Organization (DORG).

CHAPTER II - FRAMEWORK

2.1. Definitions

"Customers" are individuals and/or legal entities that enter into a contract with the Bank, or express or indicating an intention to do so, including, in particular, advisers, counterparties, suppliers or other service providers;

"*Know Your Customer*" translates into your customer's knowledge.

'Politically Exposed Persons' are nationals or foreigners who perform or have performed prominent public functions in Angola, or in any international organization;

'*Shell Bank*' is a bank that is incorporated and authorized to operate in a jurisdiction but has no physical presence in that jurisdiction and is not affiliated to a regulated financial group and is subject to effective supervision;

"False Positive" Occurs when there is no name match during the entity/customer screening process;

"Hit" is the possible match of name during the screening process against sanctions lists that indicates a sanctioned person(s).

"Enhanced Due Diligence" A set of enhanced due diligence measures performed whenever an increased risk of ML/CTF/P is identified as part of the calculation of the customer risk score.

"**Terrorist financing**" is the provision, deposit, distribution or collection of funds, by any means, directly or indirectly, with the intention of using them or with the knowledge that they will be used, wholly or in part, in the planning or execution of any terrorist offense.

"Proliferation of Weapons of Mass Destruction" is the process by which an agent provides, collects or holds funds or goods of any kind or nature, whether of lawful or illicit origin, as well as goods or rights that could be transformed into funds for the proliferation of weapons

capable of causing a high death toll in a single use, whether of nuclear, chemical or biological weapons, and related materials.

"Money laundering" is participation in any activity with the purpose to acquire, hold, use, convert, transfer, conceal or disguise the nature, origin, location, disposition, movement or beneficial ownership of property or rights in property, knowing that such property is derived from an infringing activity or from an act of participation in an infringing activity.

The process of money laundering consists of three (3) stages:

1. **Placement** - refers to the process of introducing cash derived from illicit activities into financial or non-financial institutions.
2. **Layering/Circulation** - signifies the separation of proceeds from illegal activities through the use of complex financial or non-financial transactions. These transactions aim to hinder their detection, obscure the origin of funds, and facilitate anonymity.
3. **Integration** - denotes the reintegration of laundered proceeds into the legitimate economy, either in the same sector from which they originated or in a different sector, giving them the appearance of legitimacy.

Financial Institutions may be used at any stage of the Money Laundering or Terrorist Financing process.

CHAPTER III - AML/CTF-P RISK PREVENTION PROGRAM

3.1. AML/CTF-P Risk Management System

The AML/CTF/P Risk Management System is the proper identification, assessment, and mitigation of money laundering and terrorist financing risks to which BIR is exposed in the course of its activities, enabling efficient monitoring of its customers and transactions, as well as effective prevention and detection of potentially suspicious operations.

The BIR AML/CTF/P Risk Management System encompasses the following aspects:

- Risk Assessment Model (*Scoring* - KYC);
- Customer and Transaction Filtering Systems;
- internal AML/CTF/P Risk Management policies;
- *Governance* Model;
- Internal Processes and Procedures;
- Established Risk Mitigation Controls;
- Management Information;
- Awareness and Training Plan.

The BIR Bank formally appoints a Chief *Compliance Officer*, responsible for ensuring compliance with obligations regarding the prevention of money laundering and counter-terrorist financing and the proliferation of weapons of mass destruction. This officer is officially called the "*Compliance Officer*".

The responsibilities of the *Compliance Officer* are as follows:

- Coordinate and monitor the effective implementation of policies, procedures, and adequate controls for the efficient management of risks related to money laundering, terrorist financing, and the proliferation of weapons of mass destruction to which the financial institution is or may be exposed;
- Participate in defining and provide prior opinion on policies, procedures, and controls aimed at preventing money laundering, terrorist financing, and the proliferation of weapons of mass destruction;
- continuously monitor the adequacy, sufficiency and timeliness of policies and procedures and controls on the prevention of money laundering, the terrorist financing and the proliferation of weapons of mass destruction and propose the necessary updates to the Management Board and the Directorate for Internal Audit and Control Committee;
- participate in the defining, monitoring and evaluating of the internal training policy of the financial institution's;
- ensure the centralization of all relevant information from the various business areas of the Financial Institution;
- Communicate, without internal or external interference, the operations mentioned in Article 17 of Law No 05/20 of January 27th to the Financial Intelligence Unit;
- Act as the point of contact for law enforcement, supervision, and oversight authorities, including compliance with the reporting obligation set forth in Article 17

of Law No. 05/20 of January 27th, ensuring compliance with other communication and collaboration obligations;

- Support the preparation and execution of risk assessments related to Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction to which the Bank is exposed concerning individual customers and transactions, taking into account the key risk assessment factors reflected in national and international regulatory and legal best practices;
- Coordinate the preparation of reports, and other information to be sent to the National Bank of Angola regarding the prevention of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction;
- Ensure that all Bank employees, regardless of the nature of their relationship, are aware of: (i) the identity and contact details of the *Compliance Officer*; (ii) the procedures for reporting to the person, the conduct and suspicious activities or transactions they detect.

To this end, the Bank ensures that the selection of employees assigned to the *Compliance* area or function is made on the basis of high ethical standards and demanding technical requirements and that it informs the National Bank of Angola of the identity and other necessary elements of the *Compliance Officer*, as well as any changes to these details, as soon as they occur.

The Risk Management System for AML/CTF is based on a risk-based approach, allowing the Bank to identify higher-risk customers and tailor the due diligence measures and level of monitoring according to the assessed risk level. To achieve this, mechanisms have been developed to enable an adequate risk assessment based on the intrinsic characteristics of customers and their activities, as well as effective monitoring of established business relationships, enabling the effective mitigation of risk and the prevention and detection of money laundering, terrorist financing, and proliferation financing activities.

The characterization of the Bank's customer portfolio in terms of AML/CTF risk determines the application of risk-adjusted measures and controls, allowing for a better understanding and monitoring of the behaviors and transactional activity of customers that pose higher

risk, considering their specific characteristics, business segments, and subscribed products.

The classification of the Bank's customers' risk also determines the level of due diligence to be applied, the frequency of information updates and risk reassessments, as well as the need for additional measures to monitor transactional activity.

CHAPTER IV - GENERAL AML/TF PREVENTION POLICIES OF

4.1. AML/TF-P Risk Management Policy

BIR's AML/TF Risk Management Policy aims to identify the general principles that support the Bank's risk management system, identify implemented risk mitigating factors, and reflect the BIR's risk appetite based on the identified risks.

4.2. Customer Acceptance Policy

In the context of establishing business relationships, all necessary information and documentation should be collected to reasonably exclude the inclusion of customer in prohibited situations. The customer acceptance policy is mandatory with no exception and applicable to all customer segments, and must be followed by all units within the Bank's structure.

4.2.1. Prohibited Customers

Based on the risk classification of AML/TF/P, the institution cannot agree to establish business relationships with the following categories of customers:

- persons included in any of the official Sanctions Lists;
- Persons who have information that may be inferred to be related to illegal activities;
- persons who have business activities the nature of which is impossible to verify the legitimacy of the business or the merits of the funds;
- Those accounts whose owners or representatives are anonymous customers or with manifestly fictitious names;

- persons refusing to provide the information or documentation required;
- legal persons whose ownership or control structure cannot be determined;
- Casinos or betting entities not officially authorized;
- Financial entities resident in countries or territories in which they have no physical presence (so-called 'shell banks') and which do not belong to a regulated financial group.

4.3. Acceptance of Customers Subject to Prior Authorization

In accordance with the AML/TF/P Risk Management model defined by BIR Bank (AML/TF Risk Management Policy) (Chapter V, pp. 11 to 15), the following types of customers will only be admitted with the prior authorization of the *Compliance* or Management Directorate:

- Customer rated **High Risk** - prior authorization from the *Compliance* Management and/or Manager is required.
- customers classified as **PEP/ Politically Exposed Person** - prior authorization from the Administration is required.
- **Non-profit organizations** - prior authorization from the Administration is required.
- **Casinos and Gambling Houses** - prior authorization from the Administration is required.

4.4. Governance Model

The *Governance* Model comprises of:

- ▶ *Governance* structure, including the allocation of responsibilities and competencies and the definition of reporting lines, ensuring the principle of separation of duties;
- ▶ Adequacy of technical and human resources and technological support; and
- ▶ Management information to ensure the monitoring and control of the AML/TF Risk Management System.

Under the AML/TF Risk Management system, the following units of the BIR Bank structure are involved:

Structure Unit	Main areas of intervention
Board of Directors (BD)/Executive Board (EB)	<ul style="list-style-type: none"> • Definition of the AML/TF Risk Management strategy; • approval of internal policies, processes and procedures; • approval of the level of exposure in terms of AML/TF risk, depending on the results obtained by applying <i>Scoring</i> KYC to the customer portfolio of BIR Bank; • Approval of Entities classified as High Risk and PEPs, according to the defined approval hierarchy; • decision to report suspicious transactions after communication by DCOMP; • Analysis of the results obtained as a result of the evaluations carried out under the AML/TF Risk Management model; • Ensure effective implementation of the corrective actions identified; • Ensure that BIR Bank complies with the regulatory requirements laid down for the prevention of ML/TF crimes; • Ensure that DCOMP has the necessary (human and technical) resources to perform its tasks effectively.
Directorate of <i>Compliance</i> (DCOMP)	<ul style="list-style-type: none"> • Identification and assessment of existing AML/TF risks; • Continuous monitoring to identify the need for any adjustments to the AML/TF prevention program; • Revision of the AML/TF Risk Assessment Model; • updating of identified risk mitigation processes, procedures and controls; • implementation of defined internal processes and procedures; • delivering an opinion on High-Risk Entities and PEPs; • Analysis of Entity and Transaction filtering results; • Analysis/investigation of potentially suspicious transactions;

Structure Unit	Main areas of intervention
	<ul style="list-style-type: none"> continuous monitoring of customers and transactions according to the degree of risk identified and the alerts defined; reporting suspicious transactions to the Financial Intelligence Unit; Preparation of management reports on the AML/TF Risk Management model and submission to the Executive Board/Board of Directors; Participation in the definition, monitoring and evaluation of the Bank's internal training policy on AML/TF prevention; as part of the internal control system, ensure compliance by business units with defined AML/TF Prevention policies, means and procedures;
Directorate of Internal Audit (DIA)	<ul style="list-style-type: none"> an assessment of the adequacy and effectiveness of the model and of the policies, processes, procedures and controls put in place; Identification of deficiencies and proposal of corrective actions to be implemented.
Directorate Information Systems (DIS)	<ul style="list-style-type: none"> implementation of technological equipment; Providing tools to the branch network and control areas; Extraction of necessary information from the Bank's systems for the production of DCOMP reports; Continuous monitoring of IT systems; Implementation of the necessary changes to the information systems in order to comply with the functional, business and reporting requirements defined within the AML/TF Risk Management System. Ensure the operation and maintenance of <i>Scoring KYC tools</i>, developed in the framework of <i>Onboarding</i> of customers; Ensure the normal functioning of the filtering tool against Sanctions Lists, Country Lists, Politically Exposed Persons Lists (PEPs), among other external and internal Lists that are adopted by the BIR Bank;
Business Network: Counters, <i>Private</i> , Company	<ul style="list-style-type: none"> Implementation of identification and due diligence processes and procedures; collecting the necessary information and documentation in accordance with national rules and existing legal and regulatory requirements; Knowledge and monitoring of customers; Conducting the initial assessment of ML/TF risk using customer <i>onboarding</i>; Adequacy in filling out the "<i>Know Your Customer</i>"-" form; Exercise of the duty of refusal and the duty to abstain; reporting potentially suspicious transactions to DCOMP; collaborate with DCOMP whenever additional information on customers and transactions is required;

Structure Unit	Main areas of intervention
	<ul style="list-style-type: none"> Participate proactively in training activities and whenever invited to do so.

4.5. Management Information

The Directorate of *Compliance* should produce management reports for the purpose of reporting statistical information relating to the monitoring of the ML/ TF Risk Management System, as well as the analyses carried out in compliance with the duties of examination, due diligence, and communication.

Reports produced as part of the monitoring of the ML/ TF Risk Management System must be formally submitted to the *Compliance Manager (quarterly reports)*, the Executive Board (monthly and/or quarterly reports) and the Board of Directors (annual reports) for review and approval.

The internal reporting process and procedures are detailed, including the structure, frequency, and contents of the management information reports. The stakeholders involved in this process are also identified, as well as the affected IT systems.

CHAPTER V - ML/TF PREVENTION PRINCIPLES AND PROCEDURES

5.1. Identification Duty ¹

BIR Bank is subjected to the obligation of identification and should require the identification of its customers, representatives and beneficial owners in whenever:

- They establish business relationships;
- They carry out occasional transactions with an amount equal to or greater than the equivalent of 15,000.00 USD (Fifteen thousand United States dollars) in the national currency, regardless of whether the transaction is conducted through a single operation or multiple operations that appear to be related;
- There are suspicions that the transactions, irrespective of their value, are related to the crime of money laundering or terrorist financing, taking into account the nature of the transaction, its complexity, and its atypical character compared to the profile or activity of the customer;
- there are doubts as to the authenticity or conformity of customer identification information.

In fulfilling the duty of identification, it is important to comply with all the requirements set forth in Banco Nacional de Angola Notice No. 14/20, dated June 22nd, as well as the provisions in the current account opening checklist. The verification of any required elements for the account opening can only be conducted through original documents or certified copies thereof. The opening of anonymous accounts or accounts with fictitious names is expressly prohibited.

I In this regard, all business units of BIR, with greater responsibility falling on the Commercial Directorate, must ensure effective and comprehensive knowledge of their

¹ **Protection of personal data:** the processing of personal data, as well as the files, automated or otherwise, created for compliance with the provisions of the current regulation on money laundering and terrorist financing, are subject to the provisions of the Law on the protection of personal data.

customers, representatives, and ultimate beneficiaries, as well as their respective activities, by:

- Confirming and documenting the true identity of customers with whom any type of business relationship is established, as well as their representatives and ultimate beneficiaries;
- Confirming and documenting any additional information collected about the customer, representatives, and ultimate beneficiaries, in accordance with the model for assessing the risks of money laundering and terrorist financing;
- Ensuring that BIR's business units do not engage in transactions with individuals or entities whose identities cannot be confirmed, who do not provide the necessary information, or who have provided false or significantly inconsistent information that cannot be clarified;
- Demanding supporting documents for the powers of individuals authorized to carry out financial transactions on behalf of the customer, obtaining their identification, and determining their relationship with the customer;
- Establishing the true identity of the person with whom a relationship is established, an account is opened, or an important transaction is executed (i.e., the beneficial owners) when the customer acts on behalf of third parties or in cases where there are doubts about whether the customer is acting on their own behalf;
- In situations where the customer is a legal entity or an unincorporated collective investment scheme, in any case where there is knowledge or reasonable suspicion that a customer is not acting on their own behalf, the obligated entities must obtain information from the customer that makes it possible to identify the ultimate beneficial owner², based on the risk of money laundering or terrorist financing

² Under Law No 5/20 of 27 January 2011, 'beneficial owner' means a natural person or persons who:

- (1) ultimately owns or controls a share in the capital of a legal person and/or the person on whose behalf the transaction is being conducted;
- (2) exercises, as a last resort, effective control over a legal person or entity without legal personality, in those situations where ownership/control is exercised through a chain of ownership or through non-direct control;
- (3) ultimately own or directly or indirectly control the capital of the company or the voting rights of the legal person, other than a company listed on a regulated market, which is subject to disclosure requirements consistent with international standards;
- (4) they have the right to exercise or exercise significant influence or control over the company regardless of the level of participation.

5.2. Due Diligence

As part of the due diligence, and without prejudice to the fulfillment of the identification obligation, the Bank should apply enhanced due diligence measures such as requesting declarations of origin and destination of funds, up-to-date information on KYC in relation to customers and transactions that, by their nature or characteristics, may reveal an increased risk of money laundering or terrorist financing.

5.3. Adaptation to the risk level

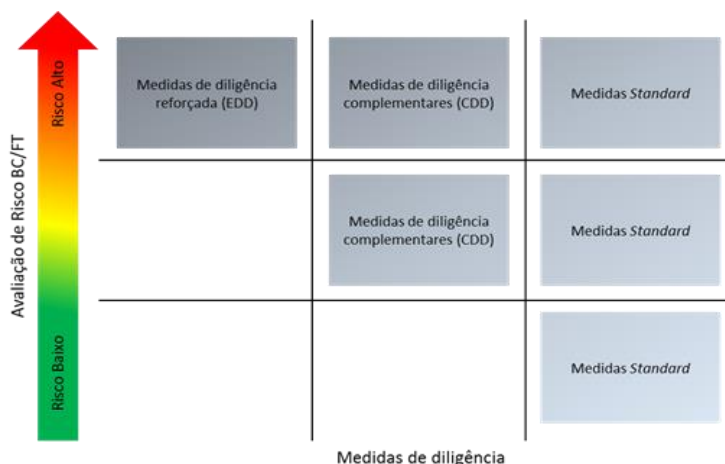
Given that each customer carries a different level of risk, the nature and extent of the due diligence measures to be applied depends on the assessment of the risk associated with each customer, the characteristics of the business relationship, the type of product or services subscribed, as well as the transactions and origin and destination of the funds (Article 9 of Law No 5/20 of January 27th and Article 4 of Notice No 14/20 of June 22nd).

Thus, depending on the outcome of the risk assessment (*Scoring* - KYC), obtained in the context of the opening of the account, or throughout the business relationship arising from the reassessment of risk, additional information on the customer, representatives or beneficial owners should be obtained and additional/enhanced due diligence measures undertaken (see Figure 1below):

Figure 1 - Due diligence measures to be applied depending on the degree of risk

ii. in the case of legal entities administering or distributing funds, the natural person or persons who:

- 1) they benefit from their assets when the future beneficiaries have already been determined;
- 2) are considered to be the category of persons in whose main interest the legal person was incorporated or operates when the future beneficiaries have not yet been determined;
- 3) exercise control over the assets of the legal person;



5.4. Enhanced Due Diligence

The internal procedures for additional and enhanced due diligence are set out in the document "**Entity and Customer Due Diligence Procedures**".

In addition to the *standard* due diligence measures, additional due diligence measures should be applied to distance transactions, and in particular to those that may favor anonymity, to politically exposed persons (PEPs) residing outside the national territory, to correspondent banking transactions with credit institutions established in third countries or to any others that are designated by the BNA.

The specific due diligence procedures concerning correspondent banking relationships are detailed in the internal legal framework "**AML/TF risk-based correspondence procedures**" and the PPE management procedure is found in the "**High Risk Customer Policy**".

5.5. Continuous Monitoring Obligation

For the purpose of continuous monitoring of the business relationship, and depending on the money laundering and terrorist financing risk assessment, the following information should be requested:

- Nature and details of the business, occupation or employment;
- Changes of address registration;
- Origin of funds to be used in the business relationship;
- Origin of initial and continuing income;
- The various relationships between signatories and their beneficial owners.

The *above* information is collected through the Customer Opening Form.

For Entities classified as Medium and High Risk, additional information is collected and recorded on the *Know Your Customer* Form (" **KYC** Form").

The commercial areas and DCOMP, as well as the other business units of the Bank, should continuously monitor the business relationships and examine the transactions carried out, verifying their compliance with the previously obtained information and the Entities' risk profile.

In the defined risk assessment model, procedures for periodically checking the timeliness and accuracy of Entity information against materiality and risk criteria are established. The specifications for ongoing customer monitoring are detailed in the internal "**Continuous Customer Monitoring**" regulation.

5.6. Obligation to refuse

BIR employees must refuse to conduct transactions where the customer fails to provide their identification, or of the representative or the beneficial owner, as well as in circumstances where information is not provided on the customer's control structure, the nature and purpose of the business relationship and the origin and destination of the funds.

In such situations where, due to customer fault, it is not possible to proceed with the identification, verification of identity, simplified due diligence, and/or enhanced due diligence procedures, the Bank acts in accordance with Article 15 of Law No. 05/20, dated January 27th, and decides to terminate the business relationship as follows:

- a) Restrict any movement of funds or other goods associated with the business relationship, including through any means of distance communication;

- b) Contacts the customer within a maximum period of 30 (thirty) days, requesting them to indicate the account to which the funds should be returned or to appear in person at the Bank for the restitution process defined by the Financial Institution.
- c) Hold the funds or other assets, keeping them unavailable until their restitution becomes possible.

If the customer, during the contact with the Bank, provides the missing elements that led to the decision to terminate the business relationship, and there are no suspicions, a reassessment of the request is carried out, performing all legally required identification and due diligence procedures.

5.7. Obligation to abstain

The duty to refrain consists in prohibiting the carrying out of any transaction relating to a particular customer where it is established that a particular transaction gives grounds for suspecting that it is connected with the commission of ML/TF-P offenses.

If BIR Bank employees suspect that a transaction may be related to the commission of ML/TF-P crimes, they must refrain from carrying out the transaction and immediately inform the *Compliance* Directorate. The Directorate of *Compliance* should review the transaction in accordance with the '**ML/TF Risk Operations Review Procedures**' set out in **Chapter VI** of this Policy and, if there are grounds for suspicion, report them to the Financial Intelligence Unit.

The operation must be suspended until a decision from the FIU is made, which will be communicated in writing, or by any other means. The FIU authority may determine the suspension of its execution.

The operation may, however, be carried out if the suspension order is not confirmed by the FIU within three (3) days of the communication made by the Bank.

If abstaining is not possible or, after consultation of the Financial Intelligence Unit, it appears that it would bring on about future investigations in the context of the prevention

of money laundering or terrorist financing, the operation may proceed and. The obligated entity must immediately provide the FIU with information regarding the operation.

5.8. Examination Duty

The duty to examine consists in the obligation to examine, with particular attention, any conduct, activity or transaction, the characteristics of which make it particularly likely to be associated with the commission of the crimes of ML/TF-P or any other crime, in particular:

- the nature, purpose, frequency, complexity, uncommon nature and atypical nature of the conduct, activity or operation;
- the apparent absence of an economic objective or a lawful purpose associated with the conduct, activity or operation;
- the amount, origin and destination of the funds moved;
- the means of payment used;
- The industry and behavioral pattern/profile of the actors;
- The type of transaction or product that may particularly favor anonymity.

The assessment of the degree of suspicion evidenced by an activity, behavior, or transaction does not presume the existence of any confirmatory documentation of the suspicion. Instead, it arises from the evaluation of the specific circumstances, in light of the due diligence expected from the bank's employees. The procedures for analyzing transactions are detailed in **Chapter VI** of this policy.

5.9. Obligation to report operations to competent authorities

BIR is obliged to report transactions in the following circumstances:

- when it knows, suspects or has reasonable grounds to suspect that a transaction which could constitute money laundering or terrorist financing has taken place, is being or has been attempted;

- Cash transactions of an amount equal to or greater than 15,000.00 USD (Fifteen Thousand United States Dollars) in national currency or equivalent; and
- When, at the inception and during the business relationship, or before the completion of a transaction, the identity of a customer, or potential customer, or any other person, group or entity corresponds to the identity of a person, group or entity designated on the Sanctions List ³.

The specific reporting obligation also applies in the event that transactions reveal a particular risk of ML/TF-P, in particular when they relate to a particular country or jurisdiction subject to additional measures decided by the Angolan Government.

The supervisory authorities of the respective sector may determine the duty to immediately report such transactions to the FIU when the amount is equal to or greater than the national currency equivalent of 15,000.00 USD (Fifteen Thousand United States Dollars).

When the business units or employees of the Bank communicate suspicious transactions or activities to the *Compliance Directorate*, the latter is completely prohibited from providing any information both internally and externally about the Customers or transactions to which the information relates without complying with the obligation of secrecy.

5.10. Internal procedure for reporting suspicious transactions

³ **‘Designated persons, groups or entities’ means** designated persons, groups or entities (Directive 03/ISD/2012 - BNA):

- i. by the Sanctions Committee of the United Nations in accordance with United Nations Security Council Resolution 1267, in the form of the Sanctions Committee's updated list;
- ii. by the Sanctions Committee pursuant to United Nations Security Council Resolution 1988 maintaining an up-to-date list of persons, groups and entities associated with the Taliban who constitute a threat to the peace, stability and security of Afghanistan;
- iii. any other Sanctions Committee established by the United Nations or any other body of the United Nations that maintains lists of persons, groups or entities associated with terrorism, including terrorist financing, terrorists or terrorist organizations, with a view to the application of restrictive measures of a financial nature; and
- iii. by the national authority competent for the national designation and application of restrictive measures, by national list, in accordance with Law No 1/12 of 12 January - Law on the Designation and Enforcement of International Legal Acts, where the designation relates to persons, groups or entities associated with terrorism, including terrorist financing, terrorists or terrorist organizations, with a view to the application of restrictive measures of a financial nature.

The business unit that detects or conducts the suspicious transaction must immediately communicate via *e-mail* to the *Compliance* Directorate for review and decision.

If the suspicion is confirmed, and after submission of the "Incidence Report" to the attention of the Administration, the communication to the FIU should be carried out in accordance with the decision of the Compliance Directorate.

Transactions must be reported to the FIU by electronic submission of the official forms, through the *website* (*GoAmI*) of the FIU, or when there are no technical conditions on the part of the entity to report, it shall be sent either by means of *e-mail* or by post.

- **Official FIU form:**

Suspicious transactions must be reported by submitting a Suspicious Transaction Declaration (STD), which must be completed according to the respective "STD Completion Guide" available on the FIU and BNA⁴ websites.

5.11. Notification of Designated Persons and Entities

Whenever BIR knows, suspects or has reasonable grounds to suspect that the identity of the customer, or potential, or any other person, group or entity involved in a business relationship or that a transaction is a designated person, group or entity, it must report this to the FIU.

Designated persons and entities are detected through the filtering process carried out in the context of the account opening and throughout the business relationship.

- **Official FIU form:**

Designated persons and entities should be communicated through the submission of a Designated Persons and Entities Identification Declaration (DPID), which must be completed in accordance with the respective 'Guide for the Completion of the Identification Statement (DPID)', available on the *websites* of the FIU and BNA⁵.

⁴ <http://www.bna.ao/Conteudos/All/lista.aspx?dc=881&idl=1>

⁵ <http://www.bna.ao/Conteudos/All/lista.aspx?dc=881&idl=1>

5.12. Reporting of Cash Transactions

Cash transactions in the amount equal to or exceeding 15,000.00 USD (Fifteen Thousand United States Dollars) in the national currency or its equivalent are submitted daily and directly to the Financial Intelligence Unit (FIU) by the Compliance Department (DCOMP) in XML format through the web-based (GoAML) system.

The reporting of cash transactions is not dependent on a judgment of suspicion and is subject to mandatory reporting. The reporting of transactions must be undertaken regardless of whether transactions are carried out in a single operation or in several operations which appear to be linked.

Splitting or structuring transactions may be used to avoid any of the systematic records or communications under applicable anti-money laundering and countering the financing of terrorism legislation.

5.13. Duty to retain documents

BIR Bank will keep, for a minimum period of ten (10) years, all records, which includes:

- a copy of the documents or other technological means proving compliance with the obligation of identification and due diligence;
- a record of national and international transactions which is sufficient to allow each operation to be reconstituted so as to provide, where necessary, evidence in the context of criminal proceedings;
- all documentation relating to transactions with correspondent banks;
- recording the results of internal investigations and recording the copy of communications made by the banking financial institution to the Financial Intelligence Unit and other competent authorities;
- Reasons for the decision not to communicate to the Financial Intelligence Unit and other competent authorities by the *Compliance Officer*;
- copy of all commercial correspondence exchanged with the customer;

- Recommendations on AML/TF prevention made by the Directorate Internal Audit (DIA).

In addition, BIR Bank will keep, for a period of five (5) years, copies of documents or records relating to training provided to its staff, including the Management and Administration Bodies.

This documentation will be kept in an appropriate manner so that it can be easily located and its confidentiality guaranteed.

The archiving system will ensure appropriate management and availability of documentation, both for internal control purposes and for the purpose of responding in a timely manner and when requested by the BNA, the FIU and other competent authorities.

5.14. Duty of Cooperation

The Bank, through the *Compliance* Directorate, will promptly provide cooperation to the National Bank of Angola and the Financial Intelligence Unit, when requested by them, providing them with information on certain transactions carried out by customers and presenting documents related to certain transactions.

It should also cooperate with the competent judicial and police authorities after the initiation of formal investigation proceedings.

Requests for information, letters and/or notifications regarding crimes of ML/TF-P addressed to the Bank, issued by Courts or any other Authority, should be sent to the Secretariat of Administration, which should inform the Executive Board and the Directorate of Compliance.

All such requests for information, letters and/or notifications received by the Competent Authorities, in relation to the crimes of ML/TF-P, will be recorded with the date of receipt in a database maintained by the Directorate of *Compliance* for that purpose. Likewise, the official replies issued by the Bank must be recorded on the same medium. The following information should be recorded, where applicable:

- Letter/Notification Number;
- Designation of the Competent Authority;
- Name and Entity Number (BIR Bank Customer) and associated account(s);
- Date of receipt/date of reply;
- Other relevant information.

In addition to the respective physical archive of the documents received and issued, they must be digitally scanned and archived by DCOMP. All letters sent by BIR to the Competent Authorities, concerning the crimes of ML/TF-P, must be signed by at least two (2) Executive Administrators. The following reporting principles and formats apply to the sending of the response to the requesting entity:

- *Email* means of submission: must include acknowledgement of receipt;
- In-person delivery: It must be ensured that the recipient signs to acknowledge receipt of the duplicate copy.

5.15. Duty of Confidentiality

Communications on this subject are strictly confidential.

The Bank, its members of the respective corporate bodies, or those who hold management or leadership positions, its employees, agents, and other individuals who provide services to them on a permanent, temporary, or occasional basis, may not disclose to the customer or to third parties that they have transmitted legally required communications or that a criminal investigation is underway.

Non-compliance with this rule is considered as a very serious infringement for those responsible.

5.16. Duty of Control

BIR Bank should implement internal policies and procedures that are appropriate to the performance of legally established duties, including internal control, risk assessment and management, and internal audit, in order to effectively prevent and detect the commission of ML/TF crime.

5.17. Training Obligation

The Bank should provide ongoing training on the prevention and detection of money laundering and terrorist financing to its staff, according to their different needs, in particular the *front - office*, supervisory or *compliance*, audit, risk management and commercial management staff.

The Directorate for *Compliance* will carry out the training activities in line with the Controls and Qualification Department (CQD) and a record will be made of all the training activities carried out, leaving evidence of the date, place, duration of each course and name of participants.

BIR sets as a priority objective the adoption of the necessary measures to ensure that all employees receive this training.

The measures should include specific and regular training, appropriate to the banking sector, enabling Bank employees to recognize operations that may be related to the commission of ML/TF-P crimes and to act in accordance with the legislation in force.

In this sense, specific training actions are included in the "Annual Training Program", addressed to the Bank's staff, including the Management and Administration Bodies, which will take into account the international standards, the laws and regulations in force in Angola in this field, as well as the "Guidelines" issued by the Financial Information Unit (FIU).

Training actions should include content on the following subjects:

- the Bank's internal policies and rules;
- internal processes and procedures for identification, due diligence, reporting of transactions, abstention and refusal;
- Internal control and risk assessment system for ML/TF-P prevention;

- *Templates* and internal forms;
- ML/TF-P risk management model;
- Business/practice trends associated with ML/TF/P;
- Types of suspicious transactions.

Regardless of general training plans, the *Compliance Directorate* must keep all employees informed at all times of any legislative changes in this area, as well as of any new arrangements, techniques or procedures that may be identified as being likely to be used to commit ML/TF-P crimes.

CHAPTER VI - IDENTIFICATION/DETECTION OF OPERATIONS AND MONITORING

The process of identifying/detecting transactions and monitoring is aimed at monitoring the customer's transactional activity (during and after the execution of transactions), with a view to identifying suspicious ML/TF-P behavior and transactions.

The monitoring carried out must focus on individual transactions and transaction flows that make up behavioral patterns or Customer transactional profiles, encompassing historical analysis of transactions performed as well as analysis of types of operations with higher risk or more vulnerable to ML/TF-P practice.

6.1. Identification and Detection of Suspicious Operations and Monitoring

The Directorate for *Compliance*, as well as the business areas and other business units, should put in place appropriate procedures for the control and analysis of transactions suspected to be related to ML/TF-P crimes, with the aim of identifying and reporting those transactions to the Competent Authorities.

The identification of suspicious transactions may take place through the following detection categories:

i. Detection of outliers against the Entity behavioral pattern/transactional profile:

For this purpose, accounts shall be taken of the specific characteristics of the operations and their actors, such as:

- Type/nature and complexity of transactions;
- Atypicality within the customer's normal business activities: It should be verified whether the transaction(s) is disruptive compared to the customer's typical behavioral pattern, considering the following factors:
 - Amounts involved;
 - Payment method used;
 - Frequency / Speed;
 - Countries and jurisdictions involved in the transaction: it should be verified that the transaction(s) involve Countries, territories or regions other than those declared by the Entity during the account opening process;
- Financial/asset situation of the parties involved: it should be verified whether the type of activity and/or amount of the transaction conducted by the entity is appropriate for the expected business activity declared during the account opening process;
- Customer's Industry sector: It should be verified whether any transaction(s), in terms of scope and nature, is incompatible (or unusual) with the type of customer (e.g., considering the purpose of the business relationship, account purpose, industry sector);
- Origin and destination of funds: the justification of the origin and destination of funds must be examined, verifying whether the cash deposits made showcase any suspicious/irregularities (including initial deposit);
- Economic justification of transactions: It should be verified whether any transaction(s) presents a purpose and characteristics that are distinct from the normal pattern associated with the respective typology of those transactions.

ii. Framing transactions in a type of suspicious transaction

- When identifying and detecting suspicious transactions, the typologies of suspicious transactions disclosed by International Organizations, Supervisors, and other Bodies should be taken into account (Annex II A of this policy).

iii. Relationship and aggregation of transactions

- It consists of the detection of suspicious transactions by aggregating or associating transactions made by Customers and related parties.

iv. Filtering against Sanctions Lists/ Suspects Lists

- Identification of suspicious transactions by filtering the parties involved (payers/payees) as well as the countries, jurisdictions or territories of origin and destination of transactions.

The analysis and investigation of suspicious transactions may be triggered by:

- **Identification and detection of suspicious transactions by the Compliance Directorate** - through ongoing monitoring of entities and accounts;
- **Identification and detection of suspicious transactions by the Commercial Network** - in direct contact with customers via *front-office* and other business units;
- **Enhanced Entity Monitoring** - through tracking high-risk customers.

6.2. Identification and Detection of suspicious transactions by the Compliance Directorate

For the purpose of identifying and detecting potentially suspicious transactions, BIR has defined parameters and risk indicators, which are used as transaction selection criteria and are subject to ongoing review by the *Compliance Directorate*.

The *Compliance Directorate* should review operations that generate "alerts" as they fall within the defined risk parameters, seeking to identify if there are indications of suspicion or if the operations performed fall within the normal activity of the customer.

When analyzing transactions, the Directorate for *Compliance* must take into account the profile of the actors and the characteristics of the transactions, as described in the previous paragraph.

If the transaction is considered to be in line with the behavioral pattern/transactional profile of the Entities, the alerts will be closed. The conclusion of the analysis of the transactions should be documented in writing, providing the rationale for closing the "alerts". If the transactions present substantial grounds for suspicion, a "Case" should be opened, and additional due diligence should be conducted.

6.3. Identification and Detection of suspicious transactions by the *front office* and other Business Units

All business units must implement measures to monitor the business relationship with the customer, including scrutiny of transactions undertaken to ensure that they are consistent with the Bank's knowledge of the Entity and its business and risk profile, including the source and destination of funds moved.

The identification and detection of suspicious transactions should take into account the types of suspicious transaction listed in **Annex II A** to this policy.

Business units should follow internal procedures that set out how to proceed when suspicious transactions need to be reported. The *Compliance Directorate*, so that it complies with the applicable legislation, carries out the necessary analysis/investigation and, if there are grounds for suspicion, carries out the communications due to the Competent Authorities (Chapter V, paragraph 15).

6.4. Entity Monitoring (high risk, PEPs, referenced by competent authorities)

For the purpose of monitoring the transactional activity of BIR Entities, a risk-based approach is adopted. In accordance with the 'Entity Monitoring process', the Directorate of *Compliance* should conduct an analysis of the transactional activity of the following Entities:

- **High Risk rated entities:** they should be monitored on a monthly basis, following the weekly history of the transactions carried out (type, amounts, frequency, volume, complexity, destination, etc.) for a period of six (6) months after the start of the business relationship;
- ☐ **Entities classified as High Risk and that are PEP's** (politically exposed persons): to be monitored on a monthly basis, following their weekly track record of the type, amounts and volume of transactions they carry out, over a period of one (1) year;
- Customers who have carried out operations where there is evidence of suspicion, but the screening process has been completed with the application of the monitoring measure, without however having been reported to the Competent Authorities. In such cases, the *Compliance Directorate* should monitor the activity of customer on a monthly basis for a period of three (3) months;
- Individuals or entities referenced by Judicial or Investigative Authorities, the Financial Intelligence Unit, or the National Bank of Angola (during the period and with the frequency determined by the competent Authority).
- Entities referenced in public knowledge situations where they are deemed to present increased ML/TF risk.

Unmarking Entities for enhanced monitoring purposes by applying risk criteria may occur when the following circumstances arise:

- after the monitoring period, if '**Closure of Monitoring** is determined'; or
- If the Customer is reclassified as Medium or Low Risk as part of the risk reassessment and knowledge of the customer's operation already exists.

6.5. Operations Investigation by the *Compliance Directorate*

The *Compliance Directorate* should review the operations that generated an alert and, if there are grounds for suspicion, should open a "Case" and carry out additional investigative steps.

The investigation should consider as an illustrative list of potentially suspicious transactions (**Annex II-A**), taking into account the specific characteristics of the customer and its transaction activity, in particular:

- Nature of the entity (Private/ENI (Entities not identified); Corporate and Institutional);
- risk characterization of the contracting parties;
- Entity transactional profile / behavioral pattern.

The investigation procedure should include:

- research using open and closed public sources, making it possible to assess the credibility and timeliness of existing information, the suitability of the entities involved, the financial and economic data of the entity or the sector of which it forms part, and to identify possible group relationships between counterparties;
- Obtaining supporting documentation for transactions through the other business units as well as additional clarifications to support the findings of the investigation.

If the alert concerns contracts that have been previously flagged with the same risk typology, the analysis process follows the aforementioned guidelines, with particular attention given to the following points:

- Validation and possible updating of previously collected information, particularly regarding personal data, nature of the contract, and ownership of the contract;
- Significant changes in the transaction profile compared to the previous analysis.

Following the completion of the investigative steps, the *Compliance* Directorate issues an **"Incidence Report"** which is submitted to the Executive Board (after review by the Head of the Compliance Directorate) in the following situations:

- i. When the outcome of the investigation is '**Case closed with confirmation of suspicion**' and one of the following measures is proposed:
 - a. Report Customer to Competent Authorities; and/or
 - b. Account closure.
- ii. when the case involves high-risk entities and/or PEPs (politically exposed persons);
- iii. When the transactions that determined the investigation involve Entities referenced by the Competent Authorities.

"Incidence Report" must contain the following information:

- **Source of analysis/incidence:**
 - Identification by the *Compliance Directorate* - alert analysis;
 - Identification by Business Directorates or other Business Units;
 - Identification by the Operations Directorate;
 - Entity Monitoring (high risk /PEPs (politically exposed persons); or
 - Monitoring of Entities referenced by Competent Authorities;
- **Entity Risk Level** (*Scoring* KYC);
- **details of suspicious behavior/transaction and reasons for suspicion** (identification and justification of relevant facts associated with account movement and identified counterparties);
- **Additional information collected and documentation of evidence** (information on research performed and clarifications obtained to support the conclusions of the investigation);
- **Conclusion of the analysis/focus:**
 - Case closed without suspicion;
 - case closed without suspicion with monitoring; or
 - Case closed with confirmation of suspicion;

- **If applicable, proposal for measures to be implemented:**
- Customer reporting to Competent Authorities;
 - extension of the monitoring/monitoring period for a specified period; and/or
 - Account closure.

CHAPTER VII - CONTROL OF ENTITIES SUBJECT TO FINANCIAL COUNTERMEASURES

7.1. Entity and Transaction Filtering

BIR Bank should match, at the inception and during the business relationship or prior to the completion of a transaction, the identity of an actual or potential customer, or any other person, group or entity involved in a business relationship or transaction, with the data of persons, groups or entities designated in Sanctions Lists in order to determine whether their identity corresponds to a designated person, group or entity.

7.2. Entity Filtering

Entity filtering is performed through *Lexis Nexis Compliance Link/Eagle AML*. According to these IT solutions, in the event of a match, or similarity between the Entity's identity and

a sanctioned person or entity, the *Compliance Directorate* shall perform additional due diligence measures to determine whether the match is confirmed or a False Positive.

7.3. Filtering and Blocking Transactions

In the process of issuing and receiving SWIFT transactions, as well as non-automatically processed cross-border transactions through the SWIFT system (e.g., documentary remittances), the transactions should be screened against the Sanctions Lists (UN, OFAC, and EU) using the filtering tool prior to executing the transaction.

All transaction data should be filtered, including:

- (i) Details of all parties involved - payer (s) and payee (s); and
- (ii) Countries, jurisdictions, regions or territories of origin or destination of transactions.

If a *hit* is detected between the identification of the actors and the identity of a designated person or entity, the transaction must be pending until the *hit* analysis (for confirmation of the match) is completed.

Filtering	Analysis	Stakeholders
False Direct Positive: the <i>hit</i> stems from information that is not directly related to the content of the operation, nor to its participants, being a 'false' coincidence (e.g., Angola - Portugal vs. Angola - Algeria)	<ul style="list-style-type: none"> No additional due diligence required The operation must therefore be justified and duly authorized for filtering. 	<ul style="list-style-type: none"> Compliance Directorate

Filtering	Analysis	Stakeholders
<p>False Positive Potential: The <i>hit</i> is generated by the fact that some element of the operation actually coincides with a constant element in the Sanctions Lists, the operation must be analyzed in detail.</p>	<ul style="list-style-type: none"> • Additional due diligence ("Matching Filter Result Analysis Procedures") is required • Need to obtain detailed knowledge of the operation, and additional information may need to be requested from the Commercial Network, including transaction support documents. 	<ul style="list-style-type: none"> • Compliance Directorate • Counter • PDO

➤ Confirmation of the "*hit*":

If the match is confirmed, i.e., if the *Compliance Directorate* concludes that it is a designated person or entity on a Sanctions List, the transaction must be blocked. The Directorate of *Compliance* must *then* communicate them to the FIU (Financial Intelligence Unit) by submitting a "SDPE"- Statement of Designated Persons and Entities.

Where a transaction is to or from a country, jurisdiction, region or territory subject to financial countermeasures (financial sanctions/embargoes), according to an official listing shared by the competent authority, the transaction should also be blocked.

➤ False Positive:

If the *Compliance Directorate* concludes that this is a False Positive, it must authorize the transaction to be executed by the Operations Directorate (PDO).

The conclusion of the analysis should be duly recorded and substantiated by DCOMP, including the justification for the operation or the reason for the refusal (registration on a database maintained by DCOMP and in the filtering tool).

7.4. Freezing of Funds and Economic Resources

BIR Bank is prohibited from making funds, economic resources or other related services available, directly or indirectly, to persons, groups and entities designated by the Sanctions Committee of the United Nations, in accordance with United Nations Security Council


Resolution 1267, and by the competent authority at national level. It is also required to freeze immediately and without prior notice all funds or economic resources belonging to, owned or held, directly or indirectly, individually or jointly by such persons, groups and entities and to communicate them to the FIU and the BNA.

In accordance with the provisions of the law, when BIR Bank is made aware of, suspects or has reasonable grounds to suspect that the identity of the payer, the payee or any other person/entity involved in a transaction matches the identity of a designated person, group or entity, it must refrain from carrying out the transaction. The Directorate of *Compliance* has to this report to the Financial Intelligence Unit and wait for the issuing of the Instruction by this Entity of the terms of the freeze.

Until receipt of the Instruction, the frozen funds or economic resources is owned or controlled by the Bank.

CHAPTER VIII - ANNEXES

ANNEX I - *Template* for "Incidence Report"



Incidence Report

DCOMP

Entity Data

Name/Denomination of the Entity

Entity No

Identification Number (ID/Passport/Other)

Tax Identification Number

Entity Type

Particular/ENI ☐
(Mark with an X)

Company/Institutional ☐
(Mark with an X)

Entity Risk Profile

SCORING(NYC) Low risk ☐ Medium risk ☐ High risk ☐

Reason for opening the Case

Suspicious Operation ☐
(Mark with an X)

Suspicious Behaviour ☐
(Mark with an X)

ANNEX II - Type of Suspicious Operations

This section aims to guide BIR staff in identifying and detecting transactions with a potential risk of association with money laundering and terrorist financing activities.

This is a list of possible cases of money laundering transactions.

A. Type of suspicious transactions or activities identified by the Financial Intelligence Unit for banks and non-bank financial institutions related to money and credit ⁶

In this sector, we can find some indicators of operations that may be related to ML/TF/P:

- a potential customer has a large amount of cash in his possession and opens several accounts or purchases several products with variations in the names of the accounts;
- a prospective customer has several different currencies and wishes to conduct foreign exchange operations as part of the transaction;

⁶ Website of the Angolan Financial Intelligence Unit - "General Guidelines of the FIU"

- the customer structures a transaction in such a way that the total amount is split into several smaller transactions so that the limits laid down are not exceeded (*smurfing*);
- a foreign customer uses alternative remittance services (ARS) to transfer significant amounts of money, with the false pretense of transferring money to his family abroad;
- the customer purchases several similar financial products and moves funds between them in addition to cash payments;
- the high asset value of a customer is not compatible with the information about it or its business;
- a customer repeatedly uses an address, but frequently changes the names involved;
- the customer's business or home telephone number is disconnected or it is detected that it does not exist when attempting to make the first contact within a short period of time after opening the account;
- The customer is involved in an unusual activity for the type of person or the type of business.

B. Illustrative catalog of risk transactions for credit entities

(i) Unusual and/or frequent changes in the type or nature of the means of payment, not reflected in the customer's account:

- Exchange of foreign currency for high denomination banknotes performed by one and the same person or by several in an apparently concerted manner, at one time or in a split manner, in low - value operations spaced over time;
- Procurement of bearer instruments of payment (bank checks, electronic money, *traveler checks*) against cash delivery on a systematic or large scale.

(ii) Atypical cash operations

- a significant increase in cash deposits made by any person or corporation for no apparent reason, especially if the deposits are later transferred, within a short

period of time, to a destination that is not normally related to the customer's business or activity;

- customers transferring large amounts of capital abroad, followed by instructions to pay in cash;
- large cash deposits, made under conditions designed to avoid direct contact with the staff of the Bank;
- large number of natural persons depositing in the same account without adequate explanation;
- cash deposits, as the main means of feeding the account, which records payments for valuable or sumptuous goods (real estate, pleasure boats, luxury vehicles, jewelry);
- cash deposits on high denomination banknotes, and it is normal in the type of business to use lower denomination banknotes;
- Deposits of cash, of a relevant amount, made directly to the credit card, without going through the current account and generating a positive balance in favor of the credit card.

(i) Unusual activity on bank accounts:

- Any person or company whose accounts do not show normal banking or business activities but use them to receive or debit significant sums that do not have a clear purpose or relationship with the account holder and/or his business (e.g., a substantial increase in the volume of movement in an account);
- customers who have accounts with several financial institutions in the same geographical location, and especially when the Bank knows that there is a process of regular consolidation of such accounts prior to the request for a transfer of funds;
- a balance between payments and deposits made on the same or the previous day;
- Accounts of corporations making payments through transfers to a limited number of alleged suppliers, with funds previously received in cash or through transfers from alleged customers matching, or close to, the amounts of the movements to the alleged suppliers;
- Withdrawal of large amounts from a previously dormant/inactive account or from an account that has just received a large unexpected amount from abroad;
- Significant increases in cash deposits or deposits in negotiable instruments by a professional or firm's office using accounts opened in the name of a third party,

especially if deposits are transferred quickly between another customer and the fiduciary account;

- Accounts recording repeated receivables for the payment of lotteries and gaming prizes;
- Credits for returns of taxes and/or subsidies that are produced repeatedly and to a significant amount, associated in particular with trade in Angola, with respect to customers who do not have a real business or commercial activity justifying them;
- Systematic bearer checks issued for quantities equal to or less than AOA = 300 000 or the foreign currency equivalent;
- Customers legal entities that perform more transactions using cash than through other usual means of payment and collection for that type of commercial activity;
- Transfers of funds between the accounts of various companies with identical natural persons (directors, authorized representatives, public prosecutors) and/or with common domiciles (head office or mailing address);
- Opening of accounts in the name of new companies by the same natural persons (directors, authorized representatives, public prosecutors) with management or domiciles common to other companies with accounts in the entity that apparently have ceased their activities (short-lived company);
- Receipt of electronic transfers from abroad without the payer's identity or the account number of the transfer;
- Carrying out on the same date multiple deposit transactions using cash or other monetary instruments and in quantities that are per system slightly below the threshold that would be required to be identified or justified, especially if the numbering of such documents is sequential;
- Large check credits, in favor of third parties and endorsed to our customer;
- Accounts in the name of minors or incapacitated persons, the representatives of which carry out a large number of transactions or movements in those accounts.

(ii) Unusual use of fictitious company structures, existing companies or associations or foundations with little real activity:

- Operations through accounts of national companies owned by entities established in tax havens or high-risk countries, represented by independent professionals or other intermediaries, which receive high-value transfers from abroad;
- Transactions carried out by domestic companies with real economic activity which at a certain time receive transfers from tax havens or risk countries for the purpose of increasing capital, making supplies or similar transactions, without changes in the management of the company or its representatives;
- Operations of recently established companies with low share capital that, since their opening, receive or make high-value transfers abroad for the payment or receipt of computer equipment, mobile phones, or similar items, and receive or make domestic transfers originating from or destined to a small number of companies in the same sector, maintaining significant activity for a short period of time, only to cease or be replaced by other companies occupying their position;
- transactions carried out by companies engaged in the import of vehicles whose funds are mostly in cash deposits or orderly transfers from a number of related companies;
- Accounts opened in Portugal that receive small transfers ordered by individuals, usually from abroad, in small individual amounts, but adding up an important overall quantity, without identifying in the account operation movements appropriate to a business activity (personnel costs, payment of raw materials, supplies of third parties, etc.). Generally, cash withdrawals and/or transfers are made to tax havens or countries at risk from the funds received. This operation is particularly relevant in the investment services business sector, where they are acting without a corresponding authorization and/or where there is no evidence in their accounts of the realization of the investments and how the funds received have been spent;
- Deposits in accounts of associations or foundations, as a donation, solicitation or similar activity in a relevant amount at a given time, without the existence of a disaster or advertising campaign justifying the recoveries being known, and subsequently remitting most of the funds to countries where they are not known to be habitually active;
- Movements in the accounts of legal persons (companies, foundations, associations, etc.) provided that payments are generally made and that they lack social security charges, wages, taxes, water, electricity, etc., but nevertheless

show a significant volume of movement of funds, without identifying a link with the declared use of the account.

(iii) Atypical international fund movements, unusual or without economic justification, in significant amounts:

- Customers who feed their accounts through cash deposits and withdraw funds through ATM withdrawals, especially abroad, in countries considered to be exporters of narcotic substances. Deposits may coincide with withdrawals. Often you hire several cards associated with the same account. Withdrawals generally reach the daily limit allowed for this type of operation;
- the use of letters of credit and other commercial financing methods to move capital between countries where such trade is illogical in relation to the normal business of the customer or by making changes to the name, direction or place of payment of the letter of credit at the time immediately preceding payment of the letter of credit;
- use of invoices and import documents, insurance, or evidence of obviously false goods transport, in support of transfers sent from outside;
- the systematic use of over-invoicing or under-invoicing in international trade transactions, reflecting a much higher or lower than market price, commonly known, as experienced by the entity in past similar transactions;
- A customer who acts as a collector of funds from other individuals of the same nationality, in small amounts, pooling them together and sending them abroad, acting as an informal money transmitter;

- Movements of funds made by foundations or associations formed in Angola and made up mainly of foreign citizens;
- Private (usually foreign) or corporate (usually newly incorporated limited liability companies with minimum share capital) accounts which, since their opening, have recorded strong cash deposits and immediate transfers abroad, keeping low balances in relation to the volume of funds transiting through the account, supporting transactions in economic activities that are difficult to verify;
- Accounts under the ownership of natural persons (usually non-residents), who say that they are traders or simple intermediaries in foreign trade transactions, in which large cash deposits or smaller cash deposits are recorded directly but from different points in the country, immediately ordering large transfers abroad, resulting in the beneficiaries being distributors (usually from Asian countries) of very varied products with diversified economic activity.

(iv) Loans, credit lines or captive transactions, whether secured or unsecured:

- Customers who unexpectedly cancel problematic loans or repeatedly write off significant amounts of loans early, mainly with cash deliveries;
- Loans guaranteed by third-party persons who do not appear to have any relationship with the customer and which result in their non-liquidation and, in the end, one of the guarantors is the one paying;
- Loan application supported by assets deposited with the financial entity or with third parties, the origin of which is unknown or the value of which is unrelated to the situation of the customer;
- Request for asset-backed loans deposited in tax havens or at-risk countries;
- Loan application, credit line and asset transaction by a customer whose formally declared repayment capacity (tax returns) is ostensibly lower than its actual repayment capacity and the difference is quantitatively relevant;
- Resident enterprises or individuals that finance themselves with loans or equity from abroad, where the lender is an individual or non-financial entity.

(v) Politically Exposed Persons from High-risk countries, jurisdictions, regions or territories:

- Accounts opened in Angola by persons holding prominent political, high office or similar positions (directors of public enterprises, etc.) in generally undemocratic countries, including close family members, and who receive funds from abroad that they invest in the purchase of real estate or financial assets of a relevant amount or the constitution of high deposits;
- transactions in cash or monetary instruments falling directly below the amounts for which there is an obligation to inform the authorities;
- Large transactions that are not in line with the account type or deposits of the holder and the sources of wealth;
- transactions carried out using illogical circuits for no apparent reason, except that of concealing the identity of the fund owner;
- a request for an operation indicating that it is to be handled by a third party;
- Transactions channeled through banking secrecy jurisdictions or through entities based in countries with limited customer identification regulations;
- Transactions involving funds that originate from central bank or government-owned bank accounts;
- Transfers from or to other accounts of relevant public persons;
- inflows of funds by any means that are immediately transferred for a similar amount to another institution in a third country;
- Refusal to provide information on the economic motive or purpose of the transfers issued or received;
- Questions on how to avoid reporting requirements to authorities or the scope of banking secrecy laws, or other rules on reporting suspicious transactions;

- Offering of collateral provided by *offshore* or domiciled *institutions* in a jurisdiction with impenetrable banking secrecy.

(vi) Lack of data, lack of deliberate contact with BIR or lack of concern for the profitability or advantages of the products:

- customers who do not act on their own behalf and who do not wish to reveal the true identity of the beneficiary;
- resistance to providing normal information when opening an account, providing minimal or false information or providing information that is difficult to verify by BIR;
- customers who have an acceptable degree of 'financial culture' but who decline to provide information that would normally allow them to access credit or other banking services that would be advantageous;
- representatives of undertakings which avoid contact with BIR without justification;
- Insufficient use of normal banking advantages, e. g. not using interest rates for high credit balances;
- Repeated difficulties for the entity to contact the customer at home or on the telephone indicated by the Customer, resulting in mail returns due to the customer's ignorance at that address;
- Customers presented to the entity by known and reputable persons (professional offices, entrepreneurs, etc.), and that this presentation appears to facilitate the duties of knowing the Customer's data;
- customers who are reported in the media as being involved in criminal activities that may generate economic benefits;
- Customers with a greater than usual interest in establishing direct and personal relationships with the head of the Counter and its employees for the purpose of relieving the entity's duties or controls;
- Customers who show curiosity about the entity's internal systems, controls and policies regarding the prevention of money laundering and terrorist financing.

(vii) Correspondent accounts with foreign entities insufficiently known and/or located in tax havens:

- request to subscribe to correspondent relationships with foreign financial entities incorporated in risk areas for which no money laundering prevention policies are applied;
- Accounts opened in Angola by a financial entity, which appears as the account holder, structured in several sub-accounts to specifically reflect transactions carried out by customers of the financial entity formally holding the account;
- Accounts opened in Angola by foreign financial entities that keep correspondent accounts with shell banks open;
- unusual attitudes of employees and representatives of financial institutions;
- Changes in the employee's characteristics, for example, sumptuous lifestyle unrelated to his expected situation or income level;
- Change in the employee's or representative's results, for example, the commercial who sells products against cash and has a noticeable or unexpected increase in their results;
- Any contact with a representative in which the identity of the ultimate beneficiary or person corresponding to him remains hidden, contrary to the normal procedure for the type of business;
- Employees whose duties involve dealing with customers and who resist accepting a change of position as a result of which they will no longer be engaged in the same activities.

ANNEX III - List of categories of underlying crimes related to money laundering (listed in the glossary of the 40 Recommendations of the FATF, supplemented by Law No. 38/20 of November 11th, the Angolan Criminal Code):

- Participation in an organized criminal group and in unlawful actions to obtain funds, including through blackmail, intimidation or other means;
- terrorism, including the proliferation of weapons of mass destruction;
- trafficking in human beings, including trafficking in human organs or tissues and the smuggling of migrants;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- trafficking in stolen property and other property;
- Corruption;
- bribery;
- fraud;
- counterfeiting currency;
- Counterfeiting;
- Product piracy;
- environmental crime, including trafficking in protected species;
- Murder;
- Serious bodily harm;
- abduction;
- kidnapping;
- hostage-taking;
- theft;
- Smuggling;
- extortion;
- Falsification;
- Piracy;
- insider dealing and market manipulation;
- Tax crimes.