Policies and Procedures for the Prevention of Money Laundering and the Combat of Terrorist Financing and the Proliferation of Weapons of Mass Destruction

Banco BIR, S.A

Document Details

Title:	Policies and Procedures for the Prevention of Money Laundering and the Combat of Terrorist Financing and the Proliferation of Weapons of Mass Destruction
File:	DCOMP_ Policies and Procedures for the Prevention of Money Laundering and the Combat of Terrorist Financing and the Proliferation of Weapons of Mass Destruction

Document Review

Date:	Version	Responsible	Cause for Action
05-2025	V.5	DCOMP	Update
05-2025	V.5	DOQ	Formatting
05-2025	V.5	CI	Validation

Approved by:

Date:	Version	Name
02-06-2023	V.5	Board of Directors

Document Updates:

Version	Effective Date	Amendments
V.1	01-12-2015	Creation (CA.OS.MP.006.2015)
V.2	09-09-2019	Update (CA.OS.MP.006.2015)
V.3	08-12-2020	Update (CA.OS.007.2019)
V.4	15-05-2023	Update (CA.OS.007.2020)
V.5	02-06-2025	Update (CA.OS.005.2023)

Applicable Legislation/Regulation Supporting the Document:

Legal Instrument	Effective Date	Subject
Notice No. 02/2024	March 22	Rules and Procedures for the Effective Implementation of Conditions for Exercise, Instruments, Mechanisms, Formalities, and Information Disclosure Related to the Prevention and Combat of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.
Regulation No. 5/2021	November 8	Prevention and Combating of Money Laundering and Terrorist Financing.
Law No. 1/2012	January 12	Designation and Enforcement of International Legal Acts.
Presidential Decree No. 2/18, of January 11	January 11	Establishes the organization and functioning of the Financial Intelligence Unit (FIU), providing for the obligation of financial institutions to report certain types of transactions.
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 January 27	January 27	Law on the Prevention and Combat of Money Laundering, Terrorist Financing and the Proliferation of Weapons of Mass Destruction, which establishes preventive and punitive measures against ML/TF and defines the applicable sanctions regime in the event of non-compliance.

Law No. 38/20	November 11	Law Approving the Angolan Penal Code
Law No. 19/17	August 25	Law on the Prevention and Combat of Terrorism, which establishes preventive, repressive, investigative, and special procedural measures, as well as support and protection for victims of terrorism. It applies to acts related to the phenomenon of terrorism committed within Angolan territory by national or foreign citizens, as well as to 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 Transaction Report Form.
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 9	Defines the template for the Anti-Money Laundering and Counter-Terrorism Financing Report, as well as the implementation of Risk Validation.
Instruction No. 13/2018	September 19	Establishes the Anti-Money Laundering and Counter- Terrorism Financing Criteria for International Trade Operations.
Law No. 12/24	July 4	Law Amending Law No. 38/20 of November 11, which Approves the Angolan Penal Code.
Law No. 09/24	July 3	Law Amending Law No. 19/17 of August 25, the Law on the Prevention and Combat of Terrorism.
Law No. 11/24	July 4	Law Amending Law No. 5/20 of January 27, the Law on the Prevention and Combat of Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction.

Guidelines on the Identification and Reporting of Designated Persons, Groups, and Entities – Freezing of Funds and Economic Resources	May 30	Guide on the Identification and Reporting of Designated Persons, Groups, and Entities – Freezing of Funds and Economic Resources.

Abbreviations:

- **UN –** United Nations
- **OFAC** – Office of Foreign Assets Control (U.S.)
- **EU –** European Union
- **BIR –** Banco de Investimento Rural
- **FIU** – Financial Intelligence Unit

INDEX

CHAPTER I – SCOPE AND OBJECTIVES

1.1. Scope

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

The standards set forth in this Manual and adopted by Banco BIR reflect the implementation of international principles and guidelines on Anti-Money Laundering, Counter-Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (AML/CTF-P), as well as the applicable legal requirements, the regulatory obligations established by the National Bank of Angola (hereinafter "BNA"), and the guidance issued by the Financial Intelligence Unit of Angola (hereinafter "UIF").

1.2. Objectives

In this Manual, Banco BIR sets out its internal Policies and Procedures on the Prevention and Combating of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (AML/CTF-P), with the following main objectives:

- To ensure the implementation of an effective system for the prevention and combating of money laundering, terrorist financing, and proliferation of weapons of mass destruction, adopting a risk-based approach.
- To ensure that Banco BIR has adequate knowledge of its customers ("Know Your Customer" – KYC), their business activities, and their transactions ("Know Your Transactions" – KYT);
- To ensure compliance with the legal and regulatory obligations applicable to the Bank.

- To raise employee awareness of the rules on AML/CTF and hold them accountable in the event of non-compliance.
- To ensure that international trade-related transactions are subject to enhanced due diligence procedures, given their high risk for money laundering, terrorist financing, and underlying offences.
- To establish appropriate controls to mitigate identified risks.
- To establish mechanisms that enable the effective detection of suspicious transactions, and their reporting to the competent authorities, namely the Financial Intelligence Unit (FIU).
- The department responsible for this Manual is the Compliance Department (DCOMP). The Manual is subject to formal approval by the Board of Directors (CA) of Banco BIR.

Any amendments or updates to this Manual must be approved by the Board of Directors, upon proposal by the Compliance Department (DCOMP) and with the knowledge of the Internal Audit Department (DAI) and the Organization and Quality Department (DOQ).

CHAPTER II – FRAMEWORK

2.1. Definitions

«Customer» Any natural or legal person, national or foreign, public or private, affiliated or not, who enters into a bank account agreement with the Bank, and to whom the Bank offers financial products and services.

«Know Your Customer» The KYC process involves identifying and verifying the identity of a customer at the time of account opening and periodically throughout the business relationship. It is a mandatory procedure to ensure the Bank knows who its customers are.

«Politically Exposed Persons (PEPs)» National or foreign individuals who hold or have held prominent public functions in Angola or in any international organization. For the purposes of this Law, the following are considered high-ranking political or public positions, among others:

1. President of the Republic or Head of State.
2. Vice-President of the Republic.
3. Prime Minister or Head of Government.
4. Senior officials reporting directly to the President of the Republic or members of Government, including Ministers of State, Ministers, Secretaries of State, Vice-Ministers, and other equivalent positions.
5. Members of Parliament or equivalent legislative bodies.
6. Judges of the Supreme Courts and Courts of Appeal whose decisions are not subject to appeal, except in exceptional circumstances.
7. Public Prosecutors at levels equivalent to the judges mentioned above.
8. Ombudsman and Deputy Ombudsman.
9. Members of the Council of the Republic, National Security Council, and other State advisory bodies.

10. Members of the National Electoral Commission.
11. Members of the Superior Councils of the Judiciary and the Public Prosecutor's Office.
12. Members of the governing and supervisory bodies of Central Banks and other financial sector regulatory and supervisory authorities.
13. Heads of diplomatic missions and consular posts.
14. General Officers of the Armed Forces and Senior Officers of Internal Security and Law Enforcement Forces.
15. Members of the governing and supervisory bodies of public companies, companies with wholly or majority public ownership, public institutes, public associations and foundations, public establishments, regardless of their designation, including governing bodies of enterprises within local business sectors.
16. Members of the Board of Directors, Directors, Deputy Directors or persons in equivalent roles in international organizations.
17. Members of the executive leadership bodies of political parties.
18. Members of local government and municipal authorities.
19. Religious leaders.

a) Within the scope of this Law, the following are also considered Politically Exposed Persons (PEPs): family members and persons closely associated with the individuals mentioned above, specifically:

1. The spouse or partner in a de facto union.
2. Relatives up to the third degree of collateral kinship, and in-laws up to the same degree, as well as their respective spouses or partners in a de facto union.
3. Individuals with recognized close personal relationships.
4. Individuals with recognized close corporate or business relationships.

5. namely:

(i) Any natural person who is publicly known to be a joint owner of a legal entity with the holder of a high-ranking political or public position, or who maintains close business relations with said person

(ii) Any natural person who owns shares or voting rights in a legal entity, or

owns the assets of a collective interest center without legal personality, that is publicly known to have the politically exposed person as its sole beneficial owner.

«High-Risk Profile Persons (HRPP)» - Individuals who are more likely to be involved in illegal activities that may lead to money laundering or terrorist financing. These persons, due to their characteristics or circumstances, represent a greater risk to the Bank.

«Beneficial Owner» - The natural person(s) who:

Ultimately owns or controls a legal entity and/or the natural person on whose behalf a transaction is conducted.

(i) ultimately exercises effective control over a legal entity or legal arrangement, in cases where ownership/control is exercised through a chain of ownership or indirect control.

(ii) ultimately holds ownership or direct/indirect control over the company's share capital or voting rights, except for publicly listed companies on regulated markets subject to disclosure requirements aligned with international standards.

(iii) has the right to or actually exercises significant influence over or control of the company, regardless of the ownership level.

b) In the case of legal entities managing or distributing funds, the beneficial owner is the natural person(s) who:

(i) benefit from the assets, where future beneficiaries have already been determined.

(ii) are considered to be the category of persons in whose main interest the legal entity was established or operates, where beneficiaries have not yet been determined.

(iii) exercise control over the assets of the legal entiy.

«Shell Bank»: A bank that is legally incorporated and licensed in a jurisdiction but has no physical presence there and is not affiliated with a regulated financial group under effective supervision.

«False Positive»: Occurs when there is no actual name match during the screening process of a client/entity.

«Positive Hit»: Occurs when there is a confirmed name match during the client/entity screening process.

«Hit»: A potential name match found during screening against sanctions lists, indicating a person(s) under sanctions.

«Enhanced Due Diligence (EDD)»: A set of additional due diligence measures applied when a higher risk of ML/TF/P is identified during the client risk scoring process.

«Terrorist Financing»: Involves the provision, deposit, distribution, or collection of funds, by any means, directly or indirectly, with the intent to use them or knowing they will be used, in whole or in part, for planning or executing any terrorist act.

«Proliferation of Weapons of Mass Destruction»: The process by which an agent provides, collects, or holds funds or assets of any type or origin, whether lawful or unlawful, including products or rights that can be converted into funds used for the proliferation of weapons capable of causing mass casualties in a single use — nuclear, chemical, or biological weapons, and related materials.

«Money Laundering»: The participation in any activity intended to acquire, possess, use, convert, transfer, conceal,

or disguise the nature, origin, location, disposition, movement, or true ownership of assets, knowing that such assets derive from or are related to criminal activity.

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

1. **Placement** – The introduction of illicit funds (usually in cash) into financial or non-financial institutions.
2. **Layering** – The process of separating illicit proceeds from their source through complex layers of financial or commercial transactions to obscure their origin and enhance anonymity.
3. **Integration** – The re-entry of laundered funds into the economy, appearing as legitimate income or assets.

Financial institutions may be used at any stage of the money laundering or terrorist financing process.

CHAPTER III – AML/CFT-P RISK PREVENTION PROGRAM

3.1. AML/CFT-P Risk Management System

The Anti-Money Laundering, Counter-Terrorism Financing, and Proliferation Risk Management System consists of the appropriate identification, assessment, and mitigation of money laundering and terrorist financing risks to which BIR is exposed in the course of its activities. This enables effective monitoring of its customers and transactions and facilitates the efficient prevention and detection of potentially suspicious operations.

The AML/CFT/CPF Risk Management System of BIR includes the following components:

- Risk Assessment Model (Scoring – KYC).

- Client and Transaction Screening Systems.
- Internal Policies for AML/CFT/CPF Risk Management.
- Governance Model.
- Internal Processes and Procedures.
- Established Risk Mitigation Controls.
- Management Information.
- Awareness and Training Plan.

BIR formally appoints a person responsible for the Compliance function, tasked with ensuring compliance with the obligations related to the prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction. This person is officially referred to as the Compliance Officer.

The Compliance Officer's responsibilities include, but are not limited to:

- Coordinating and monitoring the effective implementation of policies, procedures, and controls to manage the risks of money laundering, terrorist financing, and proliferation financing to which the financial institution is or may become exposed.
- Participating in the design and issuing prior opinions on policies, procedures, and controls aimed at preventing money laundering, terrorist financing, and proliferation financing.
- Continuously assessing the adequacy, effectiveness, and relevance of the AML/CFT/CPF policies and procedures and proposing necessary updates to the Board of Directors and the Audit and Internal Control Committee.
- Contributing to the development, monitoring, and evaluation of the institution's internal training policy.
- Ensuring the centralization of all relevant information coming from different business units of the Financial Institution.
- Reporting, without internal or external interference, the operations referred to in Article 17 of Law no. 05/20, of 27 January, to the Financial Intelligence Unit (UIF)

- Acting as the liaison with supervisory and law enforcement authorities, especially in fulfilling the reporting obligations set out in Article 17 of Law no. 05/20 and ensuring compliance with all other reporting and cooperation requirements.
- Supporting the preparation and execution of AML/CFT/CPF risk assessments related to customers and transactions, based on key risk assessment factors consistent with the best national and international regulatory and legal practices.
- Coordinating the preparation of reports and other information required to be submitted to the National Bank of Angola (BNA) on AML/CFT/CPF matters.
- Ensuring that all Bank employees, regardless of the nature of their contract, are aware of: i) the identity and contact details of the Compliance Officer; ii) the procedures for reporting suspicious conduct, activities, or transactions to the Compliance Officer.

To this end, the Bank ensures that the selection of staff for the Compliance function is based on high ethical standards and rigorous technical requirements. The Bank also notifies the National Bank of Angola of the identity and contact details of the appointed Compliance Officer, as well as any subsequent changes, as soon as they occur.
The AML/CFT/CPF Risk Management System is based on a risk-based approach, allowing the Bank to identify customers that present a higher risk and to adjust due diligence measures and the level of monitoring according to the risk assessed level.

To this end, the Bank has developed mechanisms that enable the proper assessment of risk in accordance with the intrinsic characteristics of its customers and their activities, as well as effective monitoring of established business relationships. This facilitates the effective mitigation of risk, and the prevention and detection of money laundering, terrorist financing, and proliferation financing crimes.

The risk-based classification of the Bank's customer portfolio determines the application of tailored measures and controls, enabling a deeper understanding and ongoing monitoring of behaviors and transactional activity of higher-risk clients, based on their

specific characteristics, business segments, and subscribed product

Customer risk classification further determines the level of due diligence to be applied.

the frequency of information update and risk re-assessment processes; and the need to implement additional monitoring measures for transactional activity.

CHAPTER IV – GENERAL POLICIES FOR AML/CFT-P COMPLIANCE

4.1. AML/CFT-P Risk Management Policy

The BIR's AML/CFT Risk Management Policy aims to identify the general principles that underpin the Bank's risk management system, outline the risk mitigation factors implemented, and reflect BIR's risk appetite based on the identified risks.

4.2. Customer Acceptance Policy

As part of the establishment of business relationships, all necessary information and documentation must be collected to reasonably rule out the classification of clients under any prohibited categories. The customer acceptance policy is mandatory without exception and applies to all customer segments. It must be strictly observed by all structural units of the Bank.

4.2.1. Prohibited Customers

Based on the BC/FT/P (Money Laundering, Terrorist Financing, and Proliferation Financing) risk classification, the institution shall not establish business relationships with the following categories of clients:

Individuals or entities listed on any official sanction's lists.

- Individuals or entities for whom there is information suggesting a potential link to illicit activities.
- Clients engaged in businesses whose legitimacy or source of funds cannot be reasonably verified.

- Accounts involving anonymous clients or clients using clearly fictitious names.
- Clients who refuse to provide the requested information or documentation.
- Legal entities whose ownership or control structure cannot be determined.
- Casinos or betting entities not officially authorized.
- Financial institutions operating in jurisdictions where they have no physical presence (so-called "shell banks") and that are not part of a regulated financial group.
- Entities registered under a name that does not match their business profile or corporate purpose.
- Entities registered under a corporate name that differs from the nature of their actual activities or services.

4.3. Customer Acceptance Requiring Prior Authorization

According to the BC/TF/P Risk Management Model defined by Banco BIR (as outlined in the BC/TF Risk Management Policy – Chapter V), the following types of clients shall only be accepted with prior authorization from the Management Body:

- Clients classified as **High Risk**
- Clients classified as **PEPs / Politically Exposed Persons**
- **Non-profit organizations**
- **Casinos and/or Gambling Houses**

4.4. Governance Model

The Governance Model includes the following components:

- Governance structure, including the assignment of responsibilities and competencies, and the definition of reporting lines, ensuring the principle of segregation of duties.
- Adequacy of technical and human resources, as well as technological support; and
- Management information, to ensure effective monitoring and control of the

AML/CFT Risk Management System.

Within the scope of the AML/CFT Risk Management System, the following structural units of BIR are involved:

Structural Unit	Key Areas of Intervention
Board of Directors (BoD) / Executive Committee (EC)	• Definition of the AML/CFT Risk Management Strategy. • Approval of internal policies, processes, and procedures. • Approval of the level of exposure to AML/CFT risk, based on the results obtained through the application of the KYC scoring model to the BIR customer portfolio. • Approval of entities classified as High Risk and PEPs, according to the defined approval hierarchy. • Decision on reporting suspicious transactions, following communication submitted by the Compliance Department (DCOMP); • Analysis of the results obtained from assessments conducted under the AML/CFT Risk Management model. • Ensure the effective implementation of identified corrective measures. • Ensure BIR's compliance with regulatory requirements related to the prevention of AML/CFT offenses;

	• Ensure that the Compliance Department (DCOMP) has the necessary human and technical resources to effectively perform its duties.
Compliance Department (DCOMP)	• Identification and assessment of existing ML/TF risks. • Ongoing monitoring to identify the need for any adjustments to the ML/TF prevention program. • Review of the ML/TF Risk Assessment Model. • Updating processes, procedures, and controls to mitigate identified risks. • Implementation of the defined internal processes and procedures. • Issuing opinions on entities classified as High Risk and PEPs. • Analysis of entity and transaction screening results. • Analysis/investigation of potentially suspicious transactions. • Ongoing monitoring of customers and transactions based on the identified risk level and defined alerts. • Reporting suspicious transactions to the Financial Intelligence Unit (FIU); • Preparation of management reports related to the ML/TF Risk Management Model and submission to the Executive Committee / Board of Directors. • Participation in the definition, monitoring, and

	evaluation of the Bank's • internal training policy on ML/TF prevention. • Within the internal control system, ensuring that business units comply with the policies, tools, and procedures defined in the area of ML/TF prevention;
Internal Audit Department (IAD)	• Assessment of the adequacy and effectiveness of the model, policies, processes, procedures, and controls in place. • Identification of deficiencies and proposal of corrective measures to be implemented.
Information Systems Department (DSI)	• Implementation of technological equipment. • Provision of tools to the Branch Network and control areas. • Extraction of necessary information from the Bank's systems for the production of reports by the Compliance Department (DCOMP). • Continuous monitoring of IT systems. • Implementation of necessary changes to the information systems in order to meet the functional, business, and reporting requirements defined within the scope of the AML/CFT Risk Management System. • Ensure the proper functioning and

	maintenance of the KYC Scoring tools developed for customer onboarding. • Ensure the regular operation of the screening tool against Sanctions Lists, Country Lists, Politically Exposed Persons (PEPs) Lists, and any other internal or external lists adopted by Banco BIR;
Structural Unit	**Key Areas of Intervention**
Commercial Network: Branches, Private Banking, Corporate Banking	• Implementation of customer identification and due diligence processes and procedures. • Collection of required information and documentation, in accordance with internal regulations and applicable legal and regulatory requirements. • Knowledge and ongoing monitoring of customers. • Conducting the initial AML/CFT risk assessment through the customer onboarding process. • Proper completion of the "Know Your Customer" form. • Execution of the duty to refuse and duty to

	abstain. • Reporting potentially suspicious transactions to the Compliance Department (DCOMP). • Collaborating with DCOMP whenever additional customer or transaction information is required. • Actively participating in training sessions and whenever summoned for that purpose.

4.5. Management Information

The Compliance Department must produce management reports with the purpose of providing statistical information related to the monitoring of the AML/CFT Risk Management System, as well as analyses conducted in compliance with the duties of examination, due diligence, and reporting.

The reports produced in the context of monitoring the AML/CFT Risk Management System must be formally submitted for review and approval by the Board Member responsible for the Compliance portfolio (quarterly reports), the Executive Committee (monthly and/or quarterly reports) and the Board of Directors (annual reports).

The structure, frequency, and content of the management information reports are detailed in the Management Information Reporting Procedure. This document also identifies the responsible stakeholders and the Information Technology systems involved.

CHAPTER V – PRINCIPLES AND PROCEDURES FOR AML/CFT-P COMPLIANCE

5.1. Customer Identification Obligation[1]

BIR is subject to the duty of identification and must require the identification of its customers, their representatives, and beneficial owners whenever:

A business relationship is established.

Occasional transactions are carried out in an amount equal to or greater than the equivalent of USD 15,000.00 (Fifteen thousand United States dollars) in national currency, whether the transaction is conducted through a single operation or through multiple operations that appear to be related.

There are suspicions that the transactions, regardless of their value, may be connected to the crime of money laundering or terrorist financing, taking into account the nature of the transaction, its complexity, or its atypical nature in relation to the customer's profile or activity.

There are doubts regarding the authenticity or accuracy of the customer identification data.

[1] **Protection of personal data**: The processing of personal data, as well as the files — whether automated or not — created to comply with the current regulations on money laundering and terrorist financing, shall be subject to the provisions of the applicable law on personal data protection.

In fulfilling the duty of identification, it is essential to comply with all requirements set out in Notice no. 2/2024 of 22 March, issued by the National Bank of Angola, as well as those established in the current account opening checklist.

Verification of any elements required for account opening may only be carried out upon presentation of original documents or certified copies thereof.
The opening of anonymous accounts or accounts under fictitious names is strictly prohibited.

In this regard, all business units of BIR — with particular responsibility falling on the Commercial Directorate — must ensure a thorough and effective understanding of their customers, representatives, and beneficial owners, as well as of their respective activities. They must:

- Confirm and document the true identity of all customers with whom a commercial relationship is established, including their representatives and beneficial owners.
- Confirm and document any additional information gathered on the customer, representatives, and beneficial owners, in accordance with the money laundering and terrorist financing risk assessment model.
- Ensure that BIR's business units do not conduct transactions with individuals or entities whose identities cannot be verified, who fail to provide the required information, or who submit false or significantly inconsistent information that cannot be clarified.
- Require supporting documentation for the powers of individuals authorized to conduct financial transactions on behalf of the customer and identify those individuals and determine their relationship with the customer.
- Determine the true identity of the person with whom the relationship is being established, the account is being opened, or a significant transaction is being executed — that is, the beneficial owners — when the customer acts on behalf of third parties, or whenever there is doubt that the customer is acting in their own

name.

In cases where the customer is a legal person or an unincorporated collective

- Interest entity — or whenever there is knowledge or reasonable suspicion that the customer is not acting on their own behalf — the obliged entities must obtain from the customer information that enables the identification of the beneficial owner. Appropriate verification measures must be taken, in accordance with the level of money laundering or terrorist financing risk.

5.2. Due Diligence Requirement

Within the scope of the duty of due diligence, and without prejudice to the fulfilment of the identification duty, the Bank must apply enhanced due diligence measures — such as requesting declarations of the origin and destination of funds, as well as updated Know Your Customer (KYC) information — in relation to customers and transactions which, by their nature or characteristics, may present a higher risk of money laundering or terrorist financing.

2 Under the terms of Law No. 5/20, of 27 January, a "Beneficial Owner" is understood to mean the natural person or persons who:

1) Ultimately hold a share in the capital of a legal entity or control it and/or are the person on whose behalf the transaction is being conducted.
2) Ultimately exercise effective control over a legal entity or an entity without legal personality, in cases where capital holdings or control are exercised through a chain of ownership or through indirect control.
3) Ultimately, own or control, directly or indirectly, the share capital or voting rights of a legal entity, which is not a company listed on a regulated market subject to disclosure requirements in line with international standards.
4) Have the right to exercise, or who actually exercise, significant influence or control over the company, regardless of the level of ownership.

ii. In the case of legal entities that manage or distribute funds, the individual or individuals who:

1) Benefit from its assets when the future beneficiaries have already been identified.
2) Are considered the category of persons in whose main interest the legal entity was established or carries out its activity when the future beneficiaries have not yet been determined.

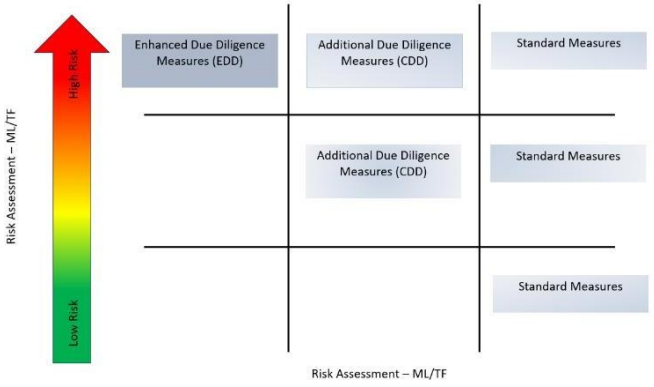
3) Exercise control over the assets of the legal entity;

5.3. Risk-Based Approach

Considering that each customer carries a different level of risk, the nature and extent of the due diligence measures to be applied depend on the risk assessment associated with each customer, the characteristics of the business relationship, the type of products or services subscribed to, as well as the transactions and the origin and destination of the funds (Article 9 of Law No. 5/20, of 27 January, and Article 5 of Notice No. 2/2024, of 22 March).

Accordingly, based on the result of the risk assessment (Scoring – KYC) obtained during the account opening process or throughout the business relationship as a result of risk reassessment, additional information must be obtained about the customer, representatives or beneficial owners, and enhanced or supplementary due diligence measures must be undertaken (see Figure 1 below):

Figure 1 – Due diligence measures to be applied according to the level of risk



5.4. Enhanced Due Diligence

The internal procedures for enhanced and additional due diligence are defined in the document **"Due Diligence Procedures for Entities and Customers."**

In addition to standard due diligence measures, enhanced due diligence must be applied to remote transactions, particularly those that may facilitate anonymity, to Politically Exposed Persons (PEPs) residing outside the national territory, to correspondent banking operations with credit institutions established in third countries, or to any others designated by the BNA.

The specific due diligence procedures regarding correspondent banking relationships are detailed in the internal regulation **"Correspondent Banking Procedures Based on ML/TF Risk,"** and the procedure for managing PEPs is outlined in the **"High-Risk Customer Policy."**

5.5. Ongoing Monitoring Obligation

For the purposes of ongoing monitoring of the business relationship, and depending on the assessed risk of money laundering and terrorist financing, the following information must be requested:

- Nature and details of the business, occupation, or employment.
- Record of address changes.
- Source of funds to be used in the business relationship.
- Origin of initial and ongoing income.
- Various relationships between signatories and their respective beneficial owners.
- The above information is collected through the Customer Account Opening Form. For entities classified as Medium or High Risk, additional information is gathered and recorded in the Know Your Customer Form **("KYC Form").**

The commercial departments and the Compliance Department (DCOMP), as well as other business units of the Bank, must maintain continuous monitoring of business relationships and review transactions carried out, verifying their consistency with previously obtained information and the entity's risk profile.

The risk assessment model establishes procedures for the periodic verification of the accuracy and currency of information related to the entities, based on materiality and risk criteria. Specifications regarding the continuous monitoring of customers are detailed in the internal regulation **"Ongoing Customer Monitoring".**

5.6. Duty to Refuse

BIR employees must refuse to carry out transactions whenever the customer fails to provide identification for themselves, their representative, or the beneficial owner, as well as in situations where no information is provided about the customer's control structure, the nature and purpose of the business relationship, and the origin and destination of the funds.

In cases where, due to reasons attributable to the customer, it is not possible to complete the identification procedure, identity verification, or to apply simplified and/or enhanced due diligence, the Bank shall act in accordance with Article 15 of Law no. 05/20, of 27 January, and terminate the business relationship as follows:

a) Restrict any movement of funds or other assets associated with the business relationship, including via any remote communication channels.
b) Contact the customer within a maximum of thirty (30) days to request that they indicate an account for the return of funds or appear in person at the Bank to carry out the return procedures as defined by the Financial Institution; and
c) Retain the funds or other assets, keeping them unavailable until their return is possible

If, upon contact with the Bank, the customer provides the missing elements that led to the decision to terminate the business relationship, and no suspicions arise, the request is re-evaluated and all legally required identification and due diligence procedures are carried out.

5.7. Duty to Abstain

The duty of abstention consists in the prohibition from executing any transaction related to a particular customer when it is found that a transaction raises reasonable suspicion of being connected to the commission of money laundering, terrorist financing, or

proliferation financing crimes (ML/TF-P).

If BIR Bank employees suspect that a given transaction may be related to ML/TF-P activities, they must refrain from executing the transaction and immediately notify the Compliance Department. The Compliance Department must then analyze the transaction in accordance with the **"Procedures for the Analysis of Transactions with ML/TF Risk"** set out in **Chapter VI** of this Policy. If there are grounds to support the suspicion, the transaction must be reported to the Financial Intelligence Unit (FIU).

The transaction must remain suspended until the FIU issues a decision, which must be communicated in writing or through any other means. The FIU may order the continued suspension of the transaction.

However, the transaction may proceed if the suspension order is not confirmed by the FIU within three (3) days from the date the Bank reported the transaction.

If abstention is not possible, or if after consulting the FIU it is determined that abstention could jeopardize a future investigation related to money laundering or terrorist financing, the transaction may be executed, provided that the Bank immediately submits all relevant information regarding the transaction to the Financial Intelligence Unit.

5.8. Duty to Examine

The duty of examination refers to the obligation to carefully analyze any conduct, activity, or transaction whose characteristics make it particularly likely to be associated with the crimes of money laundering (ML), terrorist financing (TF), or any other crime, especially in cases involving:

- The nature, purpose, frequency, complexity, unusualness, and atypicality of the conduct, activity, or transaction.

- The apparent lack of economic rationale or legitimate purpose behind the conduct, activity, or transaction.
- The amount, origin, and destination of the funds involved.
- The payment methods used.
- The industry sector and behavioral profile of the parties involved.
- The type of transaction or product that could particularly favor anonymity.

The assessment of the degree of suspicion raised by a behavior, activity, or transaction does not require documentary evidence confirming the suspicion. Instead, it stems from the analysis of the specific circumstances, based on 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 Transactions to Competent Authorities

BIR is obligated to report transactions in the following circumstances:

- Whenever it knows, suspects, or has sufficient reason to suspect that a transaction has occurred, is underway, or has been attempted that may constitute the crime of money laundering or terrorist financing;
- Cash transactions in an amount equal to or greater than the national currency equivalent of USD 15,000.00 (Fifteen Thousand United States Dollars).
- Whenever, at the start or during the course of a business relationship, or prior to executing a transaction, the identity of a client—actual or potential—or any other person, group, or entity matches the identity of a person, group, or entity listed in any Sanctions List[3]

The specific duty to report also applies when transactions pose a particular risk of ML/TF/P, especially if they are associated with a country or jurisdiction subject to additional countermeasures enacted by the Angolan Government.

Regulatory authorities within the relevant sector may also require immediate reporting of

such transactions to the Financial Intelligence Unit (FIU) when the transaction amount is equal to or exceeds the local currency equivalent of USD 15,000.00.

Whenever the Bank's business units or staff submit suspicious activity or transaction reports to the Compliance Department, the department is strictly prohibited from disclosing any information—internally or externally—regarding the client or the transactions mentioned without respecting the duty of confidentiality.

[3]**« Designated persons, groups or entities »,** designated persons, groups or entities (Directive 03/DSI/2012 – BNA):

By the United Nations Sanctions Committee pursuant to UN Security Council Resolution No. 1267, through the updated List issued by said Sanctions Committee;

By the Sanctions Committee pursuant to United Nations Security Council Resolution No. 1988, which maintains an updated list of persons, groups, and entities associated with the Taliban that pose a threat to the peace, stability, and security of Afghanistan.

By any other Sanctions Committee established by the United Nations or another United Nations body that maintains lists of persons, groups, or entities associated with terrorism—including the financing of terrorism, terrorists, or terrorist organizations—with the purpose of applying restrictive financial measures; and

iii. By the national competent authority responsible for national designation and enforcement of restrictive measures, through a national list, in accordance with Law No. 1/12 of 12 January — Law on the Designation and Enforcement of International Legal Acts — whenever the designation concerns persons, groups, or entities associated with terrorism, including the financing of terrorism, terrorists, or terrorist organizations, with the purpose of applying restrictive financial measures.

5.10. Internal Procedure for Reporting Suspicious Transactions

The business unit that detects or carries out the suspicious transaction must immediately report it in writing, via email, to the Compliance Department for analysis and decision.

If the suspicion is confirmed, and after submission of the Incident Report to the attention of the Management, the communication to the Financial Intelligence Unit (FIU) must be carried out in accordance with the decision made by the Compliance Department.

The communication of transactions to the FIU must be done through electronic submission of the official forms via the FIU's website (GoAML), or, if the reporting entity lacks the

necessary technical resources, via email or postal mail.

- **Official FIU Form:**

Suspicious transactions must be reported through the submission of a Suspicious Transaction Report (STR), which must be completed in accordance with the corresponding STR Completion Guide, available on the websites of both the FIU and the National Bank of Angola (BNA).[4]

5.11. Reporting of Designated Persons and Entities

Whenever BIR becomes aware, suspects, or has reasonable grounds to suspect that the identity of a customer—whether actual or potential—or any other person, group, or entity involved in a business relationship or transaction corresponds to a designated person, group, or entity, it must report this fact to the Financial Intelligence Unit (FIU).

Designated persons and entities are identified through the screening process carried out during account opening and throughout the course of the business relationship.

- **Official FIU Form:**

Designated persons and entities must be reported through the submission of a Declaration of Identification of Designated Persons and Entities (DIPD), which must be completed in accordance with the respective "DIPD Completion Guide", available on the websites of the Financial Intelligence Unit (FIU) and the National Bank of Angola (BNA)[5].

[4,5] http://www.bna.ao/Conteudos/All/lista.aspx?idc=881&idl=1

5.12. Reporting of Cash Transactions

Cash transactions equal to or greater than the equivalent of USD 15,000.00, whether in local currency or a foreign equivalent, must be submitted daily and directly to the Financial Intelligence Unit (FIU) via the GoAML web platform, in XML format by the Compliance Department (DCOMP).

This type of reporting is mandatory and not dependent on any suspicion of money laundering or terrorist financing. The obligation applies regardless of whether the transaction is carried out as a single operation or through multiple operations that appear to be related.

Furthermore, the splitting or structuring of transactions to avoid triggering thresholds for reporting or systematic records is recognized as a method that may be used to evade the applicable anti-money laundering and counter-terrorist financing regulations and must be monitored accordingly.

5.13. Document Retention Obligation

BIR Bank must retain, for a minimum period of ten (10) years, all records, which must include:

- Copy of documents or other technological records that prove compliance with identification and due diligence obligations.
- Records of national and international transactions that are sufficient to allow the reconstruction of each operation, in order to provide, if necessary, evidence in a criminal proceeding.
- All documentation related to transactions carried out with correspondent banks.
- Record of the results of internal investigations, as well as copies of communications made by the financial institution to the Financial Intelligence Unit and other

competent authorities.

- Justification for the decision not to report to the Financial Intelligence Unit and other competent authorities provided by the Compliance Officer.
- Copy of all commercial correspondence exchanged with the customer.
- Recommendations on anti-money laundering and counter-terrorist financing (AML/CFT) matters issued by the Internal Audit Department (DAI).

Additionally, BIR must retain, for a period of five (5) years, copies of documents or records related to training provided to its employees, including the Management and Administrative Bodies.

Such documentation must be properly stored to ensure it can be easily located and its confidentiality preserved.

The archiving system must ensure proper management and availability of the documentation, both for internal control purposes and to enable timely responses whenever requested by the BNA, the Financial Intelligence Unit (FIU), and other competent Authorities.

5.14. Duty to Cooperate

The Bank, through the Compliance Department, must promptly cooperate with the National Bank of Angola and the Financial Intelligence Unit when requested, by providing information on certain operations carried out by customers and submitting the documents related to specific transactions.

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

Requests for information, official letters and/or notifications relating to ML/TF-P crimes addressed to the Bank by courts or any other authority must be forwarded to the Secretariat of the Administration, which must inform the Executive Committee and the Compliance

Department.

All such requests for information, official letters, and/or notifications received from Competent Authorities in connection with ML/TF-P crimes must be registered with the date of receipt in a database maintained by the Compliance Department for this purpose. Likewise, official responses issued by the Bank must be recorded in the same database. The following information must be recorded, where applicable:

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

In addition to the physical filing of the documents received and issued, they must also be digitized and stored electronically by the Compliance Department (DCOMP). All official letters sent by BIR to the Competent Authorities regarding ML/TF-P crimes must be signed by at least two (2) Executive Directors. Responses sent to the requesting entity must comply with the following principles and communication formats:

- Submission via email: an acknowledgment of receipt must be included.
- Hand delivery: ensure the recipient signs a copy as proof of receipt.

5.15. Duty of Confidentiality

Communications on this matter are strictly confidential.

The Bank, members of its corporate bodies or those performing functions of management, administration, or leadership, its employees, agents, and other individuals providing services to the Bank—whether on a permanent, temporary, or occasional basis—are prohibited from disclosing to the customer or any third party that legally required communications have been made or that a criminal investigation is underway.

Non-compliance with this rule is considered a very serious offence for those held responsible.

5.16. Control Obligation

BIR must implement internal policies and procedures that are appropriate for complying with legally established obligations, particularly in the areas of internal control, risk assessment and management, and internal audit, in order to effectively prevent and detect the crime of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (ML/TF-P).

5.17. Training Obligation

The Bank must ensure ongoing training on the prevention and detection of money laundering and terrorist financing for its employees, tailored to their specific needs—particularly new hires, front-office staff, supervisory staff, and those in Compliance, Audit, Risk Management, and Commercial Management functions.

The Compliance Department (DCOMP) will develop the training activities in coordination with the Human Capital Department (DCH), and a record of all training sessions will be maintained, documenting the date, location, duration of each course, and names of participants.

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

These measures must include specific and regular training activities, suitable for the banking sector, that enable Bank employees to identify transactions that may be related to ML/TF-P crimes and act in accordance with applicable legislation.

Accordingly, specific training activities are included in the "Annual Training Program", aimed at Bank staff—including members of the Management and Executive Boards—taking into account international standards, current Angolan legislation and regulations on the matter, as well as guidelines issued by the Financial Intelligence Unit (FIU).

Training activities must include, at a minimum, content on the following topics:

- The Bank's internal policies and regulations.
- Internal processes and procedures for identification, due diligence, transaction reporting, abstention, and refusal.
- Internal control systems and risk assessment related to ML/TF/P prevention.
- Internal templates and forms.
- ML/TF/P risk management model.
- Trends in activities/practices associated with ML/TF/P;
- Typologies of suspicious transactions.

Regardless of the general training plans, the Compliance Department must keep all employees permanently informed of any regulatory changes in this area, as well as any new methods, techniques, or procedures that are identified as potentially being used in the commission of ML/TF-P crimes.

CHAPTER VI – IDENTIFICATION, DETECTION, AND MONITORING OF TRANSACTIONS

The process of identifying/detecting transactions and monitoring aims to track the transactional activity of customers (during and after the execution of transactions), with the objective of identifying behaviors and transactions suspected of involving Money Laundering, Terrorist Financing, or Proliferation Financing (ML/TF/P).

The monitoring performed must focus on both individual transactions and on transaction flows that form behavioral patterns/transactional profiles of customers. This includes the historical analysis of transactions carried out, as well as the analysis of transaction typologies that carry a higher risk or are more vulnerable to ML/TF/P.

6.1. Identification and Detection of Suspicious Transactions and Monitoring

The Compliance Department, as well as the commercial areas and other business units, must implement appropriate procedures for the control and analysis of transactions suspected of being related to Money Laundering, Terrorist Financing, or Proliferation Financing (ML/TF/P), with the aim of identifying and reporting such transactions to the Competent Authorities.

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

i. **Detection of outliers compared to the behavioral pattern/transactional profile of the Entity:**

For this purpose, the specific characteristics of the transactions and the respective parties involved should be taken into account, such as:

- Type / Nature and complexity of the transactions;

- Atypicality within the client's normal business activity: it should be verified whether the transaction(s) are disruptive compared to the Client's typical behavioral pattern, taking into account the following factors:
  - Amounts involved.
  - Means of payment used.
  - Frequency / Speed.
  - Countries and jurisdictions involved in the transaction: it should be verified whether the transaction(s) involve countries, territories, or regions different from those declared by the Entity during the account opening.
- Financial / asset situation of the parties involved: it should be verified whether the type of activity and/or the transaction amounts of the Entity align with the expected activity declared at the time of account opening.
- Client's Business Sector: it should be verified whether any transaction(s) fall outside or are unusual for the typical scope and nature of that type of client (e.g., considering the purpose of the business relationship, the account purpose, and the business sector).
- Origin and destination of the funds: the justification for the origin and destination of the funds should be analyzed, verifying whether any cash deposits raise suspicion or irregularity (including the initial deposit).
- Economic rationale for the transactions: it should be verified whether any transaction(s) show a purpose or characteristics that deviate from the standard pattern normally associated with that type of transaction.

ii. Classification of transactions within a typology of suspicious operations

- In the identification and detection of suspicious transactions, the typologies of suspicious transactions disclosed by International Organizations, Supervisory Authorities, and other Entities (**Annex II A** of this policy) must be taken into account.

iii. Relationship and aggregation of transactions

- This consists of detecting suspicious transactions through the aggregation or association of transactions carried out by Customers and related parties.

iv. Filtering against Sanctions Lists / Watchlists

- Identification of suspicious transactions through the screening of parties involved (originators / beneficiaries), as well as the countries, jurisdictions, or territories of origin and destination of the transactions.

The analysis and investigation of suspicious transactions may be triggered through the following mechanisms:

- **Identification and detection of suspicious transactions by the Compliance Department**
  - through continuous monitoring of entities and accounts.
- **Identification and detection of suspicious transactions by the Commercial Network**
  - through direct interaction with customers via front-office and other business units.
- **Enhanced monitoring of Entities**
  - through the ongoing oversight of high-risk customers.

6.2. Detection of Suspicious Transactions by the Compliance Department

For the purposes of identifying and detecting potentially suspicious transactions, BIR has defined risk parameters and indicators, which are used as criteria for selecting transactions and are subject to ongoing analysis by the Compliance Department.

The Compliance Department must analyze transactions that trigger "alerts" due to their alignment with the defined risk parameters, seeking to determine whether there are any indications of suspicion or whether the transactions fall within the customer's normal activity.

When analyzing transactions, the Compliance Department must take into account the profile of the parties involved and the characteristics of the transactions, as described in the previous section.

If the transaction is deemed consistent with the behavioral pattern/transactional profile of the Entities, the alerts shall be closed. The conclusion of the transaction analysis must be documented in writing, with justification for closing the alerts. If the transactions present well-founded grounds for suspicion, a "Case" must be opened, and further due diligence must be conducted.

6.3. Detection of Suspicious Transactions by the Commercial Structure (Front Office) and Other Business Units

All business units must apply monitoring measures to the customer relationship, including the scrutiny of transactions carried out, in order to ensure they are consistent with the Bank's knowledge of the Entity and its commercial and risk profile, including the origin and destination of the funds involved.

In identifying and detecting suspicious transactions, the typologies of suspicious operations listed in Annex II – A of this policy must be taken into account.

Business units must follow the internal procedures that establish the steps to take when there is a need to report suspicious transactions. In order to ensure compliance with applicable legislation, the Compliance Department carries out the necessary analysis/investigation and, if there are grounds for suspicion, submits the appropriate reports to the competent Authorities (see point 15 of Chapter V).

6.4. Monitoring of Entities (High Risk, PEPs, Entities Flagged 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 Compliance Department must conduct an analysis of the transactional activity of the following Entities:

- **Entities classified as High Risk:** must be subject to monitoring, tracking the monthly history of transactions (type, amounts, frequency, volume, complexity, destination, etc.) for a period of six (6) months after the beginning of the business relationship.
- **Entities classified as High Risk and that are PEPs (Politically Exposed Persons):** must be monitored by tracking the monthly history of the type, amounts, and volume of transactions they carry out, for a period of one (1) year.
- Customers who have carried out transactions with signs of suspicion, but whose review process was concluded with the application of a monitoring measure, without being reported to the Competent Authorities. In these cases, the Compliance Department must monitor the clients' activity monthly for a period of three (3) months;
- Individuals or entities referenced by Judicial or Law Enforcement Authorities, the Financial Intelligence Unit (UIF), or the National Bank of Angola (BNA), during the period and at the frequency determined by the competent authority;
- Entities referenced in publicly known situations, whenever it is considered that they present an increased risk of ML/FT (Money Laundering / Terrorist Financing).

The declassification of Entities from enhanced monitoring, applying risk-based criteria, may occur under the following circumstances:

- After the monitoring period, if the monitoring is officially closed If the customer is reclassified as Medium or Low Risk during a risk reassessment, and the Bank already has a sound understanding of the customer's transaction patterns.

6.5. Transaction Investigation by the Compliance Department

The Compliance Department must analyze transactions that triggered an alert and, if there are grounds for suspicion, must open a "Case" and carry out additional investigation procedures.

The investigation must consider, as an indicative list, potentially suspicious transactions

(Annex II-A), taking into account the specific characteristics of the customer and their transactional activity, namely:

- Nature of the entity (Individuals / Self-Employed; Corporate and Institutional).
- Risk profile of the parties involved in the contract.
- Transaction profile / behavioral pattern of the Entity.

The investigation process also includes:

- Searches in public and restricted sources to assess the credibility and currency of available information, the integrity of the entities involved, the financial and economic data of the entity or the sector in which it operates, as well as identifying possible group relationships between counterparties.

- Obtaining supporting documentation for the transactions from other business units, as well as additional clarifications to support the investigation's conclusions.

If the alert relates to contracts previously flagged with the same risk typology, the analysis process follows the approach described above, with particular attention given to:

- Validation and potential update of previously gathered information, particularly regarding personal data, nature of the contract, and account ownership.
- Any significant changes to the transaction profile compared to the previous analysis.

After conducting the investigation, the Compliance Department issues an **"Assessment/Incident Report"**, which is submitted to the Executive Committee (after review by the Head of Compliance Department) in the following situations:

i. Whenever the investigation result is **"Case closed with confirmation of suspicion"** and one of the following measures is proposed:
   a. Reporting the customer to the competent Authorities; and/or

b. Closing the account.

i. When the case involves high-risk entities and/or PEPs (Politically Exposed Persons).

ii. When the transactions under investigation involve entities flagged by the competent Authorities.

The Assessment/**Incident Report** must contain, at a minimum, the following information:

Origin of the analysis/incident:

- Identified by the Compliance Department – alert analysis.
- Identified by Commercial Departments or other Business Units.
- Identified by the Operations Department.
- Monitoring of Entities (high risk / PEPs); or
- Monitoring of Entities flagged by competent Authorities.

- **Entity Risk Level** (KYC Scoring).
- **Details of suspicious behavior/transaction and grounds for suspicion** (identification and justification of relevant facts associated with the account activity and identified counterparties).
- **Additional information gathered and evidence documentation** (details of searches and clarifications obtained that support the investigation's conclusions).
- **Conclusion of the analysis/incident**:
  - Case closed with no suspicion.
  - Case closed with no suspicion but subject to monitoring; or
  - Case closed with confirmation of suspicion.
- **If applicable, proposed measures:**
  - Reporting the client to competent Authorities.
  - Extending the monitoring period / subjecting to a defined monitoring period; and/or
  - Closing the account.

CHAPTER VII – CONTROL OF ENTITIES SUBJECT TO FINANCIAL COUNTERMEASURES

7.1. Entity and Transaction Screening

BIR must compare, at the beginning and throughout the business relationship or prior to executing a transaction, the identity of an actual or potential customer, or of any other person, group, or entity involved in a business relationship or transaction, against the data of persons, groups, or entities listed on Sanctions Lists, in order to determine whether their identity matches that of a designated person, group, or entity.

7.2. Entity Screening

Entity screening is carried out through Lexis Nexis Compliance Link/Eagle AML. According to these technological solutions, if there is a match or similarity between the identity of the Entity and that of a sanctioned person or entity, the Compliance Department must carry out additional due diligence measures to determine whether the match is confirmed or constitutes a False Positive.

7.3. Transaction Screening and Blocking

In the process of issuing and receiving SWIFT operations, as well as cross-border operations not automatically processed through the SWIFT system (e.g., documentary remittances), a sanctions list screening (UN, OFAC, and EU) must be carried out using the screening tool and prior to the execution of the transaction.

All transaction data must be screened, namely:

(i) Details of all parties involved – originator(s) and beneficiary(ies); and

(ii) Countries, jurisdictions, regions, or territories of origin or destination of the transactions.

If a hit is detected between the identification of the parties involved and the identity of a designated person or entity, the transaction must be placed on hold until the hit analysis is completed (to confirm the match)

Screening	Analysis	Parties involved
Direct False Positive: the hit results from information that is not directly related to the content of the transaction or its parties, but is rather a 'false' match (e.g. Angola - Portugal vs. Angola - Algeria)	• It is not necessary to carry out additional due diligence • The transaction must be duly justified and properly authorized within the screening process.	• Compliance Department
Potential False Positive: the hit is generated due to some element of the transaction effectively matching an entry on the Sanctions Lists; the transaction must be analyzed in detail.	• It is necessary to carry out additional due diligence **("Procedures for analyzing the result of the filtering matching")** It may be necessary to obtain detailed knowledge of the	• Compliance Department • Branch • Operations Departme nt (DOP)

	transaction, including requesting additional information from the Commercial Network, such as supporting documents for the transaction.	

- **Confirmation of the match:**

If the match is confirmed—that is, if the Compliance Department determines that the individual or entity involved is listed as a designated person or entity on a Sanctions List—the transaction must be blocked. Subsequently, the Compliance Department must report the matter to the Financial Intelligence Unit (FIU) by submitting a DIPD – Designated Persons and Entities Declaration.

In cases where the transaction involves a country, jurisdiction, region, or territory subject to financial countermeasures (such as financial sanctions or embargoes), in accordance with an official list issued by the competent authority, the transaction must likewise be blocked.

- **False Positive:**

If the Compliance Department concludes that the alert is a False Positive, it must authorize the Operations Department (DOP) to proceed with the execution of the transaction.

The outcome of the analysis must be properly recorded and justified by the Compliance Department (DCOMP), including either the rationale for allowing the transaction or the reason for refusal. This record must be maintained in the internal compliance database and in the screening tool.

7.4. Freezing of Funds and Economic Resources

The BIR is strictly prohibited from making funds, economic resources, or other related

services available, directly or indirectly, to persons, groups, and entities designated by the United Nations Sanctions Committee, pursuant to United Nations Security Council Resolution No. 1267, and by the competent national authority.

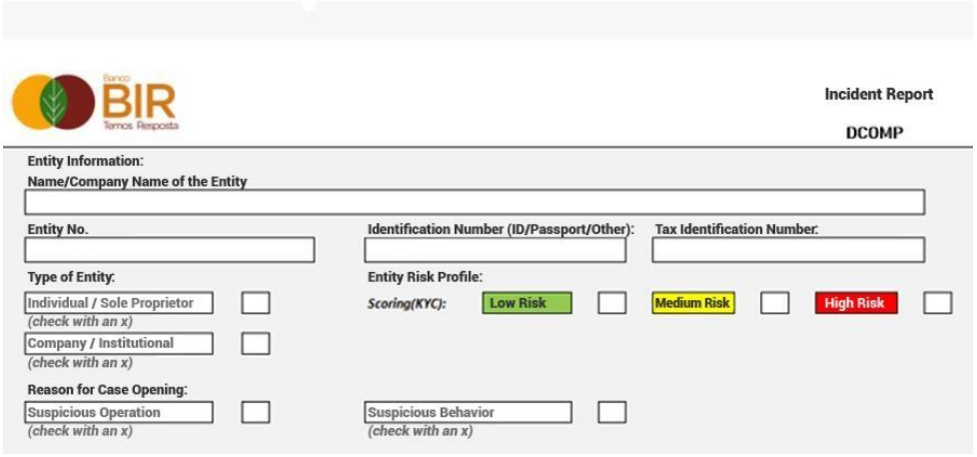
It is also required to immediately freeze, without prior notice, all funds or economic resources owned, held, or controlled—directly or indirectly, individually or jointly—by such persons, groups, or entities, and to report this action to the Financial Intelligence Unit (FIU) and the National Bank of Angola (BNA).

In accordance with the law, whenever BIR becomes aware of, suspects, or has reasonable grounds to suspect that the identity of the originator, beneficiary, or any other person/entity involved in a transaction match that of a designated person, group, or entity, it must refrain from executing the transaction. The Compliance Department must promptly report the matter to the Financial Intelligence Unit (FIU) and await official instruction regarding the terms of the asset freeze.

Until the instruction is received, the frozen funds or economic resources must be retained or kept under the control of the Bank.

CHAPTER VIII – ANNEXES

ANNEX I – "Incident Report" Template



Incident Report

DCOMP

Entity Information:

Name/Company Name of the Entity

Entity No.

Identification Number (ID/Passport/Other):

Tax Identification Number:

Type of Entity:

Individual / Sole Proprietor ☐ (check with an x)

Company / Institutional ☐ (check with an x)

Entity Risk Profile:

Scoring(KYC): Low Risk ☐ Medium Risk ☐ High Risk ☐

Reason for Case Opening:

Suspicious Operation ☐ (check with an x)

Suspicious Behavior ☐ (check with an x)

ANNEX II – Typology of Suspicious Transactions

This section aims to guide BIR employees in identifying and detecting transactions that may potentially be associated with money laundering and terrorist financing activities.
It presents a list outlining possible types of transactions that may be linked to money laundering.

A. Typology of Suspicious Transactions or Activities Identified by the Financial Intelligence Unit for Banks and Non-Bank Financial Institutions Involved in Currency and Credit [6]

In this sector, some indicators of transactions potentially related to ML/TF/PF (Money Laundering / Terrorist Financing / Proliferation Financing) include:

- A potential customer possessing a large amount of cash and opening multiple accounts or purchasing several products using variations of account names.

[6] Website of the Angolan Financial Intelligence Unit – "General Guidelines from the FIU"

- A potential customer carrying different foreign currencies and seeking to carry out currency exchange transactions as part of a broader operation.
- A customer structuring a transaction by breaking down the total value into several smaller operations in order to avoid triggering established reporting thresholds (smurfing).
- A foreign customer using alternative remittance services (ARS) to transfer significant amounts of money under the false pretext of sending funds to family abroad.
- A customer acquiring multiple similar financial products and transferring funds between them, supplementing with cash deposits.
- The high net worth of a customer being inconsistent with available information or with the nature of their business.
- A customer repeatedly using the same address while frequently changing the names of the persons involved.
- The customer's residential or business phone number being disconnected or found to be invalid when the institution attempts first contact shortly after account opening.
- A customer engaging in activity that is unusual for the type of individual or business in question.

B. Illustrative Catalogue of High-Risk Transactions for Credit Institutions

(i) Unusual and/or Frequent Changes in the Type or Nature of Payment Methods, Without Reflection in the Customer's Account:

- Currency exchanges involving high-denomination banknotes conducted by the same person or by several individuals acting in an apparently coordinated manner, either in a single transaction or in a series of low-value, spaced-out transactions (structured over time).
- Systematic or high-value acquisition of bearer payment instruments (such as bank drafts, e-money, or traveler's cheques) in exchange for cash, with no clear economic

justification or relation to the account activity.

(ii) Atypical Cash Transactions

- Significant increase in cash deposits made by any individual or company without any apparent reason, especially if such deposits are later transferred, within a short period, to a destination that is not normally related to the customer's activity or business.
- Clients transferring large amounts of money abroad, followed by instructions for cash payment.
- Cash deposits made in ways that avoid direct contact with bank staff.
- Large numbers of individuals making deposits into the same account without adequate explanation.
- Cash deposits being the primary source of funding for an account used to make payments for high-value or luxury goods (e.g. real estate, recreational boats, luxury vehicles, jewelry);
- Cash deposits in high-denomination notes where the type of business would normally deal with lower denominations.
- Significant cash deposits made directly into a credit card account, bypassing the current account and resulting in a positive balance in the card.

(iii) Unusual Activity in Bank Accounts:

- Any individual or entity whose accounts do not reflect normal banking or business activity but are used to receive or disburse significant amounts with no clear purpose or relation to the account holder and/or their business (e.g., a substantial increase in account activity).
- Clients holding accounts at multiple financial institutions in the same geographical location, especially where the bank is aware of regular consolidation of those accounts before a fund transfer request.
- Balance between deposits and withdrawals made on the same day or the day before.

- Corporate accounts making payments via transfers to a limited number of supposed suppliers, with the funds previously received in cash or via transfers from supposed clients, where the transaction amounts are similar or nearly identical.
- Large withdrawals from previously dormant/inactive accounts or from accounts that have just received unexpectedly large transfers from abroad.
- Significant increases in cash deposits or negotiable instruments made by law firms or companies using accounts opened in the name of third parties, particularly when these funds are quickly transferred between another client company and the fiduciary account.
- Accounts repeatedly credited with lottery winnings or gambling prizes.
- Repetitive and substantial tax refund and/or grant credits, particularly linked to trade in Angola, for clients who have no real business activity to justify them.
- Systematic issuance of bearer checks for amounts equal to or less than AOA 300,000 or the equivalent in foreign currency.
- Corporate clients who perform more transactions using cash than through other usual payment and collection methods for their type of commercial activity.
- Fund transfers between accounts of different companies with common individuals (directors, authorized persons, proxies) and/or shared addresses (registered office or mailing address);
- Opening of accounts in the name of new companies by the same individuals (directors, authorized persons, proxies) using addresses shared with other companies that appear to have ceased activity (shell companies);
- Incoming wire transfers from abroad where the originator's identity or account number is missing.
- Multiple cash or monetary instrument deposits made on the same date in amounts systematically just below the reporting threshold, especially if the documents have sequential numbering.
- Checks for large amounts credited in favor of third parties and endorsed to our client.

- Accounts in the name of minors or legally incapacitated individuals, where their representatives perform a high number of transactions or movements on said accounts.

(iv) Unusual Use of Fictitious Corporate Structures, Shell Companies, or Associations and Foundations with Little to No Real Activity:

- Transactions conducted through accounts of domestic companies owned by offshore entities incorporated in tax havens or high-risk jurisdictions, represented by independent professionals or other intermediaries, receiving high-value inbound transfers from abroad.
- Transactions carried out by domestic companies with legitimate economic activity that at some point receive transfers from tax havens or high-risk jurisdictions, under the justification of capital increases, shareholder loans, or similar operations, without any change in company management or legal representatives.
- Transactions involving recently incorporated companies with low share capital that, from inception, receive or send large international transfers to pay or receive computer hardware, mobile phones, or similar goods, and perform domestic transfers with a small number of counterparties from the same industry. These companies exhibit high transaction volumes over a short period before ceasing activity or being replaced by similar entities.
- Transactions by companies dedicated to vehicle imports, where funds primarily originate from large cash deposits or transfers from a network of related companies.
- Accounts opened in Portugal receiving small remittances ordered by individuals (usually from abroad), which individually are low-value but cumulatively substantial, without supporting transactional activity consistent with a business (e.g., payroll, purchase of raw materials, supplier payments). These funds are typically withdrawn in cash or transferred to tax havens or high-risk countries. This pattern is especially concerning in the investment services sector, particularly when the companies are unlicensed or fail to demonstrate actual investment activity or fund usage.

- Deposits into association or foundation accounts in the form of donations, fundraisers, or similar, in large amounts without any known disaster or campaign to justify the influx, with the majority of funds subsequently transferred to countries where the organization has no known operations;
- Movements in accounts held by legal entities (companies, foundations, associations, etc.) that perform outgoing payments but show no evidence of regular business expenses such as payroll, taxes, social security, utilities—despite significant fund movement, with no clear connection to the declared purpose of the account.

(v) Atypical, Unusual or Economically Unjustified International Fund Movements in Significant Amounts:

- Clients who fund their accounts via cash deposits and withdraw funds at ATMs, particularly abroad in countries known for drug trafficking. Cash deposits and withdrawals often occur simultaneously. Multiple cards linked to the same account are common. Withdrawals typically reach the daily transaction limits.
- Use of letters of credit and other trade finance mechanisms to move capital between countries where such trade is illogical for the client's declared business activity, often with last-minute changes to names, addresses, or payment locations of the letters of credit.
- Use of clearly falsified invoices, import documentation, insurance policies, or transport documents as justification for transfers received from abroad.
- Systematic use of over- or under-invoicing in international trade, reflecting prices substantially above or below market norms, as known from the institution's previous experience with similar transactions.
- Clients acting as informal remitters, collecting small amounts from compatriots and sending aggregated funds abroad.
- Fund movements by foundations or associations established in Angola and mostly composed of foreign nationals.
- Accounts held by individuals (usually foreigners) or companies (typically recently formed limited liability companies with minimal share capital), showing large cash

deposits followed by immediate high-value outbound transfers, maintaining low balances relative to total fund flow, backed by unverifiable economic activity.

- Accounts held by individuals (typically non-residents) who claim to be traders or mere intermediaries in foreign trade operations, in which large cash deposits or smaller cash deposits from various locations within the country are made directly, followed by immediate high-value transfers abroad. The beneficiaries of these transfers are usually distributor companies (typically based in Asian countries) dealing in a wide range of products with diverse economic activities.

(vi) Loans, credit lines or asset-based financing, with or without collateral:

- Customers who unexpectedly repay problematic loans or who repeatedly make early repayments of significant loan amounts, primarily using cash.
- Loans secured by third parties who appear to have no connection with the customer, where the loan ultimately goes unpaid and one of the guarantors ends up covering the debt.
- Loan applications backed by assets deposited with the financial institution or with third parties, where the origin of the assets is unknown or their value does not correspond to the customer's financial profile.
- Loan applications secured by assets held in offshore jurisdictions or high-risk countries.
- Applications for loans, credit lines, or asset financing by a customer who's officially declared repayment capacity (e.g., tax returns) is significantly lower than their actual financial capacity, with a substantial difference.
- Resident individuals or companies that finance themselves through loans or capital injections from abroad, where the lender is a private individual or a non-financial entity.

(vii) Politically Exposed Persons (PEPs) from high-risk countries, jurisdictions, regions, or territories:

- Accounts opened in Angola by individuals holding prominent political positions,

senior public roles, or similar (e.g., directors of state-owned enterprises) in generally non-democratic countries, including close family members, who receive funds from abroad to purchase high-value real estate or financial assets, or to make large deposits.

- Cash transactions or use of monetary instruments just below the thresholds that trigger mandatory reporting to authorities.
- High-value transactions that are inconsistent with the type of account, the customer's deposits, or their declared sources of wealth.
- Transactions conducted through illogical channels without an apparent purpose, except to conceal the identity of the fund owner.
- Requests for transactions to be executed on behalf of third parties;
- Transactions routed through jurisdictions with banking secrecy or through entities based in countries with weak client identification regulations.
- Transactions involving funds originating from accounts held at central banks or government-owned banks.
- Transfers to or from accounts held by other politically exposed persons.
- Inflows of funds by any means that are immediately transferred in similar amounts to institutions in third countries.
- Refusal to provide information on the purpose or economic rationale of incoming or outgoing transfers.
- Inquiries about how to avoid transaction reporting obligations to authorities or the reach of banking secrecy laws or other suspicious transaction reporting regulations.
- Offers of guarantees issued by offshore institutions or entities based in jurisdictions with impenetrable banking secrecy.

(viii) Lack of information, deliberate avoidance of contact with the BIR, or indifference to product profitability or advantages:

- Customers who do not act on their own behalf and who refuse to disclose the identity of the beneficial owner.

- Reluctance to provide standard information when opening an account, submitting minimal or false information, or providing details that are difficult for the BIR to verify.
- Customers who demonstrate an acceptable level of financial literacy yet decline to provide information that would, under normal circumstances, enable them to access credit or other beneficial banking services.
- Corporate representatives who unjustifiably avoid contact with the BIR;

- Limited or non-use of standard banking benefits, such as failing to take advantage of interest rates on high credit balances.
- Repeated difficulties in reaching the customer via the home address or telephone number provided, including returned mail due to the customer being unknown at the stated address.
- Customers introduced to the institution by well-known and reputable individuals (e.g. professional offices, businesspersons), where it becomes clear that the referral is intended to facilitate circumvention of the institution's customer due diligence obligations.
- Customers reported in the media as being connected to criminal activities likely to generate illicit proceeds.
- Customers who display excessive interest in establishing personal relationships with the branch manager or staff, with the apparent aim of easing the institution's controls or obligations.
- Customers who show undue curiosity regarding the institution's systems, controls, and internal policies on anti-money laundering (AML) and counter-terrorism financing (CTF).

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

- Requests to establish correspondent banking relationships with foreign financial institutions based in high-risk jurisdictions that lack proper AML policies.

- Accounts opened in Angola by a financial institution in its own name but structured into sub-accounts specifically to reflect transactions carried out by clients of that institution.
- Accounts in Angola opened by foreign financial institutions that maintain correspondent accounts with shell banks.
- Unusual behavior by employees or representatives of financial institutions.
- Sudden changes in employee behavior, such as a lavish lifestyle inconsistent with their expected financial situation or declared income level.
- Unexplained variations in employee or representative performance, such as a sales representative who handles cash transactions and records a significant or unexpected increase in results.
- Any interaction with a representative in which the identity of the ultimate beneficial owner or the actual counterpart remains hidden, contrary to standard procedures for that type of transaction.
- Employees whose role involves client contact and who resist changes to their role that would prevent them from continuing the same activities.

ANNEX III – List of predicate offences underlying money laundering (as listed in the glossary of the FATF 40 Recommendations, supplemented by Law No. 38/20 of 11 November, which approves the Angolan Penal Code,) and by Law No. 12/24, which amends Law No. 38/20 of 11 November, the Law that Approves the Angolan Penal Code.

- Participation in an organized criminal group and unlawful activities for financial gain, including extortion, intimidation, or similar means.
- Terrorism, including the proliferation of weapons of mass destruction.
- Human trafficking, including trafficking in human organs or tissues and smuggling of migrants.
- Sexual exploitation, including child sexual exploitation.
- Trafficking in narcotic drugs and psychotropic substances.
- Trafficking in stolen goods and other assets.

- Corruption.
- Bribery.
- Fraud.
- Counterfeiting of currency.
- Forgery.
- Product piracy.
- Environmental crimes, including trafficking in protected species.
- Homicide.
- Aggravated assault.
- Kidnapping.
- Unlawful detention.
- Hostage-taking.
- Theft or robbery.
- Smuggling.
- Extortion.
- Falsification.
- Maritime piracy.
- Insider trading and market manipulation.
- Tax crimes.

CHAPTER VIII – UPDATE FREQUENCY

The manual must be updated at least once a year. However, it may be revised whenever necessary, provided that such need is duly justified and/or documented.