Policy for Managing ML/TF/PF Risk

Banco BIR, S.A

Document Details

Title:	Policy for Managing ML/TF/ PF Risks
File:	DCOMP_ Policy for Managing ML/TF/ PF Risks

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
02-06-2025	V.5	Board of Directors

Document Updates:

Version	Effective Date	Amendments
V.1	2015-12-04	Creation (CA.OS.P.053.2015)
V.2	2019-10-10	Layout Change (CA.OS.P.053.2015)
V.3	2020-12-08	Inclusion of Notice No. 14/2020 and Law No. 5/20 (CA.OS.006.2019)
V.4	2023-02-27	Update (CA.OS.006.2019)
V.5	02-06-2025	Update (CA.OS.001.2023)

Applicable Legislation/Regulations:

Legal Instrument	Effective Date	Subject
Notice No. 02/2024	March 22	Rules and Procedures for the Effective Implementation of Conditions for Operation, Instruments, Mechanisms, Formalities, and Reporting Requirements Related to the Prevention and Combat of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.
Law No. 14/21	January 28	General Regime of Financial Institutions.
Law No. 5/20	January 27	Law on the Prevention and Combat of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.
Notice No. 01/2022	January 28	Corporate Governance Code for Banking Financial Institutions.
Law No. 11/24	July 4	Law Amending Law No. 5/20 of January 27 – Law on the Prevention and Combat of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.
Law No. 1/12	January 12	Law on the Designation and Enforcement of International Legal Acts.
Instruction No. 20/20	December 9	Money Laundering, Terrorist Financing, and

		Proliferation Prevention Report: Risk Assessment Tools and IT Applications
Circular No. 02/24	March 20	On the Disclosure of Measures by the Financial Action Task Force (FATF)

INDEX

CHAPTER I – DRAFTING, APPROVAL, REVIEW, AND VALIDATION

I. DRAFTING, APPROVAL, REVIEW, AND VALIDATION

This document must be formally approved by the Board of Directors and reviewed at least annually.

In accordance with the Governance Policy for the Risk Management Model for Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (ML/TF/P), the following Structural Units have responsibilities related to the ML/TF Risk Management Policy of BIR:

Structural Unit	Responsibilities
Board of Directors (BoD)	Approval of the ML/TF/P Risk Management Policy.
Executive Committee (EC)	Definition of BIR's Risk Strategy.
Compliance Department (DCOMP)	Drafting and review of the ML/TF/P Risk Management Policy and submission for approval by the Board of Directors or equivalent body.
Internal Audit Department (IAD)	Assessment of compliance with the ML/TF/P Risk Management Policy.

CHAPTER II – SCOPE, APPLICATION, AND OBJECTIVES OF THE POLICY

This document outlines the Risk Management Policy for Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (ML/TF/P) of Banco de Investimento Rural (hereinafter referred to as "BIR" or "the Bank"), with respect to its ML/TF/P Risk Management System.

The purpose of this policy is to mitigate the risk of the Bank being used as a vehicle for criminal activities related to money laundering and terrorist financing through the products and services it offers. It also aims to reduce the likelihood of the identified ML/TF/P risks occurring, thereby safeguarding the Bank from financial and reputational impacts and preventing the integration of illicit gains into the financial system, in accordance with Notice No. 02/2024 of March 22, issued by the National Bank of Angola (hereinafter "BNA").

Accordingly, and in compliance with the legal obligation established under Articles 14 and 22 of Law No. 5/20 of January 27, and Articles 18 and 34, both of Article 5 of Notice No. 02/2024, the Bank adopts internal measures, procedures, and control and management programs proportional to the identified risks. These include enhanced due diligence measures aimed at ensuring that the actions of all employees and auditors (internal and external) comply with the applicable legal framework.

Key obligations are highlighted on Page 4, as well as the 40 Recommendations of the Financial Action Task Force (FATF/GAFI) and the Basel Committee on this subject.

The Bank ensures that the results of the risk assessment are reflected in and effectively implemented through its existing internal risk management and mitigation policies and procedures. All business units and/or relevant staff are informed of the policies, procedures, and any other measures related to the management and mitigation of identified risks.

The Bank conducts, whenever necessary, periodic, regular, or ad hoc testing of its risk management and mitigation measures, policies, and procedures. These are subject to oversight by the internal control structures, namely

Compliance, Risk, and Audit. Any deficiencies identified in this context must be brought to the attention of the Compliance Officer, who is responsible for implementing the necessary adjustments.

This Policy is applied across all structural units of BIR Bank.

CHAPTER III – GENERAL PRINCIPLES

The following general principles guide BIR's ML/TF/P Risk Management Policy:

- **Transparency:** Risk assessment and management are conducted in a transparent manner, with clear evidence of actions taken and decisions made at various hierarchical levels, throughout the approval chain and during the entire course of the business relationship.
- **Segregation of Duties and Independence:** The assessment and monitoring of the level of risk exposure are carried out by an organizational structure that is effectively independent from the Bank's risk-taking units. While these units are also responsible for assessing and monitoring risks within their respective scopes and competencies, ultimate responsibility for risk management lies with the Board of Directors, which must provide BIR's structural units with the technical and human resources necessary for the effective management of money laundering and terrorist financing risks.
- **Control:** The ML/TF/P Risk Management System is subject to specific controls and is independently tested by the Internal Audit Department (IAD), acting as the third line of defense, independent from the Bank's operational structure.

CHAPTER IV – ORGANIZATIONAL STRUCTURE – LINES OF DEFENSE

Risk management is ensured through three lines of defense within the Bank's organizational structure:

LINES OF DEFENSE	STRUCTURE	RESPONSIBILITY

1st Line	Commercial Division / Commercial Department and Branch Network	• Customer Identification and Verification (Customer Due Diligence);
		• Initial Risk Assessment:
		  ○ KYC Scoring;
		  ○ Application of Enhanced Due Diligence Measures Based on Risk Level;
		• Entity Approval Hierarchy (differentiated levels based on risk, ensuring segregation of duties).

2nd Line	Compliance Department (DCOMP)	• Definition and review of the KYC Scoring Model; • Application of Enhanced Due Diligence (EDD) measures based on the risk level of entities; • Mandatory opinion on the approval of entities classified as High Risk.
	Information Systems Department (DSI).	• Ensuring data quality in information systems that serve as input for risk management systems.
	Risk Management Department (RMD).	• Ensuring the definition and implementation of controls based on the identified risks.
3rd Line	Internal Audit Department (IAD)	• Ensuring independent validation and effectiveness testing.

The responsibilities and duties of BIR's various structural units within the ML/TF/P Risk Management System are detailed in the "Manual of Policies and Procedures for the Prevention of ML/TF".

CHAPTER V – RISK MANAGEMENT MODEL

I. RISK-BASED APPROACH

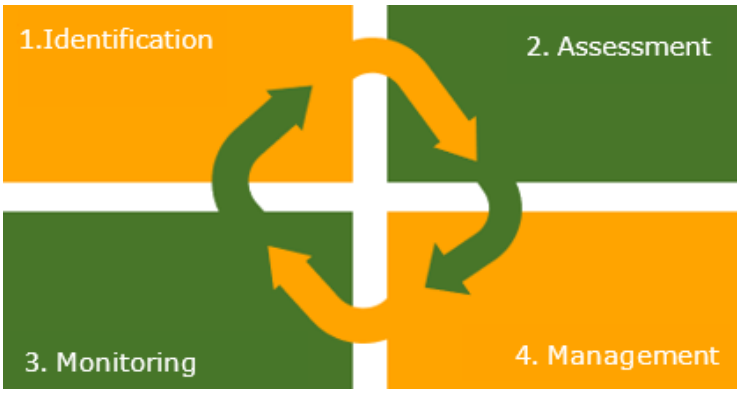
The Bank has developed a money laundering risk classification system applicable to all customers and beneficial owners. Operating in real time for the purpose of assigning risk levels, this system is based on the weighting of customer characteristics identified during the KYC process—such as professional activity, country of residence, expected transactional profile, politically exposed person (PEP) status, among others. Through an automated scoring mechanism, the system assigns each customer an appropriately calibrated and differentiated risk level.

Given that the customer money laundering risk classification process is dynamic, appropriate procedures must be applied to all customers and existing accounts, in accordance with the risk level assigned to them or in cases where their risk level increases based on criteria defined by the Bank, in line with applicable laws and regulations.

It is essential to ensure that all transactions carried out in existing active accounts are continuously monitored, and that any unusual or inappropriate activity triggers a re-evaluation of the customer's risk classification, based on an updated due diligence process.

In line with the above, the adoption of a risk-based approach offers, among others, the following benefits:

- Greater efficiency in detecting entities and transactions suspected of ML/TF/P;
- More effective risk management and cost-benefit optimization;
- More efficient monitoring of identified real threats and increased flexibility for the sector to adapt to evolving risks over time.



II. RISK IDENTIFICATION

For the identification, assessment, and mitigation of specific risks related to money laundering, terrorist financing, and the proliferation of weapons of mass destruction, the Bank relies on reputable, credible, and diversified sources of information that provide insight into the origin and nature of such risks. The main sources include:

- Information, guidance, or alerts issued or disseminated by the National Bank of Angola, related to typologies and methods for identifying specific or emerging risks, or to suspicious activity indicators.
- Information, guidance, or alerts from the Financial Intelligence Unit (FIU) or law enforcement authorities, related to

typologies and methods for identifying specific or emerging risks, or to suspicious activity indicators.

- Information, guidance, or alerts issued by the government related to the prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

- Information resulting from the national risk assessment.

- Lists issued by public bodies, namely those identifying politically or publicly exposed functions and their respective holders.

- Internal analyses and documents, i.e., information collected during customer identification and due diligence procedures, as well as internally developed and updated lists and databases maintained by the Compliance and Risk Management Departments.

- Independent and credible information from civil society or international organizations regarding corruption indexes, publicly available reports on corruption levels and income associated with political or public functions in a given country or jurisdiction, as well as mutual evaluation reports issued by the Financial Action Task Force (FATF) or its regional bodies, and any other relevant listings issued by international organizations.

- Information sourced from the internet and media outlets, provided comes from independent and credible sources.

- Information contained in databases, watchlists, risk reports, and other analyses from commercially available sources.

- Official statistical data from national or international sources.

- Relevant academic research.

- Information provided by other Financial Institutions or similar entities, to the extent legally permissible.

- Information regarding the business activity carried out by customers, as well as the products, services, and transactions they use.

- Information on the customer's history and nature.

- Geographical location of the customer or beneficial owner, including countries or regions where the customer operates directly or through third parties, whether belonging to the same group, etc.

III. CUSTOMER RISK ASSESSMENT

Customer risk assessment is a fundamental process for the Bank. It involves a detailed analysis aimed at identifying and quantifying the risks associated with a specific customer, enabling BIR to take appropriate measures to mitigate those risks.

The first step consists of identifying which ML/TF/P (Money Laundering, Terrorist Financing, and Proliferation) risks affect the Bank. In the risk assessment, it is necessary to consider legal, regulatory, and reputational aspects that may impact BIR.

Customer Risk Assessment is carried out through the KYC Scoring Model developed by the Bank.

Risk assessment is carried out at the time of account opening, throughout the business relationship, during periodic reviews, whenever an event triggers a re-assessment, and in light of any deficiencies identified within the internal

control framework.

IV. Customer Risk Classification

For the purpose of customer classification, the risk categories established in the ML/TF/P risk matrix are applied, assigning a risk score that may be classified as Low, Medium, High, or Unacceptable. Customers are classified as Unacceptable when their final risk score is equal to or greater than 150.

MONITORING

At this stage, it is ensured that the information produced in the previous phases is analyzed in a timely manner by the relevant internal bodies, and that reliable, complete, and timely information on the risk exposure profile is communicated to external entities.

V. CUSTOMER RISK MANAGEMENT

Risk management is based on the development of mechanisms that enable the reduction of risk exposure and the dissemination of information, supported by a robust and integrated ML/TF/P prevention program. Particular emphasis is placed on training programs focused on combating ML/TF, aimed at ensuring the Bank's compliance with the applicable legal and regulatory framework.

I. ORGANIZATIONAL MODEL:

RISK MANAGEMENT PHASES	RESPONSIBILITIES	KEY STAKEHOLDERS
Identification	Identify the ML/TF/P risks to which BIR Bank is exposed	Board of Directors Executive Committee Compliance Department
Assessment (Risk Quantification)	Define risk calculation matrices – development and review of the scoring methodology.	Board of Directors Executive Committee Compliance Department
Monitoring	Develop and implement measures that enable the reduction of risk exposure.	Board of Directors Executive Committee Commercial Department Compliance Department Risk Management Department
Management	Prepare and disseminate management information Conduct independent assessment	Compliance Department Internal Audit Department

CHAPTER VI – TRAINING

Without prejudice to the general duty of risk management, training is essential for employees performing functions directly related to this area, to ensure full, ongoing, and up-to-date knowledge. The Bank places special emphasis on training newly hired employees whose roles are directly relevant to the prevention of ML/TF/P. This training is based on an integrated program covering policies, procedures, and controls, ensuring that no employee begins their duties without at least having knowledge of:

- Basic principles and concepts related to ML/TF/P;
- Fundamental principles of the current internal control system, and
- Rules and procedures for implementing the above-mentioned principles.

The training program includes classroom training, on-the-job training, and/or e-learning.

Classroom and on-the-job training are primarily delivered by internal trainers, including the Compliance Officer, as well as by individuals with extensive experience and expertise in the subject matter who are part of the Compliance Department. The Bank has established and applied an appropriate training policy for its managers, employees, and other staff members, with the aim of ensuring comprehensive, ongoing, and up-to-date knowledge on, among other aspects:

a. The applicable regulatory framework, as well as the policies, procedures, and controls implemented internally for the prevention of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.
b. Identification and reporting of suspicious transactions to the Compliance Officer.
c. Reporting irregularities in accordance with regulatory requirements.
d. Guidelines, recommendations, and information issued by law enforcement authorities, supervisory bodies, or representative industry associations.
e. Risks, typologies, and methods associated with funds or other assets derived from or related to criminal activities or the financing of terrorism and the proliferation of weapons of mass destruction;

f. The vulnerabilities of the business areas developed by the Institution, as well as the products, services, and transactions offered, the distribution channels used for those products and services, and the communication methods used with customers.

g. The reputational, legal, and prudential risks, and the sanctions or penalties resulting from non-compliance with the preventive obligations related to Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction.

h. The specific professional responsibilities in the area of prevention of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction, particularly the policies, procedures, and controls associated with meeting these preventive obligations.

CHAPTER VII – UPDATE FREQUENCY

The aforementioned manual must be updated at a minimum on an annual basis. However, it may be reviewed whenever necessary, provided that the need for revision is duly justified and/or substantiated.

ANNEX I – ILLUSTRATIVE LIST OF POTENTIAL HIGH-RISK FACTORS

I. RISK FACTORS INHERENT TO CUSTOMERS

1. Business relationships or occasional transactions that occur under unusual circumstances, relative to the customer's expected profile and other characteristics of the business relationship or occasional transaction.
2. Customers/Beneficial Owners who are residents of, or operate in, countries or jurisdictions referred to in points 20 to 26 below.
3. Legal persons or entities without legal personality that serve as vehicles for holding personal assets.
4. Companies with nominee shareholders or whose share capital is represented by bearer shares.
5. Customers engaged in activities that involve intensive cash transactions.
6. Ownership or control structures of the customer (particularly the chain of ownership or control) that appear unusual or excessively complex, given the nature of the customer's business.
7. Politically Exposed Persons (PEPs).
8. Correspondent banks domiciled in third countries.
9. Customers or beneficial owners who have been subject to sanctions or restrictive measures imposed by the United Nations Security Council or the European Union.
10. Non-profit organizations whenever:

a) The organization represents, at the domestic level, a significant proportion of the financial resources controlled by the non-profit sector.

b) The organization represents a significant share of the international activities carried out by the non-profit sector. For this purpose, activities carried out through affiliated entities should be considered as part of the same organization:

c) Of the organization's own branches or subsidiaries abroad; Of associated non-profit organizations, including their respective branches and subsidiaries abroad; The ownership or control structure, or the organizational model, appears unusual or excessively complex, given the nature of the activity carried out.

11. Business relationships, occasional transactions, or operations in general expressly identified by the National Bank of Angola as involving risks associated with customers or beneficial owners.

II. RISK FACTORS INHERENT TO PRODUCTS, SERVICES, TRANSACTIONS, OR DISTRIBUTION CHANNELS

1. Private Banking
2. Trade Finance.
3. Products or transactions are likely to facilitate anonymity.
4. Business relationships or occasional transactions established/executed using remote communication channels.
5. Payments received from unknown third parties or parties unrelated to the customer or their business activity.
6. Products offered and transactions conducted within the framework of correspondent banking with credit institutions established in third countries.
7. New products and new business practices, including new distribution mechanisms and payment methods, as well as the use of new or developing

technologies for both new and existing products.

7. Business relationships, occasional transactions, or operations in general expressly identified by the National Bank of Angola as involving risks associated with products, services, transactions, or distribution channels.

III. RISK FACTORS INHERENT TO GEOGRAPHIC LOCATION

1. Countries or jurisdictions with strategic deficiencies in anti-money laundering and counter-terrorist financing, as identified by the Financial Action Task Force (FATF) in documents published on its official website.
2. Other countries or jurisdictions identified by credible sources (such as publicly available evaluation or follow-up reports) as lacking effective AML/CFT systems.
3. Countries or jurisdictions identified by credible sources as having significant levels of corruption or other criminal activities.
4. Countries or jurisdictions subject to additional countermeasures decided by the Council of the European Union.
5. Countries or jurisdictions subject to sanctions, embargoes, or other restrictive measures imposed notably by the United Nations Security Council or the European Union.
6. Countries or jurisdictions that provide funding or support for terrorist activities, or where known terrorist organizations operate.
7. Offshore financial centers.
8. Business relationships, occasional transactions, or operations in general expressly identified by the National Bank of Angola as involving risks associated with geographic factors.

ANNEX II – ILLUSTRATIVE LIST OF POTENTIAL SUSPICIOUS INDICATORS

I. GENERIC INDICATORS

1. Customers who carry out occasional transactions (any transaction conducted with obliged entities outside the scope of an already established business relationship) or engage in operations which, by their nature, frequency, amounts involved, or any other risk factor, are inconsistent with the customer's usual profile.
2. Customers who move cash without a plausible explanation:

a. In unusually large amounts.
b. In amounts not justified by the customer's profile.
c. Packaged or wrapped in an unusual manner.
d. In poor physical condition.
e. Composed of low-denomination banknotes, with the intent of exchanging them for high-denomination notes.

3. Customers who, in any way, attempt to persuade the financial institution's staff not to comply with any legal obligation or internal procedure related to the prevention of ML/TF/P.
4. Customers who show reluctance or refuse to provide identifying information, supporting documentation, or other relevant data, or who fail to cooperate with the due diligence measures deemed necessary by the financial institution:

a. The identification of the Customer, their representative, or the beneficial owner.
b. Understanding the Customer's ownership and control structure.
c. Knowing the nature and purpose of the business relationship.
d. Knowing the origin and destination of the funds.

e. Understanding the nature of the Customer's business activity.

5. Customers who show reluctance or refuse to provide original documents or equivalent evidence.
6. Customers who show reluctance or refuse to update their personal or account-related information.
7. Customers who show reluctance or refuse to engage in face-to-face contact with the financial institution.
8. Customers who provide identifying information, supporting documentation, or other data:
    a. That are not credible in terms of authenticity.
    b. That is unclear in content.
    c. That is difficult for the financial institution to verify
    d. That has unusual characteristics.

9. Customers who present different identification documents each time are requested by the financial institution.
10. Customers who, in the course of their activity, use pseudonyms, nicknames, or any other alternative expressions instead of their real name or legal designation.
11. Customers who delay or fail to submit documentation that could reasonably be expected to be provided after the establishment of the business relationship.
12. Customers who attempt to suspend or modify the business relationship or occasional transaction after being asked to provide identifying information, supporting documentation, or other relevant customer due diligence data.
13. Customers who do not wish to receive any correspondence at the declared address.

14. Customers who, without any apparent connection to one another, share the same address or contact details (such as phone number, fax number, email address, or others).
15. Customers whose address or contact details (phone number, fax number, email address, or others) prove to be incorrect or permanently out of service, especially when the financial institution attempts contact shortly after establishing a business relationship.
16. Customers whose address or contact details change frequently.
17. Customers who appear to be acting on behalf of a third party without disclosing this to the financial institution or, even if disclosed, refuse to provide the necessary information about the third party they represent.
18. Customers who attempt to establish overly close personal relationships with employees of the financial institution.
19. Customers who insist on dealing only with specific employee(s) of the financial institution and, in the absence of said employee(s), choose not to proceed with or suspend their transactions.
20. Customers who display an unusually high level of knowledge about anti- money laundering and counter-terrorism financing laws.
21. Customers who show unusual interest or curiosity in learning about the financial institution's internal policies, procedures, and control mechanisms for preventing ML/TF/P.
22. Customers who have established similar business relationships with different financial institutions in a short period of time.
23. Customers who operate in successive and varying locations, apparently attempting to avoid detection by third parties.

24. Customers who repeatedly conduct transactions just below the identification thresholds.
25. Customers who purchase high-value assets and proceed to sell them shortly afterward without an apparent reason.
26. Customers conduct transactions at different branches of the institution on the same day or within a short time frame.
27. Customers who provide unclear or inconsistent explanations about their transactions or who have limited knowledge about their purpose.
28. Customers who offer excessive and unsolicited explanations regarding their transactions.
29. Customers who appear nervous or express an unusual sense of urgency to complete transactions.
30. Customers linked to suspicious ML/TF/P operations that have been reported by the financial institution to the competent authorities.
31. Customers linked to suspicious ML/TF/P operations reported by supervisory authorities under Articles 17 and 19 of Law No. 5/20 of January 27 and known to the financial institution.
32. Customers who are or have been under investigation for criminal activities, especially ML/TF/P or any underlying predicate offenses (provided this information is either known directly by the institution or obtained from a credible public source).
33. Customers expressly identified by competent authorities as potentially linked to ML/TF/P operations.
34. Customers engage in financial activities without proper authorization or legal capacity.
35. Transactions that display an apparently unnecessary level of complexity for the intended purpose, due to, for example, the number of financial movements, institutions, accounts, involved parties, or countries/jurisdictions.

36. Transactions whose purpose or economic rationale is not readily apparent.
37. Transactions whose frequency, unusual nature, or irregularity cannot be plausibly explained given the customer's profile.
38. Transactions that appear inconsistent with the standard practices of thecustomer's business sector or area of activity.
39. Transactions involving "shell companies".
40. Transactions that show no connection to the Customer's known business activity and involve individuals or entities related to countries or jurisdictions that are publicly recognized as:
    a. Sources or transit points for narcotics production/trafficking.
    b. Having high levels of corruption.
    c. Money laundering hubs.
    d. Sponsors or supporters of terrorism.
    e. Sponsors or supporters of the proliferation of weapons of mass destruction.
41. Transactions that show no connection to the Customer's known business activity and involve individuals or entities related to countries, territories, or regions with preferential tax regimes, or other countries or jurisdictions with highly restrictive banking secrecy laws.
42. Business relationships or occasional transactions in which there is an attempt to conceal the identity of the beneficial owners, particularly through complex corporate structures.
43. Customers who maintain a significant number of bank deposit accounts, especially when some of those accounts remain inactive for extended periods of time.

44. Customers who hold bank deposit accounts with several credit institutions located in the same country/geographic area.
45. Customers who make deposits without knowing the exact amounts being deposited.
46. Customers who open accounts with large amounts of cash.
47. Customers who frequently use personal accounts to carry out transactions related to their business activities.
48. Accounts that frequently show activity for which the account holder does not provide a credible explanation.
49. Accounts opened at branches located far from the Customer's address or place of work.
50. Accounts whose activity far exceeds what was expected at the opening time.
51. Accounts that are opened or operated by a large number of individuals who have no apparent personal or professional relationship with one another.
52. Accounts held by legal entities pursuing unrelated economic activities, all operated by the same individuals.
53. Accounts show a high volume of small incoming credits and a small number of large outgoing debits.
54. Accounts with frequent cash credits and/or debits that are inconsistent with the Customer's profile or line of business.
55. Accounts receiving frequent deposits from individuals with no apparent personal or professional connection to the account holders.

56. Accounts used to consolidate funds from various other accounts, which are subsequently transferred in bulk, especially when the transfer is made abroad.
57. Accounts that, without apparent reason, show a sudden increase in activity, transaction volume, and/or average balances.
58. Dormant accounts that suddenly show large transactions or movements, especially via cash deposits.
59. Accounts used almost exclusively for inward and outward fund transfers involving foreign countries.
60. Accounts held by entities domiciled in offshore centers, sharing the same beneficial owner, with frequent and complex fund movements between them.
61. Accounts are subject to large and frequent deposits exclusively made via ATMs or night deposit boxes, especially when such deposits are in cash.
62. Accounts receiving cash deposits immediately after the account holders access their rented safety deposit boxes at the financial institution.

II. INDICATORS RELATED TO CREDIT OPERATIONS

1. Early repayment of loans when such repayments are made:
   a. Unexpectedly and without a logical or apparent reason.
   b. To the borrower's financial detriment.
   c. Using third-party funds.
   d. Using funds of uncertain origin that are inconsistent with the Customer's profile.

e. Using funds transferred from accounts held at multiple financial institutions; or
f. Using cash (especially in the context of consumer credit operations).

2. Loan applications with no apparent economic justification for the transaction, considering, for example, the high value of assets held by the Customer.
3. Loan applications by Customers who show no concern in discussing the terms of the operation, particularly the associated costs.
4. Loan applications backed by guarantees or assets (own or third-party) deposited with the financial institution, whose origin is unknown and whose value does not match the Customer's financial situation.
5. Loan applications by Customers who are already borrowers of loans granted by institutions based in offshore centers and who show no connection with the Customers' known activities.
6. Loan applications by Customers who declare income whose origin is not fully clarified by the holders.
7. Loan applications in which Customers propose, as a condition for approval, the placement of large sums in deposits or other financial products.
8. Loan applications where documentation concerning the borrower, intended to be part of the loan file, is provided to the financial institution by a third party with no apparent connection to the transaction.
9. Lack of evidence of use of the loaned funds, with the Customer withdrawing the credited amount in cash from their deposit account, corresponding to the granted loan.
10. Payments related to credit card usage repeatedly made by persons other than the actual cardholders.

III. INDICATORS RELATED TO FUND TRANSFER OPERATIONS

1. Transfers split into multiple operations to avoid compliance with legal and regulatory obligations that apply to transactions reaching a certain threshold.
2. Outgoing transfers inconsistent with the known activity of the Customer, particularly regarding the amount, frequency, or beneficiaries involved.
3. Transfers in which—at any stage of the fund flow, including at the point of availability to the final beneficiaries—individuals or entities are involved, formally or informally, without proper authorization to carry out such activity by the competent authorities of the involved countries or jurisdictions.
4. Transfers with no apparent connection between the Customer's known activity and the originators/beneficiaries or the countries/geographical areas of origin/destination.
5. Transfers for which the Customer refuses or shows reluctance to explain the reason for the operation.
6. Transfers made in favor of a beneficiary or received from an originator about whom the Customer has little information or is reluctant to provide it.
7. Transfers in amounts higher than those expected at the time the business relationship with the Customer was established.
8. Outgoing transfers to a large group of beneficiaries who apparently have no family ties with the Customer.
9. Transfers made in favor of a large group of beneficiaries who are nationals of countries or jurisdictions publicly associated with terrorist activities.

10. Transfers regularly ordered by the same person or entity to different recipients, with the amounts being identical or similar.
11. Transfers regularly ordered by the same person or entity to the same recipient, but with different amounts.
12. Transfers ordered by different persons or entities to the same beneficiary, on the same or very close dates.
13. Transfers ordered by different persons or entities sharing one or more common personal identifiers (surname, address, employer, phone number), made on the same or nearby dates.
14. Transfers ordered by different persons or entities, where the funds are provided by only one of them.
15. Transfers carried out using funds provided by a third party.
16. High-value transfers with instructions for the funds to be made available in cash to the recipient.
17. Incoming international transfers where the funds are immediately withdrawn from the Customer's account or, if no account exists, immediately transferred to other beneficiaries.
18. Transfers accompanied by instructions for the funds to be made available to third parties rather than the designated beneficiaries.
19. Cross-border transfers that occur alongside reciprocal transfers from abroad, for the same or similar amounts.
20. Transfers where Customers show unusual interest or curiosity about the fund transfer system, particularly operational procedures and/or transaction limits.

21. Outgoing transfers made during periods that do not coincide with salary payments, especially when ordered by immigrant workers.

IV. INDICATORS RELATED TO MANUAL CURRENCY EXCHANGE OPERATIONS

1. Transactions split into multiple purchases/sales to avoid compliance with legal and regulatory obligations applicable to operations that reach a certain amount.
2. Transactions inconsistent with the known activity of the Customer, particularly in terms of the amount or frequency.
3. Transactions carried out using an exchange rate that is more favorable to the financial institution than the published rate and/or payment of commissions higher than due, as proposed by the Customer.
4. Transactions where Customers wish to exchange large sums of one foreign currency for another.
5. Transactions involving non-resident Customers who appear to travel to the country specifically to carry out currency purchase/sale operations.
6. Frequent transactions using low-denomination banknotes or currencies with limited international circulation.
7. Transactions where Customers instruct the financial institution to deliver the equivalent value to a third party.
8. Transactions where Customers insist on receiving the equivalent value in the form of a bank-issued cheque, even though such practice is not commonly used by the institution.
9. Transactions where Customers request the equivalent value in foreign currency to be paid in notes of the highest denomination available.

10. Transactions in which Customers request to receive the equivalent value in multiple postal orders of small amounts, made payable to various beneficiaries.

V. INDICATORS RELATED TO EMPLOYEES OF FINANCIAL INSTITUTIONS

1. Employees who repeatedly fail to comply with legal obligations or internal procedures regarding the prevention of ML/TF/PF (Money Laundering, Terrorist Financing, and Proliferation Financing).
2. Employees who establish relationships of familiarity and closeness with Customers that exceed normal standards within the scope of their assigned duties or that are inconsistent with the financial institution's internal practices.
3. Employees who display social behavior patterns or other outward signs that are not compatible with their known financial situation as assessed by the financial institution.

VI. OTHER INDICATORS

1. Real estate transactions in which:

a. The sale price is significantly higher than the market value.
b. Payment is made by bearer cheque or by cheque endorsed in favor of a third party with no apparent connection to the transaction.
c. Payment is made in cash, especially when originating from a bank deposit account held by a third party with no apparent connection to the buyer; or
d. The property being transacted was recently acquired by the seller.

2. Transactions related to non-profit organizations when:

a. The nature, frequency, or amount of the transactions is not consistent with the size of the organization, its objectives, and/or its known activity.
b. The frequency and amount of the transactions suddenly increase.
c. The organization holds large amounts of funds in its bank deposit account for extended periods.
d. The organization receives contributions exclusively from individuals or entities not residing in Angola.
e. The organization appears to have few or no human or logistical resources allocated to its activity.
f. The organization's representatives are not residents of Angola, especially when large amounts are transferred to their country of residence.
g. The organization has any connection with countries or jurisdictions publicly recognized as drug-producing/trafficking locations, as having high levels of corruption, as money laundering hubs, as promoters or supporters of terrorism, or as promoters or supporters of the proliferation of weapons of mass destruction.

3. Customers who, suddenly, substantially increase the number of visits to their safety deposit boxes.
4. Customers who carry out high-value transactions using prepaid cards or who purchase multiple prepaid cards from the same financial institution.

ANNEX III – GLOSSARY

AML (Anti-money laundering) - Measures and procedures to prevent the laundering of illicit funds through the financial system.

Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) Policy - Internal policy outlining the bank's framework for preventing money laundering and terrorist financing.

CTF (Counter-Terrorism Financing) - Measures and controls to prevent the financing of terrorist activities.

Due Diligence - The process of assessing customer information to prevent money laundering and terrorist financing.

E-Learning - Training delivered electronically, typically over the internet.

Enhanced Due Diligence - More detailed checks applied to high-risk customers or transactions.

Financial Action Task Force (FATF/GAFI) - Intergovernmental body that sets international standards to combat money laundering and terrorism financing.

On-the-Job Training - Practical training provided in the workplace as part of skill development.

FT (Terrorism financing) - The process of providing funds or financial support to individuals or groups involved in terrorist activities.

Know your Customer (KYC)- The process of verifying the identity and background of clients.

ML (Money Laundering) - The process of disguising the origins of illegally obtained money.

Mobile Banking - Banking services provided via mobile phones or smartphones.

OFAC (Office of Foreign Assets Control) - U.S. Treasury Office of Foreign Assets Control; manages and enforces economic and trade sanction.

Offshore - Jurisdictions typically associated with low tax or secrecy regimes, often used for asset holding.

Online - Accessible via the internet or connected to a digital network in real time.

Private Banking - Personalized banking and financial services provided to high-net-worth individuals.

Risk Based Approach - A strategy that allocates resources according to the level of money laundering/terrorist financing risk.

Shareholders – Individuals or entities that legally own shares in a company.

Site – A specific location on the Internet used for accessing content or services.