ANTI-MONEY LAUNDERING (AML), COUNTER-TERRORIST FINANCING (CTF) AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (PWMD)

POLICY

Ref: POL/DC/001/V02

Effective Date: 04/11/2022

Security Classification: **PÚBLICO**

CONTENTS

1 GENERAL PROVISIONS

1.1 PURPOSE AND SCOPE

The Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction Policy (hereinafter referred to as the AML/CTF/PWMD Policy), is periodically reviewed and reassessed at the appropriate time period and/or in an earlier time schedule if deemed to be necessary, in order to comply with the legal duties and provisions laid down by the regulations and national Laws in force as well as with the best international standards and good corporate governance practices applied to the financial banking sector, with a view to ensure the following:

a. A clear perception, insight and discernment of the key concepts and main definitions adopted, implemented and performed by the Financial Institution ("BFA") within the scope of the Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction & Sanctions ("AML/CFT/PWMD") risk management system, which is embedded into the comprehensive risk management system to which the Bank ("BFA") is, or may be, potentially exposed;
b. The AML/CTF/PWMD prevention/mitigation and risk management;
c. The identification of the key players, participants and/or stakeholders main powers, roles and duties engaged in the AML/CTF/PWMD risk management system, in particular the Compliance Department ("CD");
d. The BFA's safeguarding and shielding and its Staff Members from legal, regulatory, reputational and penalty risks that may potentially emerge from any AML/CTF/PWMD events, cases or scenarios;
e. The setting up of processes and procedures to identify, assess, mitigate, control and report suspicious business/economic activities and financial transactions to the relevant supervisory authorities/oversight bodies;
f. The Bank's adherence and compliance with applicable national laws/regulations and best international standards and good corporate governance practices;
g. To mitigate the likelihood of occurrence of potential breaches/infringements or non-compliance events/cases within the scope of the AML/CTF/PWMD framework, with regard to the applicable legislation, regulations, specific provisions, rules of conduct and Customer relationships, existing and/or implemented good corporate practices, ethical principles or other duties that may cause the Bank or its Staff Members to engage or be involved in a misdemeanour or criminal offence.

The current Policy has been drawn up and developed to provide the guidelines, rules and procedures in force within the Financial Institution or the Bank with respect to the AML/CTF/PWMD control system and aims to ensure that its target audience understands and complies with the laws and regulations in force, as well as with good corporate governance practices and standards applicable to the financial banking sector.

The current Policy is applicable to both the Bank and BFA's Group's Companies, to all Staff Members, whether permanent or temporary, as well as to the governing bodies members and to all entities, natural and legal persons, who have a legal and/or contractual relationship with the Financial Institution ("BFA").

The current Policy strengthens and does not jeopardise or undermine the compliance and/or fulfilment of the duties/obligations laid down in other BFA's internal corporate policies in force.

1.2 LEGAL, REGULATORY AND NORMATIVE FRAMEWORK

The current document addresses the following Legislation, Regulations and Standards:

Table 1— Legislation, Regulations and Standards addressed

NAME	ADDITIONAL REGULATIONS
Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction Act	Law N. º 05/2020 dated 27th January
Prevention and Counter-Terrorist Financing Act	Law N. º 19/17 dated 25th August
Regulation on Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF)	Notice N. º 14/2020 dated 22nd June
Report on Anti-Money Laundering, Counter-Terrorism Financing and Proliferation of Weapons of Mass Destruction (AML / CTF / WMD); Risk Assessment, IT Tools and Applications.	Instruction N. º 20/2020 dated 9th December
Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) in International Trade Operations	Instruction N. º 13/18 dated 19th September
Partial Amendment of Instruction No. 20/20 dated 9th December Report on Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction (AML/CTF/PWMD)	Instruction N. º 04/2021 dated 24th of February
Law N. º 1/12 dated 12th January	Law on the Denomination and Enforcement of International Legal Acts
Notice N. º 10/2021 dated 18th June	Financial Institutions Corporate Governance Code
Instruction N. º 13/18 dated 19th September	Anti-Money Laundering and Counter-Terrorist Financing in International Trade Operations
Directive N. º 01/DSI/2012 dated 10th May	Report on Suspicious Money Laundering Transactions
Directive N. º 04/DSI/2012 dated 24th July	Administrative Freezing of Funds and Economic Resources
Directive N. º 03/DSI/2012 dated 24th July	Identification and Reporting of Designated Persons, Groups and Entities
Regulation N. º 05/21 dated 8th November of the Angolan Capital Markets Commission	Regulation on Anti-Money Laundering, Counter-Terrorism Financing and Proliferation of Weapons of Mass Destruction (AML/CTF/PWMD)
Instruction N. º 09/CMC/12-21 dated 20th December	Designated Persons Identification Declaration Form
Instruction N. º 10/CMC/12-21 dated 20th December	Suspicious Transaction Declaration Form
Instruction N. º 13/CMC/12-21 dated 20th December	Freezing of Funds and Economic Resources

Table 2 – References I Lists the documents that served as a reference for the preparation of this document:

Table 2— References

NAME	VERSION
FATF Guidance - Financial Action Task Force	V.2022

Table 3 – Material Internal Regulations I Lists the relevant internal regulations to the subject matter regulated in this paper.

Table 3— Material Internal Regulations

NAME	VERSION
Compliance Policy	2021
Internal Control Policy	2022
Training Policy	2021
Identification, Prevention and Management of Conflict of Interests and Related Party Transactions Policy.	2022
Code of Conduct	2022
Irregularities' Reporting Policy (Whistleblowing Policy)	2022

1.3 DEFINITIONS, ABBREVIATIONS AND ACRONYMS

The key definitions, abbreviations and acronyms used in the current Policy are detailed below:

1.3.1 ABBREVIATIONS & ACRONYMS

- **Bank** – Banco de Fomento de Angola, S.A.
- **BO** – Beneficial Owner
- **BFA** – Banco de Fomento de Angola, S.A.
- **BOD** – Board of Directors
- **AICC** – Audit and Internal Control Committee
- **ECBOD** – Executive Committee of the Board of Directors
- **RC** – Risk Committee
- **UNSC** – United Nations Security Council
- **CD** – Compliance Department
- **FATF** – Financial Action Task Force
- **Financial Institution / Institution** – Banco de Fomento de Angola, S.A.
- **PEP** – Politically Exposed Person
- **AML/CTF/PWMD** - Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction
- **EU** – European Union
- **FIU** – Financial Intelligence Unit

1.3.2 DEFINITIONS

- **Correspondent Bank** – An incorporated and established financial institution that provides a bank account or other financial banking services, on behalf of other Financial Institutions, to meet the need of funds settlement, funds management, lending, or investment needs of other established Financial Institutions.
- **Shell Bank** – A Financial Institution or a Bank that is incorporated and authorised to operate in a particular jurisdiction but has no physical footprint or location in such jurisdiction and is not affiliated/associated with a regulated financial group whose banking activities are under an effective regulatory oversight by the relevant authorities.
- **Beneficial Owner** – A Natural Person(s) who:
  - Ultimately own or control a holding or a stake in the share capital of a legal person and/or the natural person on whose behalf the transaction is being performed;
  - Ultimately have actual control over a legal person or an unincorporated entity, either in cases where the shareholdings/stakes control are acquired and held by means of an ownership chain in the share capital or through non-direct control;
  - Ultimately holds direct or indirect ownership or control of the company's share capital or the voting rights in the legal person, other than a company listed on a regulated market that is subject to information disclosure requirements consistent with international standards;
  - Have the right to hold or exert significant influence or control over the company regardless of the shareholding position/stake control percentage;
  - With regard to legal entities/bodies that manage or allocate funds to natural person(s) that:
    - Benefit from their real estate assets/property portfolio when the future beneficiaries have already been determined;
    - Are understood to be included or comprise the group, category or scope of persons in whose primary interest the legal person/entity or company was incorporated or operates its business activity, where the future beneficial owners have not yet been determined;
    - Have control over the legal person's real estate assets/ property assets portfolio.
- **Money Laundering** – The business or financial activity designed to convert, transfer, assist or facilitate any unlawful assets, illegal proceeds, or ill-gotten gains transfer and/or conversion transaction obtained by the perpetrator or a third party, directly or indirectly, with the purpose of concealing the illegal origin/source, the funds' end-use and/or the identity of the beneficial owner. It is assumed and understood that money laundering takes place even when the business activities that has generated access to the acquisition of unlawful assets, illegal proceeds or ill-gotten gains is carried out in the territory of another country. As described above, Money Laundering is typically carried out through the implementation of three independent phases, as follows:
  - **Placement** – The placing of the unlawful assets, illegal proceeds or ill-gotten gains obtained directly or indirectly through criminal activity into the financial system.
  - **Concealment** – The conversion of the unlawful assets, illegal proceeds or ill-gotten gains obtained through criminal activities into another type of financial asset, product or instrument, by concealing its unlawful origin/source through the creation of financial transactions complex schemes and/or financial products arrangements;
  - **Integration** – The placing of the unlawful assets, illegal proceeds or ill-gotten gains obtained through criminal activities back into the regular or official economy in order to create the perception and/or the "illusion" of legitimacy.

- **Dual-use goods and technology** – All goods, products, or items, including software and technology, which can be used for both civil and military purposes, including all goods which can be used for both non-explosive purposes and to assist in any way in the manufacture of nuclear weapons or other military explosive devices.
- **Assets, Proceeds and Gains** – It is understood to mean unlawful assets, illegal proceeds or ill-gotten gains derived from criminal economic activities, all kinds of assets, proceeds and gains, whether tangible or intangible, personal/private property or real estate, tangible or intangible, as well as legal documents or instruments in any form, including electronic or digital, the acquisition or possession of which originates from a criminal offence/activity and which provide evidence of the assets ownership or a legal right over them, including tax fraud.
- **Customer Risk Level Score** –It is underpinned on the Customers' assessment concerning the ML/TF/ PWMD risk level that such customers potentially entail for the financial institution, using certain parameters previously stipulated and drawn up by the Bank's Governing Bodies and which determines the Customers' breakdown into risk level categories.
- **Customer** – Natural or legal persons who have entered into a legal agreement with the Bank, or who state or display an intention to do so, including, but not limited to, consultants/advisors, counterparties, suppliers, or other service providers.
- **Staff Member** –Any natural person who, on behalf of the financial institution and under BFA's authority or dependency, is engaged in performing any operational activities, acts or procedures inherent to the business banking activity undertaken by the Financial Institution, regardless of whether him/her has an employment contract (in-house staff member) or non-employment relationship (third-party collaborator) with the financial institution.
- **Compliance Officer** – The Compliance Officer is in charge of coordinating and monitoring the implementation of the Anti-Money Laundering, Counter-Terrorism Financing and the Proliferation of Weapons of Mass Destruction (AML/CTF & PWMD) system, including the underlying internal control procedures, as well as for operational central reporting and communication of financial transactions which may potentially involve or be related to money laundering, terrorism financing and the proliferation of weapons of mass destruction to the Financial Intelligence Unit and other relevant authorities.
- **Freezing of Funds** –Interdiction or provisional ban on wire transfers transactions, exchange operations, provision, disposal or allocation of any funds or assets owned or controlled by designated persons, groups, or entities, as well as the custodianship or provisional control of unlawful assets, illegal proceeds or ill-gotten gains obtained as a result of business or financial criminal activities.
- **Freezing of Economic Resources** –Any actions aimed at preventing the use of assets or resources for obtaining additional funds, assets or services by any means, notably through the sale, lease or mortgage of real estate assets/property assets.
- **Wire transfer correspondent bank account** –Banking accounts at correspondent banks, used directly by third parties to conduct financial transactions by means of wire transfers on one's own-account trading. In other words, it means a particular Financial Institution that provides a banking current account or other financial banking services to other Financial Institutions in order to meet the funds settlement, funds management, lending or investment needs of other Financial Institutions.
- **Due Diligence/Ongoing Monitoring** – Ongoing monitoring of the business relationship with its Customers, within the scope of the Customer's Identification and Verification (ID&V) procedures and validity/accuracy of the customer identification information details as well as the transactional analysis aimed at checking and validating the coherence of the financial transactions/deals with the customer's transactional profile and track record in terms of total amounts, transactions turnover, jurisdictions involved and counterparties.
- **Enhanced Due Diligence** – A set of enhanced due diligences measures carried out whenever an increased or higher risk of ML/TF/PWMD is identified within the scope of the Customers' risk score measurement/rating. These enhanced due diligence

measures must include obtaining additional data/information and documentary evidence (supporting documentation) within the scope of the Customer's Identification & Verification (ID&V) procedures and due diligence mandatory requirements/duties, as well as reducing the period for updating Customer data/information. Furthermore, the implementation of enhanced due diligence measures implies a Customers' close monitoring approach in order to identify potential deviations or mismatches between the Customer's expectable transactional profile and the actual one.

- **Identification Documents** –Comprises all the documents legally and procedurally required by the Government Authorities and the Financial Institution ("BFA" or the "Bank") for Customers' Identification & Verification (ID&V).
- **Shell Entity** – It is understood to mean a front or letterbox company, a shell business/legal entity or a ghost organisation or corporation, whether with a corporate or non-corporate structure, such as a cooperative, a religious or political group, or an actual criminal organisation under the control of another, acting in the interests of the control party, which usually remains hidden and cannot be held legally accountable for its actions. The Letterbox companies often present themselves as independent voluntary associations, charitable organisations or as companies owned by law firms based in tax havens and without a physical location or address, employees or equipment.
- **Terrorism Financing** – The process by which a perpetrator (market player) provides, collects or holds funds or assets of any type or nature, whether lawful or unlawful, as well as the proceeds, gains or rights that can be converted into financial resources or funds, intended for the planning, preparation or actual perpetration of terrorist acts. It is deemed to occur terrorism financing even when the provision or collection of funds or assets is carried out in another State's territory.
- **Financing and Proliferation of Weapons of Mass Destruction** – The process by which the perpetrator (market player) provides, collects or possesses funds or assets of any type or nature, whether lawful or unlawful, as well as proceeds, gains or rights that can be converted into financial resources or funds, intended to finance the proliferation of weapons of mass destruction (WMD) with the potential to cause large-scale casualties through a single application of such type of weaponry, such as nuclear, chemical and radiological weapons.
- **Risk Impact** – Measurement of the risk materialisation outcome/results.
- **Know Your Customer** – The Anglo-Saxon expression meaning "knowledge of the Customer". The various institutions or entities, within the scope of their customers' business relationship, must have an in-depth knowledge of their Customers.
- **Restrictive Measures** – A set of measures adopted by the United Nations Security Council (UNSC), the European Union (EU) or by the Angolan State aimed at freezing assets and economic resources related to terrorism, the financing and proliferation of weapons of mass destruction (WMD), against designated persons or entities.
- **One-off Transaction** – One-time financial transactions performed by a specific/particular Customer.
- **High-Risk Countries** – Countries qualified as high-risk in terms of ML/TF/PWMD as a result of national and international legal and regulatory non-compliance, within the scope of the AML/CTF/PWMD guidelines, standards and regulations framework, high levels of corruption, organised crime, political turmoil, military conflicts, proven and/or known involvement in the production or trafficking of narcotics, among others. Some of these jurisdictions are placed under FATF monitoring or qualified as non-cooperative.
- **Politically Exposed Persons** (**PEPs**) – National or foreign individuals who perform or have performed prominent public functions in Angola, or in any other country or jurisdiction or in any other International Body/Institution/Organization.
- **PEP Family Members** – Are understood to be family members of a Politically Exposed Person (PEP) the spouse or unmarried partner or relatives up to the 3rd degree of kinship, or other relatives with kinship up to the same degree, and their spouses or unmarried partners.

- **Person(s) closely associated with PEP(s)** – Persons closely associated with PEPs are deemed to be persons with well-known connections/ties and close corporate or business relationships.
- **Probability** – Measurement of the risk materialisation probability.
- **Correspondence Relationship** – Provision of banking or financial services by a commercial or universal bank, financial institution or other similar service provider (the correspondent), to another bank, financial institution or other entity of equivalent nature, which is its Customer (the respondent), which includes the provision of a current account or other type of bank account that entails an obligation to provide related financial services, such as cash management, processing of wire transfers and funds and other payment services on behalf of the respondent bank, cheque clearing, corresponding transfer accounts, foreign exchange services and securities transactions.
- **Business Relationship** – Any relationship of a corporate, professional or commercial nature between the Bank and its Customers which, at the time that it is formed or is set up, is intended to be permanent or foreseen to become a long-term business relationship, one that is designed to be stable and ongoing over time, regardless of the number of individual operations that comprise or come to form part of the relational framework that has been set up.
- **Inherent Risk** – The ML/TF/PWMD risk level framework connected with the Bank's business operational activities.
- **Residual Risk Exposure** – The risk level exposure following the implementation of controls. If the controls are effective, the residual risk will be less than the inherent risk.
- **Financial Services** – A set of financial products made available by the Financial Institution or the Bank, namely: i) banking account opening; ii) loans; iii) investment products; iv) guarantees; v) among others.
- **Terrorism** – It is understood to mean criminal activities or practices aimed at provoking a mental state of terror, panic, or fear in the general public, perpetrated by a group of people or individuals pursuing political purposes, regardless of the public, philosophical, ideological, racial, ethnic, religious grounds or any other factors or matters that may be taken into consideration.
- **Suspicious Transactions** – Non-standard transactions with uncommon features or patterns when compared to the regular transactions performed by Customers. Suspicious transactions have certain common traits and generic features, including, but not limited to, deviations from the normal or typical patterns of an account's activity. Any complex financial operation or unusually high amount transaction - beyond any unusual patterns of financial transactions with no obvious economic, commercial or lawful reason or justification - shall be deemed as a suspicious financial transaction and, therefore, should be subject to further investigation or enhanced due diligence by the financial institution. For example, a transaction of a very high amount in a customer's account that is inconsistent with the customer's balance is a cause for suspicion.
- **Occasional Transaction** – Any transaction carried out by the relevant legal entities or parties outside the scope of an ongoing business relationship.
- **Financial Intelligence Unit (FIU)** – The National Central Unit incorporated in the form of a legal body under public law, autonomous and independent with powers and authority to receive, analyse and disseminate the information reported as suspicious related to ML/TF/PWMD cases, events or scenarios, as well as to cooperate with its international counterparts and other relevant authorities with regard to Anti-Money Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction (AML/CTF/PWMD).

1.4 REGULATORY REPEAL

The current Policy repeals the following regulations:

- REF. POL-DC-001 – Version 1

1.5 ACCOUNTABILITY

The Compliance Department is accountable for the ongoing updating of the current Policy.

The current Policy materialises the stakeholders' duties and obligations as identified and highlighted in the current policy under section 2.2 on AML/CTF/PWMD Risk Management Governance.

1.6 OMISSIONS

The cases of regulatory omission or gaps must be addressed and reported to the Compliance Department prior to the adoption of any measures.

1.7 NON-COMPLIANCE

The non-compliance with the provisions laid down in the current policy shall be the object of analysis, assessment and investigation by the Compliance Department and, where deemed appropriate, necessary and/or relevant, the Audit and Monitoring Department will also be involved and perform its own due diligence and analysis. All cases of non-compliance identified (breaches, infringements and/or violations) shall be submitted and/or reported to the Compliance Department, which shall keep an auditable record of all non-compliance cases identified, submitted and/or reported, as well as of the outcome of the corresponding analysis, assessment and investigation.

1.8 CONTACT DETAILS

Any queries concerning the content of this policy should be submitted to the Compliance Department:

- Compliance Department E-mail Address – Regulatory Compliance Office: compliance.regulatorio@bfa.int

2 GENERAL GUIDELINES

2.1 AML/CTF/PWMD - COMPREHENSIVE RISK MANAGEMENT MODEL

The BFA has implemented and is focused on ensuring compliance with the regulatory guidance and applicable provisions, laws and regulations set forth by the National Authority and/or Oversight Body with regard to Corporate Governance and Internal Controls rules. Within the scope of the Internal Control System, the BFA is equally committed on ensuring the implementation of the Compliance Risk Management and AML/CTF/PWMD standards, requirements and procedures in accordance with the regulatory framework in force. Furthermore, in order to strengthen its internal control system, BFA has adopted and implemented a set of key concepts internationally recognised and accepted, in particular the guidelines and recommendations issued by the Basel Committee on Banking Supervision (BCBS) and the Financial Action Task Force (FATF).

The Financial Institution draws heavily upon the principles of accountability, integrity, accuracy and transparency. As such, the Bank guarantees that its business activity is performed in accordance with principles of ethical behaviour, integrity and good professional conduct and standards, with a view to ensure compliance with the national applicable laws and regulations and the Banking and Financial Services sector's good corporate practices.

Pursuant to BFA's approach and positioning concerning this subject matter, the AML/CTF/PWMD Policy is periodically reviewed and reassessed with a view to comply with the applicable laws and regulations as well as with the best international standards and corporate governance best practices, in order to ensure:

a. The ML/TF/PWMD prevention/ monitoring /mitigation and risk management;
b. The BFA's safeguarding and shielding and its Staff Members from legal, regulatory, reputational and penalty risks that may potentially emerge from any ML/TF/PWMD events, cases or circumstances;
c. The establishment of processes and procedures that enable the recognition, investigation and reporting of suspicious business activities and financial transactions to the relevant authorities;
d. The establishment and implementation of policies and procedures that enable the proper management and mitigation of ML/TF/ PWMD risks, and the due acknowledgement, investigation and reporting of suspicious business activities and financial transactions to the relevant authorities;
e. The implementation of the ML/TF/PWMD risk management and mitigation measures shall take into account the regulatory guidance provided by the Oversight/Supervisory Authorities.

Accordingly, the current policy aims to guarantee the accountability of the market players, participants and/or parties involved, to lay down the guidelines on the Customer Identification and Verification process (ID&V), Politically Exposed Persons (PEPs) and Beneficial Owners (BOs), as well as to implement the rules, standards and procedures on control and transactional record-keeping, the customers and products accurate risk assessment and rating score, along with the terms/definitions of confidentiality and banking secrecy.

The AML/CTF/PWMD comprehensive risk management model aims to identify and set out standards on which the Bank's organisational culture should be primarily founded and built on, particularly with regard to the ML/TF/PWMD framework, as well as to lay down and implement procedures to comply with the preventive and regulatory risk measures to which the Bank is bound and/or exposed. Within this scope, the BFA's management and supervisory bodies are entrusted with the duty of developing and

implementing a cross-sectional and comprehensive risk culture encompassing the different Bank's business areas, with a view to identify, assess, monitor, and mitigate the comprehensive risks to which the Financial Institution is, or may be, potentially exposed.

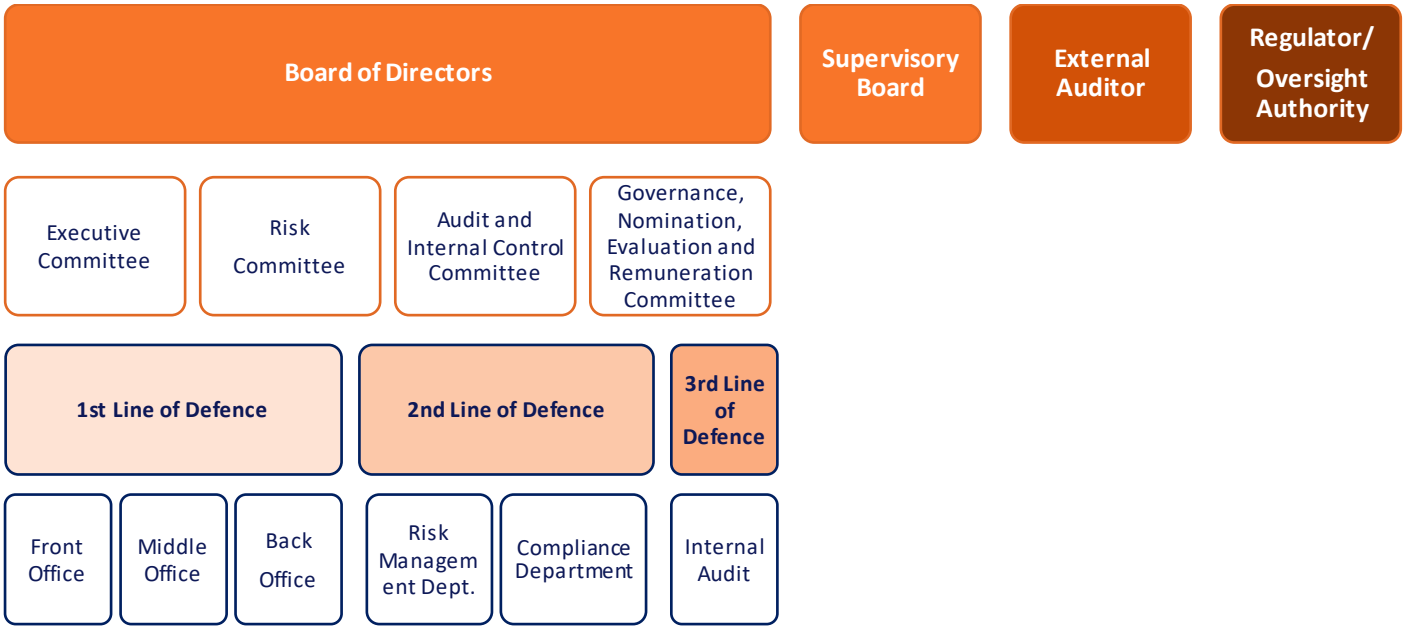
2.2 AML/CTF/PWMD - RISK MANAGEMENT SYSTEM GOVERNANCE MODEL

The BFA's AML/CTF/PWMD risk management system governance model is divided and developed on two main levels, as detailed hereunder:

a. **Strategic:** Falls under the powers and authority of the Board of Directors ("BOD"), assisted by the Executive Committee ("EC") and a wide range of specialised support and advisory committees, which are entrusted and tasked with the follow-up, monitoring and control of the Bank's business and operational risk exposure.

b. **Operational:** Implementation of the three lines of defence model with the assignment of clear duties/roles and cross-sectional risk management.

Figure 1 - Organizational model / Corporate Governance Model



2.2.1 THE THREE LINES OF DEFENCE AS AN ORGANISATIONAL MODEL

The setup of the ML/TF/PWMD risk management system follows a structural model based on the core principle of separation of functions, ensuring a full segmentation between the functions responsible for originating (or taking) risks and the functions responsible for managing and controlling such risks. The aforementioned principle is implemented and applied in accordance with the three-lines of defence model, schematically depicted in Figure.1 above. The adoption of this model aims to clarify the distribution of duties, obligations and functions between the different business units, departments and support areas, the supervisory and control units as well as the independent auditing /monitoring areas. The Figure 2. provides an overview of the duties, obligations and functions assigned to the three lines of defence, which are detailed in the following subsections/under items.

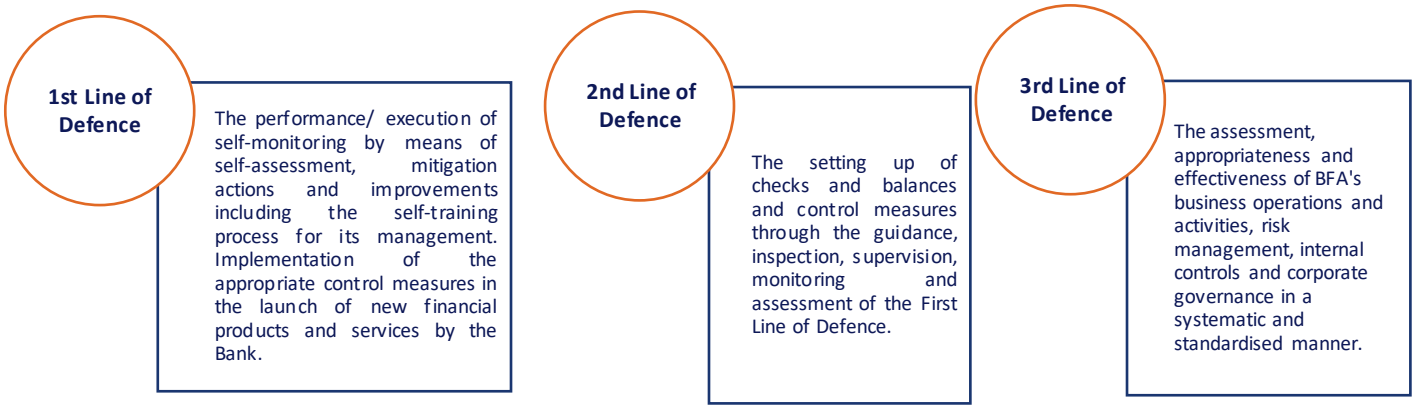


Figure 2 – Duties, Obligations and Functions according to the Lines of Defence

In addition to the three lines of defence model, the Financial Institution or the Bank is also subject to scrutiny by external auditors and oversight by the relevant supervisory authorities.

2.2.1.1 FIRST LINE OF DEFENCE

The First Line of Defence comprises the Front, Middle and Back Office, which must be primarily accountable to identify, assess, control and report the ML/TF/PWMD risks inherent to their business areas and activities, as well as in accordance with the applicable laws and regulations, namely:

a. To implement the relevant requirements and provisions in the operational procedures within the different business areas of activity and to oversee the implementation of the measures within the scope of the first line of defence staff's day-to-day operational activities, performance and powers;
b. To draw up the procedures and processes regulating the first line of defence staff's day-to-day operational activities and performance, supported by the Compliance Department (CD) and the Risk Management Department (RMD) where deemed appropriate, useful or relevant, and to recommend their approval, while ensuring their effective implementation;
c. Periodically review its business requirements taking a holistic view, in particular with regard to the comprehensive business operational needs, conditions and drivers, as well as the requirements associated with the products, services and distribution channels provided by the Bank, in accordance with the core principles and provisions laid down in the current Policy, as well as with the identified standards, procedures and regulations required for Compliance and ML/TF & PWMD risk management.
d. To perform the Customer's Identification & Verification (ID&V), proceed to their acceptance and ongoing monitoring in terms of updating the data/identification details and corresponding legal documents, in order to ensure the proper allocation of AML/CTF/PWMD risk level/score and continuously monitor the Customer's transactional profile;
e. To assess the Customers' transactional profile proactively, in a preventive manner;
f. To ensure that the sale/availability of products and services is only made available if the Customers information/data is updated within the Bank's internal systems and applications;
g. Considering that the AML/CTF/PWMD Risk Management is an integral part of the Bank's business, it also falls under the scope of the first line of defence in broad terms, the performance of the following duties and tasks:
    - To implement an appropriate methodology for communication and reporting to the Compliance Function on any identified cases of suspected breach, infringement or violation (non-compliance cases);

- To identify, measure, analyse and manage ML/TF/PWMD risk events that may compromise the proper fulfilment and/or achievement of the Bank's corporate operational purposes and/or business strategic targets and the provision of an accurate and effective ML/TF/PWMD control environment;
- To set up and implement the action plans associated with the non-compliances cases identified or suggestions for improvement, including in the event of the implementation/launch of new products and services by the Bank;
- To implement and stress test the AML/CTF & PWMD control/monitoring measures in their operational business units.
- To implement and perform self-monitoring processes (through self-assessment), which shall also encompass self-training.

2.2.1.2 SECOND LINE OF DEFENCE

The Second Line of Defence departments perform their corporate function with independence, authority and autonomy, and report directly to the Board of Directors. Within the scope of their activity are included monitoring the effective implementation of risk management practices and compliance internal control methodologies, as well as providing advisory support and assistance to the Bank's structures in the First Line of Defence. Moreover, they are accountable for stress testing and assessing compliance with regulations, policies and procedures, upholding and maintaining high levels of integrity and professional standards in alignment with the Bank's core principles, guidelines and risk appetite, whilst periodically and timely reporting to the Board of Directors the outcomes and findings of their analysis/reviews/assessments with regard to the Bank's compliance level.

The Second Line of Defence is comprised of and supported by the following Departments:

2.2.1.2.1 Risk Management Department (RMD)

Without setting aside or disregarding the powers and duties assigned under the provisions of the applicable Organisational Structure Handbook (OSH), the Risk Management Department is entrusted particularly with the performance of the following duties, obligations and functions:

a. To ensure that the operational losses associated with ML/TF/PWMD risks, are properly identified and classified according to the different types of operational risk events reported;
b. To set up Key Risk Indicators (KRIs) in cooperation with the Compliance Department, in order to ensure better control and reporting of the main ML/TF/PWMD associated risks, as well as ensure that they remain within (in alignment or even under) the Bank's approved risk appetite levels;
c. To assess risk situations arising from actual or potential events and impacting the approved operational risk limits and Key Risk Indicators (KRIs);
d. To perform self-assessment of the processes and/or procedures risks and controls, including control processes, particularly with regard to AML/CTF/PWMD and, if deemed appropriate, monitor the implementation of the action plans to mitigate the processes' residual risk.

2.2.1.2.2 Compliance Department (CD)

Without setting aside or disregarding the powers and duties assigned under the provisions of the applicable Organisational Structure Handbook (OSH) and internal regulations, the Compliance Department is particularly entrusted within the scope of the AML/CFT/PWMD framework with the performance of the following duties, obligations and functions:

a. To ensure the appropriateness, enforcement and effective implementation of policies, procedures and controls as appropriate for the effective and smooth management of the ML/TF/PWMD risks to which BFA is or may be potentially exposed, ensuring that these measures, procedures and processes are tailored and developed taking into account the regulations in force and the best international standards and good corporate governance practices;

b. To propose appropriate and enough controls to ensure compliance with internal and external regulations, and the Bank's core principles and guidelines, as well as to monitor their effective implementation;
c. To report periodically to the Boards and Committees, in accordance with the stipulated periodicity, in compliance with the provisions laid down in the Organisational Structure Handbook (OSH) as well as with the Compliance Policy;
d. To support the Board of Directors, the Executive Committee and the Bank's Staff members in fostering a culture of ML/TF/PWMD in a cross-sectional manner throughout BFA's entire organizational structure, which includes the development and maintenance of a proper and effective Corporate Governance structure with regard to ML/TF/PWMD control risks, as well as the coordination of the ML/TF/PWMD general control framework;
e. To engage and work closely with the Executive Committee in the effective and smooth management of the Compliance Risk with regard to ML/TF/PWMD;
f. To assess the appropriateness, effectiveness and updating of the AML/CTF/PWMD policies, procedures and processes, and propose such amendments and updates as it may deem appropriate at any particular instance or moment in time;
g. To raise awareness among the Bank's Staff members to the need to comply with the provisions laid down in the current Policy, monitoring its effective implementation and enforcement;
h. To provide and undertake training courses and skill-building activities and to assist in the setting up, implementation, monitoring and assessment of suitable training and skill-building activities in order to ensure an effective and smooth market risk management concerning ML/TF/PWMD;
i. To provide counselling, support and assistance to BFA's Staff Members, where deemed useful, relevant and/or appropriate, concerning matters of potential ML/TF/PWMD market risks;
j. To receive, assess and report suspicious or unusual operations and/or activities to the proper/relevant authorities and to ensure full cooperation, including the provision of data/information to these bodies, as required by law;
k. To decline to perform financial transactions and to recommend the termination of the business relationship with Customers, whenever are identified abusive, fraudulent and/or malicious practices involving the Bank or cases which could be considered liable and/or to be sanctioned/subject to penalties;
l. To foster and undertake the development and implementation of standards, procedures and processes with regard to ML/TF/PWMD;
m. To provide opinions, prior to approval, on ML/TF/PWMD policies, procedures and processes;
n. To properly implement KYC - "Know Your Customer" - standards and guidelines, in order to identify, through risk-based methodology, low, medium and high-risk Customers, and being able to undertake the process of Customer Identification and Verification (ID&V) up to the level of the Beneficial Owner's (BOs) and PEPs and other well-considered remarks;
o. To monitor financial transactions and publicly available information, with the aim of detecting non-standard transactions, prevent doing business with unsuitable, untrustworthy, suspicious, unlawful and/or illicit counterparties or those that may cause harm to the Bank's business and/or corporate reputation;
p. To Perform investigations and enhanced due diligence, when required;
q. To draw up timely reports and communications to the relevant areas and Oversight/Regulatory Authorities;
r. To engage and work closely with the Counterparties / Correspondent Banks, in order to ensure the business relationship ;
s. To support and assist in the drawing up of the ML/TF/PWMD policies and procedures, as well as effectively implementing and monitoring compliance with these Policies;

t. To report all information and data concerning the performance of their functions, directly to the portfolio Director. Moreover, whenever any circumstances, events or cases occur or take place that could pose, result or lead to potential ML/TF/PWMD corporate risks to the Financial Institution, also report all the data and information of such cases to BFA's Board of Directors.

The Compliance Department may, at any time, request information and clarifications on the implemented prevention and control measures from the Bank's Management and Supervisory Bodies and BFA Group in general, as well as collect any additional information from the Staff Members, which must be provided in a timely manner.

2.2.1.3 THIRD LINE OF DEFENCE

2.2.1.3.1 Audit and Inspection Department (AID)

In its capacity as BFA's third line of defence, the Audit and Inspection Department reviews and assesses compliance with the current Policy as part of its regular assessments and according to the approved annual audit plan. It reports the results of this assessment to the Executive Committee of the Board of Directors ("ECBOD") and to the Audit and Internal Control Committee (AICC), proposing potential measures to improve the appropriateness and effectiveness of the current Policy.

2.2.2 GOVERNANCE BODIES

2.2.2.1 SUPERVISORY BOARD (SB)

The Supervisory Board powers and duties shall be enshrined in a specific and/or particular Regulation and take into account the provisions laid down in the regulations provided by the National Bank of Angola. The Supervisory Board is particularly empowered to perform the following duties and functions:

a. To oversee the effectiveness and efficiency of the internal control system with regard to the ML/TF/PWMD framework;
b. To draw up duly reasoned opinions on the quality of the internal control system with regard to the AML/CTF/PWMD framework (regulations, procedures and processes);
c. To report on the potential identification/finding of high-risk shortcomings, weaknesses, failures, gaps or imperfections in BFA's internal control system with regard to the AML/CTF/PWMD framework (regulations, procedures and processes).

2.2.2.2 BOARD OF DIRECTORS (BOD)

The Board of Directors is particularly empowered to perform the following duties and functions:

a. To approve the current Policy and ensure its review and proper implementation;
b. To approve the procedures and controls, which are appropriate and risk-proportional with regard to AML/CTF/PWMD;
c. To gain proper knowledge of the ML/TF/PWMD risks to which the Bank is exposed at all times, as well as the processes used to identify, assess, monitor and control such risks within the scope of the global financial system;
d. To ensure that there is an effective framework for regulatory compliance risk management, in particular concerning the ML/TF/PWMD exposure risks;
e. To develop a Compliance framework, which shall be properly substantiated and documented under compliance risk management and AML/CTF/PWMD internal standards, regulations and policies;
f. To ensure that BFA's organisational structure enables the proper implementation and enforcement of policies, procedures and internal controls, preventing cases or scenarios of conflicts of interest and guaranteeing in a clear and transparent manner the proper separation of functions;

g. To develop and implement a corporate culture of AML/CTF/PWMD risk management that encompasses all BFA's Staff and governing bodies members, based on high-quality standards of ethics and integrity and which takes into account all the risks to which the Financial Institution ("BFA") is, or may be, potentially exposed.

h. To appoint the Compliance Officer and ensure that him/her performs as follows:
   - Carries out its duties, obligations and functions in an independent, ongoing and effective manner;
   - It has decision-making autonomy;
   - Possesses good repute (trustworthiness), professional skills and qualifications and has professional availability;
   - It has the means and resources (technical, material and human) required for the proper and efficient performance of its functions;
   - It has complete access to all data and information needed for the proper performance of its duties and functions, namely access to information related to the duty of identification and verification, due diligence and records of all transactions performed;
   - It is not faced with a scenario of operational/functional internal conflict;
   - Oversees and monitors the performance of the senior management leadership executive members, particularly when they are in charge of business areas that are, or may be, potentially exposed to ML/TF/ PWMD risks;
   - To monitor and periodically assess the effectiveness of internal policies, procedures and controls and, if any shortcomings, weaknesses and/or dysfunctions are identified, the Board of Directors (BoD) shall ensure that corrective measures are implemented;
   - To foster a reasoned assessment of reliability and credibility in the hiring of new Staff members to perform highly sensitive and risky functions, positions and/or job roles, particularly those concerning the ML/TF & PWMD area/subject matter.
   - To receive data/information reported to the portfolio Director responsible for the Internal Control functions, on any cases, circumstances or events that may entail potential ML/TF/PWMD risks;

i. To ensure that there is no interference with the mandatory duty to report to the Financial Intelligence Unit (FIU) any actual or suspected criminal offence, particularly if related to ML/TF/PWMD.

2.2.2.3 Governance, Nomination, Evaluation and Remuneration Committee (GNERC)

2.2.2.4 (GNERC)

The GNERC is particularly empowered to perform the following duties and functions:

a. To support and assist the Board of Directors in the process of nomination, removal and transfer/rotation/deployment of the Compliance Function Manager/Compliance Officer;
b. To suggest new guidance and/or recommendations within the scope of the Compliance Function personnel assessment and remuneration and of the primary Compliance Manager/Compliance Officer;
c. To provide an opinion concerning the variable remuneration proposal for the primary Compliance Manager/Compliance Officer.

2.2.2.5 Audit and Internal Control Committee (AICC)

The AICC's duties and powers are enshrined in a separate/particular regulation in accordance with the standards, provisions and regulations set forth by the National Bank of Angola and BFA's internal policies on AML/CTF/PWMD.

2.2.2.6 RISK COMMITTEE (RC)

The RC's duties and powers are enshrined in a separate/particular regulation in accordance with the standards, provisions and regulations set forth by the National Bank of Angola and the Bank's internal policies on AML/CFT/PWMD.

2.2.2.7 EXECUTIVE COMMITTEE OF THE BOARD OF DIRECTORS (ECBOD)

The ECBOD is particularly entrusted and empowered with the task of fostering, supporting and enabling the adoption of a Compliance Culture in a cross-sectional manner within the entire organizational structure of the Bank, as well as implementing and monitoring the AML/CTF/PWMD comprehensive risk management model and any relevant or potential amendments that may be made to the aforementioned model.

Within the scope of the AML/CTF/PWMD risk management, the ECBOD shall undertake and perform all the powers and duties laid down in its separate/particular Regulation, in accordance with the national legislation and regulations in force and BFA's complementary internal rules and standards, of which the following are worthy to be highlighted:

a. To ensure that is aware and has a clear, sufficient and proper understanding and knowledge on AML/CTF/PWMD risks;
b. To assess, rule and follow up through proposals and reports on the Bank's ML/TF/PWMD risk exposure and BFA's business risk as well as to implement appropriate policies, procedures and processes while enforcing their compliance in a cross-sectional manner within BFA's organisational structure;
c. To ensure that BFA's organisational structure allows, at all times, the proper implementation and performance of the applicable policies, procedures and controls, preventing conflicts of interest and, where deemed to be appropriate, fostering and enhancing the separation of functions within the Bank's organisation;
d. To refrain from any interference during the performance of the reporting mandatory duty, where, upon the completion of the preceding reporting mandatory duty, it is concluded that potential suspicions may exist;
e. To ensure that there are appropriate structures, resources and means in place and available with regard to ML/TF/PWMD identification, prevention, management, control and reporting of risk exposure;
f. To report to the Board of Directors on a timely manner on ML/TF/ PWMD risk management as well as potentially relevant Compliance procedures/processes/controls shortcomings, deficiencies or failures that may lead to potential legal risks or liability, regulatory sanctions, financial losses and/or corporate reputation harm and damages.
g. To review and assess on an annual basis, with the support of the Compliance Function, BFA's internal control system with regard to the AML/CTF/PWMD policy and identify the key risks, follow-up and monitor on the relevant mitigation action plans, as well as report to the Board of Directors on their effectiveness, efficiency and overall performance.

2.3 ML/TF/PWMD - RISK ASSESSMENT

Within the scope of its business operational activity, the Bank must adopt, develop and implement, on a mandatory basis, appropriate measures to identify, assess and mitigate the ML/TF/PWMD risks to which the Financial Institution is or may be potentially exposed. For this purpose, the Bank performs on a regular basis detailed assessments that analyse and determine BFA's risk exposure level, based on several factors laid down in the national legislation in force, as well as ensuring to implement the banking sector's best international standards and good corporate governance practices, thus reinforcing the Bank's long-term sustainability and stability and, consequently, the integrity of the overall financial system.

The accurate and effective assessment of the ML/TF/PWMD risks to which the Financial Institution or the BFA is, or may be, potentially exposed, requires the implementation of a set of measures aimed at analysing, understanding and properly mitigating such market risks, as follows:

a. The identification and recording of the ML/TF/PWMD inherent risks, as well as the identification and assessment processes implemented, thereby ensuring the corresponding documentary record-keeping;
b. The record of the assessment and appropriateness of the control means and procedures implemented with a view to mitigating the risks (identified and assessed);
c. Take into account all the factors, set out below, before setting the overall risk level and the appropriate type and extent of the mitigation measures to be applied;
d. Ongoing review of the assessments undertaken with regard to the comprehensive risks identified and assessed;
e. Use of the proper technical and technological tools, means and resources to provide data/information on risk assessments to the relevant authorities;
f. Providing evidence of the proper suitability of the procedures adopted, whenever requested by the relevant supervisory body and/or oversight authority.

2.3.1 INSTITUTIONAL RISK ASSESSMENT DUTY

The Bank in accordance with its business operational activity, undertakes annually an institutional risk assessment through the detailed identification of the Institutional and/or corporate risks to which BFA is exposed, the risks materialisation probability and the potential impact that such risks may entail in terms of ML/TF/PWMD, and accordingly, the BFA carries out the development, adoption and implementation of the appropriate mitigation measures.

For this purpose, the Bank must take into account the nature and complexity of the Banking business activity, as well as the types of Customers and other entities, the products and services provided, the distribution channels, the Customers' and/or Entities' countries or territories of origin where they operate, as well as the countries or territories in which the Bank conducts its banking business activity.

The risk weights with regard to each risk factor may be modified or adjusted, in accordance with BFA's risk level exposure. In its whole range, the risk weights must add up to 100%. The final assessment is impacted by the changes made to the risk factor weights, which in turn influence/change each risk factor's assessment.

According to the Institutional Risk Assessment, and taking into account a risk-based approach, the Bank implements detection and/or preventive control measures, sets up the frequency of these control measures as well as the corresponding nature of such control measures. To this purpose, the Bank uses proper advanced technological solutions to ensure compliance with the regulatory duties and obligations to which it is bound.

Figure 3 - Institutional Risks

Considering a risk-based approach, the institutional risk assessment should comprise at least the risk(s) materialisation probability, risk(s) impact, inherent and residual risk(s), foreseeing the following levels of risk(s):

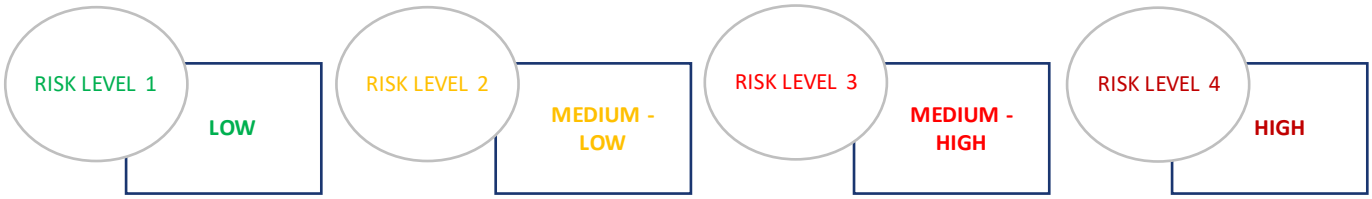


Figure 4 - Institutional Risks Levels

2.3.2 PRODUCTS, SERVICES AND DISTRIBUTION CHANNELS RISK ASSESSMENT

Whereas the importance of the risk-based approach in terms of ML/TF/PWMD for products, services and distribution channels that are provided by the Bank or shall be made available, as well as the measurement of their vulnerability within the ML/TF/PWM framework, the BFA adopts the inherent vulnerability qualitative methodology, in view of the permissibility or inadmissibility features of the misuse of products, services and distribution channels. For this purpose, it is laid down the products, services and distribution channels risk assessment standard as follows:

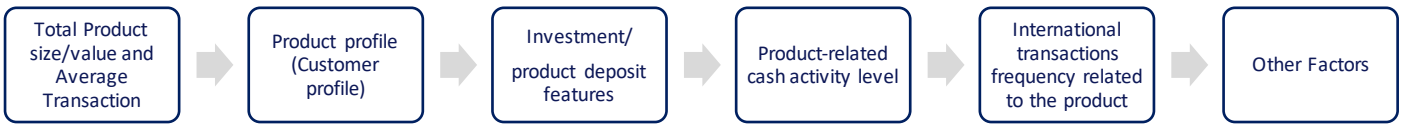


Figure 5 – Products, Services and Distribution Channels Risk Assessment Standard

2.3.3 CUSTOMER RISK ASSESSMENT

When performing customer risk assessment, the Bank must at least take into account the nature, size and complexity of the business activity it carries out, as well as the types of customers and other entities, the products and services provided, the distribution channels, the customers' and entities' countries or territories of origin as well as the countries or territories in which the Bank performs its business activity.

Accordingly, when establishing new customer business relationships, as well as during their review process, the Bank must consider at least the following factors:

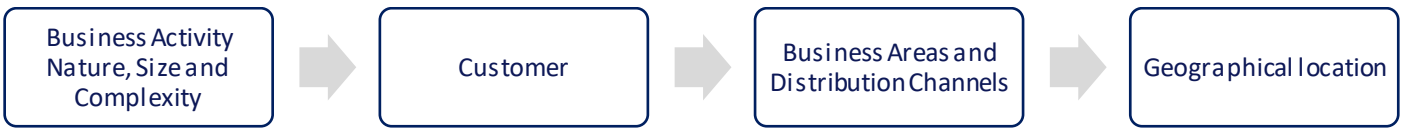


Figure 6 – Customer risk assessment factors

In view of the risk-based approach to BFA's Customer risk scoring/rating, the risk-based approach should encompass at least the following risk levels:

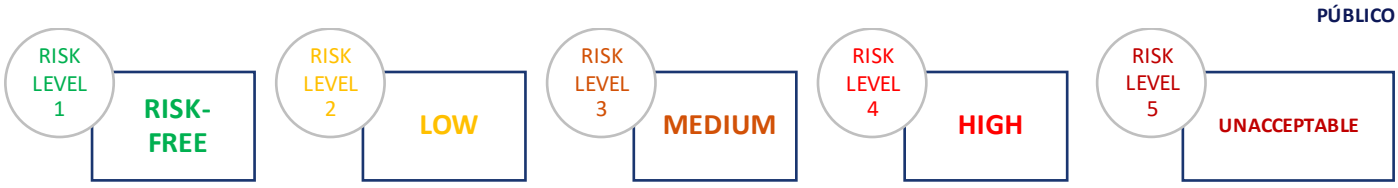


Figure 7 – Customer Risk Levels

The above-mentioned factors, as well as others that may be identified by the Bank in a later moment, will be used to calculate the final Customer ML/TF/ PWMD risk level. The risk score will dictate the type of due diligence procedures to be carried out, which can be: i) simplified; ii) ordinary; or iii) enhanced, as well as the updating time periods, and the potential need for conducting a close follow-up/monitoring of the business relationship.

Moreover, the risk assessment carried out by the Bank must take into account, on the one hand, the overall risk of the Financial Institution and, on the other hand, the probability degree and corresponding level of impact of each one of the perceived risks, in order to adopt the appropriate control mechanisms and procedures to mitigate them.

The assessment should take into account, among other regulations and internal documents, the Anti-Money Laundering (AML) – Customer Assessment/Acceptance risk matrix/framework.

2.3.3.1 CUSTOMER RISK-RATING SCORE

The Bank must rate its customers according to the ML/TF/PWMD risk level that they entail to the Financial Institution ("BFA"). The following elements are only indicative criteria that help to rank/classify the Customers' inherent risk:

a. **Customers with an ("Unacceptable Risk")**

- Customers whose accounts have been closed by recommendation of the Internal Audit and Inspection Department, within the scope of their fraud management responsibilities;
- Customers whose accounts have been closed on the Compliance Department's instruction;
- Customers who are on the United Nations sanctions list and/or in other international bodies sanctions list to which the Bank adheres to, as well as relevant foreign governments and local regulatory authorities, whose engagement or involvement in any type of business relationship is barred/prohibited by the Bank;
- Customers in respect of whom the Bank and/or the Regulatory Bodies/ Oversight Authorities have issued an order prohibiting the provision of banking current account services;
- Shell Banks / Shell Entities/ Ghost Corporations/ Front or Letterbox Companies;
- Customers who do not have a business license or whose licenses have been withdrawn;
- Customers who, for some reason, are not submitted to regulatory oversight;
- Other customers that may be eventually identified by the Bank.

b. **High-Risk Customers**

- PEPs, family members and very close associates;
- Non-banking Financial Institutions;
- Casinos or other gaming/ gambling related industries;
- Industries trading in jewellery, antiques and fine art works;

- Legal Persons whose shareholders or other entities holding in fact a controlling stake/position, reside in and/or do business with high-risk countries or jurisdictions and/or are incorporated in a tax haven / offshore jurisdiction in accordance with BFA's current Reference List of High-Risk ML/TF/PWMD Countries or Jurisdictions;
- Customers who are on the sanctions list of the United Nations and other International Organisations, namely HTML, OFAC and EU and relevant foreign governments and local regulatory authorities, whose setting up of business relationships is not prohibited by the Bank or the Regulatory Authority;
- Local Government Bodies and Public Institutions;
- Diplomatic Embassies and Consulates;
- Travel and Tourism Agencies;
- Non-governmental and non-profit organisations
- Legal persons operating in the mining sector;
- Other Customers listed by the Regulatory Authority as high-risk Customers;
- Customers identified by the Compliance Department as high-risk customers.

c. **Medium-Risk Customers**

- Customers with a proven remuneration settled/deposited at the Bank and who are not involved in proceedings connected with the practice of ML/FT/PWMD criminal offences and/or activities, as well as involvement in other types of financial crimes;
- Incorporated and regulated financial institutions operating in countries or regions that comply with strict financial regulatory requirements on AML/CFT/PWMD;
- Listed companies and subsidiaries on regulated markets operating in countries or regions that comply with strict regulatory requirements on information disclosure;
- Other Customers identified/rated as medium-risk customers by the Bank.

d. **Risk-Free and Low-Risk Customers**

- Customers whose ML/TF/PWMD risk-rating criteria do not fit into the previous classifications.
- A state-owned entity or a legal person under public law, and of any business form/nature, incorporated in the national, regional or local government;
- A public authority or body subject to clear, audited and supervised accounting practices;
- Natural Persons, holders of a qualified bank account.

2.3.3.2 CUSTOMERS' RISK RE-RATING (RECLASSIFICATION)

In order to ensure full compliance with BFA's Customer's risk profile rating/classification, the Compliance Department must ensure the implementation of full re-rating/reclassification procedures and/or processes of the Bank's Customers' portfolio in accordance with the risk criteria laid down in the current Policy.

2.4 IDENTIFICATION AND DUE DILIGENCE DUTY

Due diligence measures comprise a set of procedures and processes that enable the Bank to reasonably know the identity of the customers and other legal entities and to keep a complete record of the data/information details in order to understand the customers business nature, core activity and its risk profile.

The Customer identification data/information details and the probative/supporting/evidential documentary means that must be submitted to the Financial Institution are laid down in BFA's internal regulations related to Customer Acceptance. Moreover, internal regulations set out the minimum customer information data to be obtained at the beginning and during the course of the business relationship, or when occasional transactions are undertaken, notwithstanding the particular ML/TF/PWMD risks that have been identified.

A proper understanding and knowledge of the Bank's Customers is a key tool and component for ensuring that not only does the Bank perform due diligence to identify and verify its Customers at the start of a business relationship, but also in terms of providing financial products and services, by adopting and implementing appropriate precautionary measures to mitigate the ML/TF/PWMD risks to which the Financial Institution is exposed within the scope of its business operational activities.

In the event that the Bank determines that it is impossible to perform any of the due diligence measures listed below, it shall not proceed with the establishment or maintenance of the business relationship, nor with the performance of any potential financial transaction, and shall undertake or perform the refusal or abstention duty, as the case may be.

2.4.1 CUSTOMER ACCEPTANCE MEASURES

The Customer acceptance rules, establishes a set of information that is necessary to determine the Bank's interest in (i) setting up a Customer business relationship, (ii) keeping/maintaining a Customer business relationship and (iii) terminating an isolated transaction with a non-Customer or a business relationship.

The Customer acceptance process contemplates and addresses the client's inherent risk and for this reason comprises three (3) separate stages, as depicted and detailed hereunder.

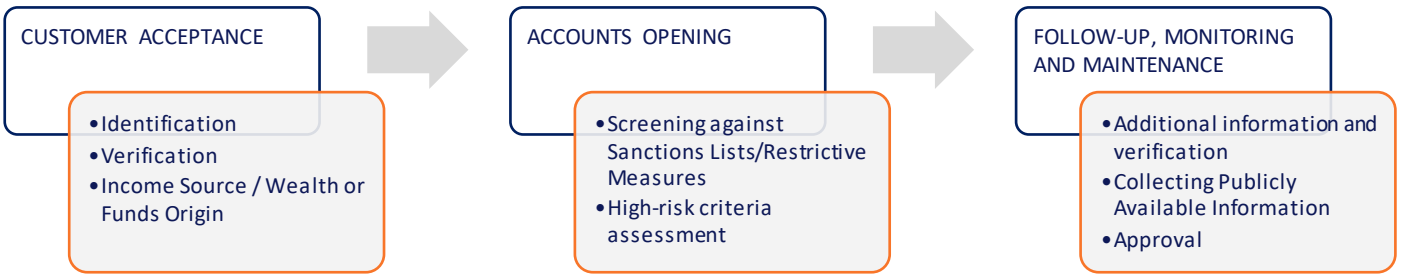


Figure 8 – Customer Acceptance Stages

2.4.2 KNOW YOUR CUSTOMER ("KYC")

The "KYC" scheme/framework plays an important part in the Customer acceptance process, and should generally comprise the following stages:

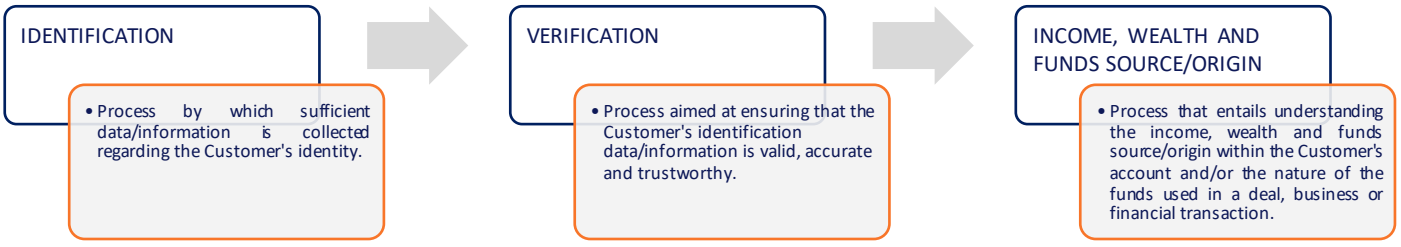


Figure 9 –Know Your Customer Stages

The "KYC" scheme/framework is pivotal at an operational level and with a different impact/outcome when it comes to face-to-face "KYC" and/or non-face-to-face "KYC" risk assessment, and therefore strong and sound control mechanisms should be put in place for non-face-to-face "KYC" risk assessment.

2.4.3 "KYC" REVIEW TIME SCHEDULE

The Customer data/information details ("KYC") review frequency should encompass the following maximum periodicity:

Figure 10 – Know Your Customer Time Schedule

The timing of the ordinary review is waived when the following particular events occur:

a. If the Customer already has an updated account;
b. If the Customer joins new products and services;
c. If the Customer renews products and/or services;
d. If the Customer voluntarily informs the Bank about a change in his/her/its data/information details;
e. If the Bank identifies and has elements/information that justify the customer data being updated, with the exception of personal data;

When the Financial Institution or the Bank is dealing with inactive Customers,There must be an understanding, insight and knowledge regarding ML/TF/PWMD risks, a guarantee of an effective, efficient and appropriate implementation of ongoing mitigation methods, procedures and processes, as well as an overall understanding of the Customers and how th ey carry out their business activities and operations. Accordingly, the proper structural conditions must also be in place to reassess and update the "KYC" data/information details, whenever changes may occur, in particular with regard to:

- Customer identification details and other relevant persons for the account opening/information update process, that is, names and identification document numbers;
- Customers' high-risk criteria, namely:

Figure 11 – Customers' High-Risk Criteria

2.4.4 TERRORIST FINANCING SCREENING

All Customers, legal representatives, attorneys-in-fact and other relevant persons who carry out isolated operations, as well as the payment beneficiaries, must be screened against international lists of Sanctions/Restrictive Measures, with greater focus on

the UNSC lists, without neglecting the other lists to which BFA adheres to, so as to ensure that no operations are carried out or commercial relations kept with natural or legal persons that may be associated with terrorist activities.

2.4.5 DUE DILIGENCE CLASSIFICATION

The Bank adopts and implements identification and due diligence measures with regard to its Customers and Suppliers, as well as with respect to all other legal entities or organizations, both prior to the commencement and during the course of a business relationship.

The due diligence measures comprise a set of processes that enable the Bank to reasonably know the identity of its customers and other legal persons or entities as well as to retain the data/information in order to understand the Customer business nature, operational activity and its risk profile.

Accordingly, the BFA must comply with the following types of due diligence:

ORDINARY DUE DILIGENCE	SIMPLIFIED DUE DILIGENCE	ENHANCED DUE DILIGENCE	ONGOING DUE DILIGENCE
• Carried out in a standardised manner for all Customers.	• Carried out for entities with proven ML/TF/PWMD low risk.	• Carried out for high-risk entities, PEP's and medium-risk entities (when applicable)	• It is underpinned by the ongoing process of risk assessment from the Customer's profile viewpoint, as well as in the Customer's transactional profile.

Figure 12 – Types of Due Diligence

In the course of the business relationship between the Bank and its Customers, despite the adoption and implementation of identification and due diligence measures, the Bank is guided by an ongoing monitoring of risk assessment, maintaining control measures from an operational and transactional perspective and, at the appropriate time and whenever deemed to be necessary, requests that certain customers' information data be maintained updated.

The Customer's due diligence is dependent on the risks identified and recognised in the account-opening process, which have an impact on the relevant risk calculation. As a result, and in accordance with the potential risks identified, it will be ascer tained whether it is necessary to carry out a simplified, ordinary or enhanced customer due diligence.

2.4.5.1 Ordinary Due Diligence Measures

Within the scope of ordinary due diligences processes, the Customers must be subject to the ordinary identification procedures set out in the legislation and BFA's internal regulations in force.

In view of the Bank's specific business operational activities, the ordinary due diligence is applicable to the Bank's customer portfolio in general and mainly consists of collecting the customer identification data/information details as set forth by law and BFA's internal regulations, a mandatory requirement for the establishment and development of any business relationship.

It should be highlighted that before establishing or maintaining any business relationship or carrying out any operations, th e Bank must ensure that it has adopted the appropriate due diligence measures to collect the Customers' identification de tails and the relevant supporting documentary evidence.

2.4.5.2 SIMPLIFIED DUE DILIGENCE MEASURES

Within the scope of the Customer identification and verification procedures, in accordance with the applicable law and regulations in force, the Bank may implement simplified due diligence measures. The application of this type of due diligence is limited to those cases/scenarios in which a proven low risk of ML/TF/PADM is identified, either in business relationships, or in occasional transactions, or even in other potential operations that are carried out. The risk assessment should be performed by the Bank or by the supervisory bodies and/or oversight authorities.

A certain number of factors are taken into account for the purposes of proving reduced/low risk, namely:

a. The purpose of the business relationship;
b. The level/value/number of assets per Customer or the volume of transactions and turnover carried out;
c. The business relationship regularity and/or lifespan.

Moreover, the Customer must fall into one of the following categories: (i) a state-owned entity or a legal person under public law, of any nature, incorporated in the national, regional or local government; (ii) a public authority or body subject to audited accounting practices and regulated by law; and (iii) natural persons holding a simplified bank account.

The data/information collected should be both relevant and comprehensive and made available to the competent authorities at all times.

The performance of a simplified procedure does not exempt the Bank from monitoring the business relationship in order to identify unusual or non-standard transactions and even limit the Customer's risk rating and the risk level escalation in the course of the business relationship.

2.4.5.3 Enhanced Due Diligence Measures

When the Financial Institution or the relevant sector-specific authorities identify an increased risk of ML/FT/PWMD regardless of its source and/or nature, the Bank ensures the strengthening/enhancement of the measures adopted within the scope of the customer identification, verification and due diligence mandatory duty.

The enhanced due diligence measures should be applied at the following steps/stages:

Figure 13 – Enhanced Due Diligence Steps/Stages

Accordingly, in order to verify the authenticity of the identification/data details or to corroborate/confirm the lawfulness of certain operations, the Customers must provide additional information. The measures in this regard include, in particular:

a. The request for independent and reliable documentation;
b. Conducting on-site visits to the Customers' facilities, when applicable;
c. Conducting research in reliable public sources and/or in tools under the Bank's management for Anti-Money-Laundering, Counter-Terrorist Financing and Proliferation of Weapons of Mass Destruction (AML/CTF/PWMD);
d. Detailed analysis of the information contained in the documentation provided by Customers;
e. Consulting Customers' credit records;

f. The ascertainment and/or fact-finding of the Customers' individual financial situation, the wealth and/or the Customers' funds source;
g. Understanding the purpose of establishing a business relationship with the Bank, namely by identifying the transactional purposes, operating jurisdictions and related counterparties;
h. The screening of the entity, market players/participants, beneficial owners, among others that may be necessary on a case-by-case basis, against international sanctions lists (ONU, OFAC, EU, HMT) and PEPs, as well as public information available in reliable sources;
i. To require the involvement and assistance of upper/senior hierarchical levels for Customers' approval and acceptance;
j. Other measures that may be identified by the Compliance Department within this scope.

All the procedures, measures and due diligences carried out within the scope of the Customer's Identification & Verification (ID&V) process, must be the object of a centralised registry/storage and documentary record keeping within BFA's internal control system, so that it is possible at any time to access the Customer's data/information, as well as to make this information available to the sector-specific regulatory authorities and other entities that express a well-founded interest and legitimacy in such information, whenever deemed necessary.

2.4.5.4 ONGOING DUE DILIGENCE MEASURES

In order to ensure that the Bank has current and complete knowledge of its Customers, it is essential to constantly monitor its Customers. On the one hand, this monitoring will ensure regular and in-depth information update, as well as the identification of breaches in the customer profile and the performance or attempts to perform unusual, suspicious or non-standard transactions, and, on the other hand, the customer risk profile assessment with regard to restrictive measures or sanctions/designated entities.

Customer monitoring should be able to identify, in a timely manner, relevant changes to the Customers' operating or functional pattern, as well as the presence of high-risk entities, particularly with regard to:

a. The funds' origin/source and purpose/end-use;
b. The transactions' purpose;
c. The changes in the value and volume of transactions;
d. The involvement/participation of third parties;
e. The intervention of PEPs, family members and very close associates;
f. The intervention of designated entities;
g. Other market players, participants or third parties that may be potentially designated/stipulated by the Bank.

The Bank ensures the implementation of the appropriate tools, mechanisms, and procedures for the effective and successful management of ML/TF/PWMD risks, namely with regard to both the Customer identification data update and the Customer behavioural monitoring.

2.4.6 CUSTOMER APPROVAL & ACCEPTANCE

The guiding principles underlying the mandatory duty of Customer Identification & Verification (ID&V) and Due Diligence are extensive to all Customers, legal representatives, and beneficial owners, and are therefore dependent upon the risk materialisation that they entail and are exposed to and that ultimately defines them.

The Bank does not allow any Customer to open an account before obtaining all the identification data details and the relevant supporting documentation, with the legally established exceptions, and without the processes having passed through the different levels of approval, operationally designed in accordance with the identified levels of risk, as follows:

a. Medium and low risk customers: subject to the ordinary procedure;
b. Customers that are Politically Exposed Persons ("PEPs") or Clients that are Legal Persons whose shareholdings and/or direct and/or indirect control in the share capital is held by a PEP: validation by the Back Office, issuance of an opinion by the Compliance Department and approval by the Executive Committee of the Board of Directors ("ECBOD");
c. Other High-Risk Customers: back-office validation and the issuance of an opinion by the Compliance Department.

2.5 DUTY TO REPORT

Whereas the Bank, in the course of its business activity and day-to-day operations, identifies any possible case or event that may be viewed/classified as a ML/TF/PWMD criminal offence, as well as the practice of other potentially related criminal economic activities, either within the scope of the setting-up or upholding of a business relationship, or within the scope of the Customers' accounts follow-up and monitoring, the Bank must report/notify such transactions/activities/offences and/or the Customers directly involved to the relevant oversight authorities.

In accordance with the legislation in force, whenever the Financial Institution (BFA) identifies, is aware or has sufficient reasons to suspect that a transaction that may be connected with the practice of a ML/FT/PWMD criminal offence, criminal economic activity/act or of any other nature, has taken place, is in progress or has been attempted, it shall immediately notify the Financial Intelligence Unit ("FIU").

Accordingly, the Compliance Officer shall ensure the fulfilment of the reporting duty to the Financial Intelligence Unit ("FIU") of any information/data/facts that may indicate the potential perpetration of a ML/TF/PWMD offence or criminal activity. For this purpose, the Compliance Officer shall use the following template:

a. **Cash Transactions Reporting**;
b. **Suspicious Transactions Reporting**;
c. **Legal Entities and Groups of Designated Persons Reporting;**
d. **Spontaneous Reporting.**

The reporting of transactions considered suspicious within the scope of the ML/TF/PWMD framework is a cross-sectional mandatory duty for all BFA's Staff Members, who must report any cases, events or suspicious facts and/or circumstances to the Compliance Department (“CD”). Accordingly, it is under the Compliance Department duties to analyse and assess any potential suspicious cases, events or scenarios and to decide whether to notify the relevant supervisory authorities in this regard.

Moreover, the Bank shall ensure that all information and documentation, as well as the analyses and assessments performed, are duly recorded and made available to the relevant oversight bodies.

The submission of information to the CD should be made through the following e-mail address: dir.compliance@bfa.int

2.6 DUTY TO REFRAIN

Within the scope of the business relationship with its Customers, the BFA has adopted and implemented the necessary and appropriate control measures and, accordingly, undertakes a Customer pre-assessment prior to the performance of any operation and/or transaction.

In order to verify the authenticity of the information data provided, as well as the effectiveness of the control measures implemented within the ML/TF/PWMD framework, particularly in terms of customer identification, due diligence and information/data verification, the Bank may abstain/refrain as follows:

a. Upon acceptance of a Customer' transaction instructions or operations, when verifying that the Customer's identification data or account information is not updated;
b. When carrying out an operation/transaction, whenever it is ascertained that a given transaction gives rise to reasonable suspicion and is likely to involve or represent a criminal offence;
c. The scenarios, cases, or events in which the Bank has no assurance that the transactions may be potentially associated with ML/TF or any other criminal offence.

2.7 DUTY OF REFUSAL

The Bank reserves the right to refuse the setting up of a business relationship, or the performance of transactions, in the event of a Customer failure to comply with the identification and due diligence duties, and in accordance with BFA's degree of satisfaction, being entitled to perform the following actions:

Figure 14 – Actions within the scope of the duty of refusal

2.8 DUTY OF COOPERATION

The BFA is guided by the key principle of cooperation with the Angolan authorities within the scope of all the banking business matters and domains of the organisation. As a result, BFA has implemented a procedure that regulates the management of cooperation with the relevant oversight bodies and/or supervisory authorities.

In accordance with the applicable law, the Customer's names and other personal information details, their deposit accounts data, relevant account transactions/movements and other banking operations are subject to professional secrecy (banking secrecy), and the Financial Institution may only disclose them to third parties when complying with the applicable law (in compliance with regulatory duties) or after receiving authorisation granted by the actual Customer or Legal Representative, upon submission of the relevant power of attorney, which must compulsorily contain the following information:

a. The Customer's identification and his/her valid signature as per ID document, or signature for account activity management;
b. The clear identification (personal data) of the power of attorney holder to whom the Customer has given permission to deliver the information.

2.9 DUTY OF SECRECY

The Bank and its direct and indirect Staff Members are strictly forbidden from disclosing any Customers' or third parties' information/data, including the Customer's risk levels, potential monitoring actions or other information on ML/TF/PWMD, apart from those individuals and/or BFA's management/supervisory departments/areas particularly appointed internally for such purpose.

All BFA's Staff members who are engaged in the analysis and/or reporting of suspicious transactions must refrain from discussing or disclosing sensitive information that may jeopardize the integrity of an ongoing investigation in progress or a potential new investigation. In addition, the Staff members must refrain from sharing this type of information with Customers as otherwise there is a risk of tipping-off by them and, as a result, the actual or potential investigation of ML/TF/PWMD activities may be affected and/or compromised.

The breach of the bank secrecy duty may, in addition to disciplinary sanctions, trigger the application of criminal sanctions, in accordance with the legislation in force. The bank secrecy duty is not suspended with the end of the Staff members' functions or services.

Without prejudice to the foregoing provisions, the BFA is committed to cooperate with all the oversight/supervisory authorities, namely the National Bank of Angola (BNA) and the Financial Intelligence Unit (FIU), as well as with the criminal investigation authorities.

2.10 MONITORING DUTY

In order to ensure that regular, periodic and systematic communications are performed in a timely manner, the implementation of appropriate and effective mechanisms, tools, systems and controls are ensured by the Bank with a view to guaranteeing the effectiveness of the following measures:

a. Cross-Sectional Processes
   - The Bank implements cross-sectional preventive processes to identify potentially suspicious conducts or behavioural patterns concerning ML/TF/PWMD criminal offences;
   - The Bank implements processes to regularly assess and update the list of high-risk countries/jurisdictions;
   - The Bank implements processes for the preventive identification of Customers or potential Customers who are PEPs, family members and very close associates, as well as control over negative public information;
   - The Bank puts in place processes for identifying and reporting potentially suspicious conducts or behavioural patterns concerning ML/TF/PWMD criminal offences/practices and for monitoring cash transactions;
   - The Bank implements reporting and cooperation processes with the Supervisory/Regulatory Authorities;
   - The Bank implements processes to control mandatory ML/TF/ PWMD trainings;
   - The Bank implements archive management processes and statutory record-keeping of its customers' documents;
   - The Bank implements processes for the termination of the business relationship with BFA and for Customer risk escalation.

b. Tools
   - The Bank implements product and corporate risk assessment tools;
   - The Bank implements automatic tools for opening and updating customer accounts within the scope of its documentary repository;

- The Bank implements automated filtering tools (restrictive measures, PEPs and family members and close persons) to ensure compliance with controls for the procedures of opening and updating accounts, and transactional processes in both domestic and foreign currency;
- The Bank implements automated tools aimed at identifying customer conducts and behavioural patterns that are potentially under suspicion of engaging in ML/TF/PWMD criminal offences/practices.

In addition, the tools implemented enable the following:

c. The ongoing monitoring of the business relationships in order to identify, on the one hand, the Customers' identification data timeliness, and, on the other hand, the PEP customers acquisition quality or the restrictive measures exposure. To this end, Customer portfolio regular filtering is carried out against PEPs' directories, restrictive measures, watchlists, among other procedures that are considered relevant;

d. The Customers' behavioural patterns transactional analysis ongoing monitoring, through the identification of certain events, cases or situations that require analysis and assessment, not only with regard to the Customers but also regarding their counterparties, and which may trigger the implementation of the duty to abstain and/or the duty of refusal and/or the duty to report.

2.11 CORRESPONDENT BANKING RELATIONSHIPS

The Correspondent Banking Relationships refer to the provision of financial services by a Bank, financial institution or other entity providing similar services (correspondent bank) to another Bank, financial institution or other entity of equal nature that is its Customer (respondent bank). These financial services may include cash management, processing of funds through wire transfers, foreign exchange transactions, among others.

Prior to establishing a correspondent banking relationship, the BFA is required to obtain the necessary corporate identification details, which are set forth in the applicable legislation, as follows:

a. Identification of legal and regulatory provisions on ML/TF/PWMD;
b. Ownership information data (corporate/shareholder structure) and management body (ies);
c. Business scope and size;
d. Business relationship purpose;
e. The AML/CTF/PWMD measures implemented by the correspondent bank;
f. Customers' oversight procedures and performance;
g. Regulatory Licences to conduct banking activities;
h. Among other information deemed to be appropriate.

In the event that the Correspondent Banking Relationship is set up with branches or subsidiaries, the Bank shall collect the information of the parent company in order to assess the relevant ML/TF/PWMD risk to which the correspondent bank may be potentially exposed and to better classify/categorise its counterparty.

The following enumerates some criteria that are used to assess a correspondent bank and/or financial institution high-risk level within the scope of the Correspondent Banking Relationships:

i. The business location/activity is carried out in countries, jurisdictions or regions commonly known to lack appropriate and effective control measures with regard to AML/CTF/PWMD and/or where there are high rates of serious/major criminal

activities, embezzlement or financing of terrorist activities or to whom sanctions/restrictive measures have been implemented;

j. Offshore Banks;

k. Entities managed or owned by PEPs;

l. Entities providing other financial institutions or their Customers with high-risk services, including direct account settlement, etc;

m. The Entities' net operating income is primarily generated from their high-risk ML/TF/PWMD customers;

n. Other events, cases or situations acknowledged and/or stipulated by the Bank.

2.12 RESTRICTIVE MEASURES (SANCTIONS)

2.12.1 RESTRICTIVE MEASURES MANAGEMENT

The purpose of the special risk of Sanctions/Restrictive measures within BFA's Internal Control programme is to ensure that the establishment and running of the business relationships, contracting/subscribing to new products and services, as well as the customers' performance of transactions, in no way implies the intervention of any designated entities or countries.

Accordingly, it is stipulated that no financial services shall be provided to sanctioned countries, entities or designated persons where the prohibition is provided for in the regulations pertaining to the relevant listings/directories to which the Bank adhered to.

The BFA recognises the following relevant authorities for issuing restrictive measures/sanctions:

a. The United Nations Security Council: The Bank is bound to rigorously comply with the restrictive measures originating from binding UNSC resolutions. Thus, the BFA has implemented tools capable of detecting, at all times, potential cases of non-compliance with the restrictive measures in force, without compromising BFA or the integrity of the financial system;

b. Office of Foreign Assets Control Special Designated Nationals (OFAC/SDN) of the United States of America: the BFA is bound to comply with the restrictive measures issued by the OFAC concerning its business operations and/or transactions. Thus, the Bank has a special responsibility when performing transactions with the USA territory/jurisdiction and/or USA - Natural or Legal Persons and/or in USD currency;

c. Her Majesty's Treasury (HMT) of the United Kingdom: The Bank is bound to comply with OFSI restrictive measures concerning its transactions/operations, in particular when performing transactions with the UK territory/jurisdiction and/or with UK natural or legal persons and/or in GBP currency;

d. European Union (EU): within the scope of its business activity and taking into account the global financial landscape in which BFA operates, the Bank complies with the restrictive measures/sanctions issued by the EU in order to ensure its cross-border trade connections and to facilitate the use of its banking and financial services in accordance with the European circulation needs of its Customers.

The restrictive measures/sanctions can consist of several types and assume different forms, including the following:

e. **Diplomacy**: A set of restrictions aimed at affecting diplomatic relationships with certain jurisdictions.

f. **Trade**: A set of restrictions on trade relationships between countries including:

- The arms embargo and related equipment/material such as ammunition, military vehicles and equipment, paramilitary equipment and spare parts for the aforementioned;

- Export and/or import restrictions on certain dual-use goods and equipment and on equipment which might be used for in-country repression;
- Embargoes on key sectors of the economy, such as oil and natural gas, among others;
- Prohibition and control of the provision of certain types of technical assistance or training, financing or financial assistance;
- Transport sector constraints.

g. **Financial**: A set of restrictions on financial institutions, services and/or markets, which may lead to the prohibition of monetary financing, freezing of funds, among others.

The Bank shall ensure that the tools, means and resources provided for customer screening purposes against sanctions lists are updated with the appropriate regularity and that Customers are screened when opening, setting up and keeping the business relationship, and also, on a regular basis, each time changes are made to the aforementioned sanctions lists.

In addition, it should be highlighted that restrictive measures may have as their origin acts promoting terrorism or the proliferation of weapons of mass destruction, namely through the supply or collection of funds or assets intended for the planning, preparation and/or effective practice of terrorist acts and/or intended for the proliferation of weapons capable of causing a large number of casualties through a single use, namely nuclear, chemical and radiological weapons.

2.12.2 RESTRICTIVE MEASURES ASSESSMENT METHODS

Whereas the restrictive measures may be motivated by acts that promote terrorism or the proliferation of weapons of mass destruction, in particular by the provision or collection of funds or assets intended for the planning, preparation and/or carrying out of terrorist acts and/or weapons capable of causing large numbers of casualties through a single use, including nuclear, chemical and radiological weapons.

During the Customer's acceptance process and upholding of the business relationship, their assessment, screening and review must be carried out, with regard to sanctions and monitoring of transactions. The purpose is to perform a Customer review and to identify the transactional risk. To this end, some key elements are listed that should be highlighted and addressed within the scope of the ongoing due diligence/monitoring of compliance with the restrictive measures, as follows:

a. Customer Assessment:
   - Sanctions screening that is not restricted to the Customer, per se, also taking into account shareholders, beneficial owners, legal representatives, related parties, among others;
   - Duly performed investigation, listing the Customers' identification data, pinpointing the types of sanctions, the Bank's level of exposure assessment, and communication and reporting of suspicious cases, if applicable.
   - Regular assessments:
   - If the Customer is included in the sanctions list, in the Relatives and Close Associates (RCAs) list and/or is a Special Interest Person (SIP)/ Special Interest Entity (SIE) subject to adverse media, the BFA shall proceed with an enhanced due diligence in view of the potential need for the Bank to perform its duty of refusal;

b. Transactions Assessment:
   - Regular transactional analysis, which should focus not only on the Customer, but also on his business and transactional activity, cross-checking the counterparties' data (those involved in the transactions) with sanction lists, in order to identify in a timely manner transactions that should be rejected and/or blocked.

The compliance with the restrictive measures, in addition to the interdiction to establish business relationships, entails the implementation of the abstention and refusal duties, when applicable, and may result in the enforcement of the freezing of funds and/or economic resources.

Failure to comply with the restrictive measures by the Bank may result in administrative or criminal liability, as well as accessory penalties and corporate reputational harm or damage.

2.12.3 SCREENING PROCEDURES

Within the scope of the automated screening procedures, the technological tools, resources and IT systems implemented to perform automated Customer screening against sanctions lists, generates notifications that are analysed in a centralised manner and thus allowing the BFA to analyse and assess the correlation information data, or otherwise, of the details contained in the notification. In accordance with the results of such analyses, the Bank may proceed, as appropriate, in the following cases:

a. False positive: notification sent to record-keeping;
b. True positive: refrain, report, refusal.

2.13 FINAL PROVISIONS

2.13.1 REPORT ON AML/CTF/PWMD

The BFA complies with its reporting duties to the National Bank of Angola, sending an annual report containing information data on its internal control system, as well as the information concerning the regulations issued by the supervisory authority, up until 31 January of each year, regarding the time period between 1st January and 31st December of the previous year.

2.13.2 COMPREHENSIVE CLAUSE ON AML/CTF/PWMD

The existence of a comprehensive clause on AML/CTF/PWMD becomes mandatory in all agreements signed between the Bank and its Customers/Suppliers/third parties, in which the parties declare their knowledge of the current policy as well as of the Angolan regulations in force on the AML/CTF/PWMD subject matter, and pledge to fully comply with its terms and provisions, by refraining from performing any unlawful or illegal business or economic activity that is or may be a violation of the applicable law.

2.13.3 DOCUMENTARY RECORD-KEEPING

The Bank shall keep on record all the documentation concerning the Customer's acceptance and approval procedure, as well as the transactional records and correspondence exchanged, which shall be kept for a minimum period of ten (10) years.

All information details collected concerning the Customer and data obtained through the CDD process shall be recorded and archived.

All records shall be filed/archived in a secure manner against damage by fire, water, or system failure, and shall be always available upon request by the relevant authorities.

2.13.4 TRAINING AND AWARENESS-RAISING

The BFA provides its Staff Members with regular training appropriate to the work they perform, which may be included in general training on the Compliance subject or other topics deemed to be appropriate. For this purpose, the Bank provides and implements a training policy and/or training plan for all its Staff Members including the members of the Board of Directors and

the Supervisory Board.

It is the collective duty of all senior managers to raise the awareness of all BFA's Staff Members on the need for and importance of complying with the provisions of the current Policy, as well as to encourage them to express and submit any doubts or concerns they may have on the implementation of the current policy.

2.13.5 ACTIONS/NON-COMPLIANCE OUTCOMES AND DISCIPLINARY LIABILITY (MEASURES/SANCTIONS)

The infringement/breaches of the provisions laid down in the current Policy, applicable laws or regulations on AML/CTF/PWMD represents an extremely serious offence, malpractice and/or negligence, which may result in the application of labour sanctions and, in the worst-case scenario, dismissal with just cause. This scenario does not necessarily comprise a possible legal action against the Staff member, be it criminal, transgressional or of any other nature.

2.13.6 LIABILITY DUE TO INFRINGEMENT/BREACH

The Bank is fully and jointly liable for the payment of fines and charges imposed on its directors, managers, authorised proxies, corporate legal representatives, or Staff Members for committing offences that are punishable under the law.

The Board of Directors members who failed to avoid the practice of an infraction when they were in a position to do so, are individually and subsidiarily liable for the payment of the fine and charges imposed on the Bank.

2.13.7 REVIEW AND ENTRY INTO FORCE

The current policy guidelines shall be reviewed and updated, at least annually and/or whenever deemed to be relevant and appropriate, in order to incorporate any amendments made to national and/or international laws and regulations, and a versions record (documentary record-keeping) must be kept so that it is possible to access and check the changes over time.

DOCUMENTARY CONTROL

DOCUMENT PROPERTIES

Table 4—Document Properties

DOCUMENT PROPERTIES					
Name	AML/CTF/PWMD POLICY				
Type	Policy	**Classification**	PUBLIC		
Version	2	**Reference**	POL/DC/001/V02	**SG Reference**	2022-262-BFA CA
Approval date	28/10/2022	**Approved by**	Board of Directors ("BOD")		
Publication Date	04/11/2022	**Effective Date**	04/11/2025		
Target Audience	Public				
Availability	This document is available and updated on the Bank's intranet and on the Internet via the BFA's official website. Normative | Compliance | Anti-Money Laundering, Counter-Terrorist Financing | POL of AML/CTF/PWMD				
Main Changes	Policy review and adjustment in accordance with the Bank's legal/regulatory and operational changes, namely: • Introduction of Institutional Risk and Products/Services assessment; • Structural introduction of legal/regulatory subject matters within the scope of the "Statutory Duties" framework; • Introduction of the SCI draft requirement on AML/CTF/PWMD; • Change of the "KYC" review schedule; • Adjustment of the Staff Members accountabilities according to the changes of BFA's corporate governance standards, rules and/or regulations;				

VERSION CONTROL

VERSION	APPROVAL DATE	APPROVED BY	ENTRY INTO FORCE	MAIN CHANGES
2	10/28/2022	Board of Directors	11/4/2022	Policy review and adjustment in accordance with the Bank's legal/regulatory and operational changes, namely: • Introduction of Institutional Risk and

				Products/Services assessment; • Structural introduction of legal / regulatory subject matters within the scope of the "Statutory Duties" framework; • Introduction of the SCI draft requirement on AML/CTF/PWMD; • Change of the "KYC" review schedule; • Adjustment of the Staff Members accountabilities according to the changes of BFA's corporate governance standards, rules and/or regulations;
1	7/31/2020	Board of Directors	8/3/2022	First Publication