AML / CTF Compliance Manual

NOVARA, S.A. DE C.V.

El Salvador

August 2025

- This AML/CTF Compliance Manual (Manual) shall apply to all branches and subsidiaries of NOVARA, S.A. DE C.V (Company).
- This Manual consists of main file, which established general principles for certain procedures in the course of the Company's activity and annexes, which describe certain processes and/or requirements in details.
- Implementation of this Manual will not detract from the obligation to comply with any other local law and is not to be regarded as enabling the implementation of acts that have been prohibited or restricted by local laws.
- The Company maintains full cooperation with law and regulatory authorities in legislations, investigations, and inquiries in El Salvador and abroad.
- This Manual shall be accepted and approved by the General Shareholders.

Administrative information

Company name: NOVARA, S.A. DE C.V.;

Registration number: 362 DEL LIBRO 4926;

Address: Av. La Revolución 25, Col. San Benito, Local 6, Presidente Plaza, San Salvador, El Salvador;

TIN: 0623-310725-107-0.

I. Table of Contents

II. Acronyms

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Counter-terrorist financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Investigation Unit
ML	Money Laundering
PEP	Politically Exposed Person
FPWMD	Financing for Proliferation of Weapons of Mass Destruction
DNFBP	Designated Non-Financial Businesses and Professions
ODD	Ongoing Due Diligence
RBA	RBA Risk-Based Approach
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
TF	Terrorist Financing
UN	The United Nations
DASP	Digital Asset Service Provider
BSP	Bitcoin Service Provider
STR	Suspicious Transaction Report
LCLDA	Ley Contra el Lavado de Dinero y Activos

III. Glossary

1. Designated Non-Financial Businesses and Professions (DNFBP): casinos and other games of chance, real estate agents, dealers in precious metals or precious stones, dealers in any saleable item with a price equal to or greater than USD 15,000, lawyers, notaries, other independent legal professionals and accountants, external auditors, Trust and Company Service Providers.
2. Customers: All natural or legal persons with whom the Company establishes a contractual relationship by virtue of which the supply of goods or services for direct consumption is sought.
3. Counterparties: natural or legal persons with whom there are business, contractual or any other type of relationships for the purpose of obtaining or providing the supply of goods or services for a purpose other than direct consumption.
4. Accounts: digital mechanisms for users/customers to carry out certain asset's transactions, including buying and selling, specifically of digital assets, electronic and fiduciary money.
5. Employees: natural persons who provide services, on a permanent basis and under a subordinate relationship, to the Company. For the purposes of implementing this Manual, this category also includes those persons who are linked to the Company through a contract for the provision of professional services.
6. Terrorist Financing (TF): Collection or provision of funds with the knowledge that they will be used in whole or in part to commit terrorist acts or to contribute to the commission of terrorist acts.
7. Financing for the proliferation of weapons of mass destruction (FPWMD): Collection or provision of funds with knowledge that will be used, in whole or in part, to create, acquire, use or transfer any weapon capable of eliminating a large number of people and generating significant economic and/or environmental damage.
8. Money and Asset Laundering (ML): The process by which criminal assets are integrated into the legal economic system with the appearance of having been obtained lawfully.

9. **Irregular or Unusual Transaction:** Any transaction that is outside the patterns of behavior of the Client's or Counterparty's usual transactions, whether or not they are significant, or that is not related to the type of economic activity carried out by the Client or Counterparty of the Company.
10. **Suspicious Transaction:** Any Irregular or Unusual Transaction that, after analysis by the Compliance Officer and on the basis of objective facts and criteria, is determined to have no apparent legal justification.
11. **Politically Exposed Persons (PEP's):** These are all those nationals or foreigners who perform or have performed public functions in our country or in their country of origin. Such classification shall be assigned for the period in which they hold office and for a period equal to the exercise of their functions once they have ceased their work, not exceeding five years. The status of Politically Exposed Person will correspond to natural persons who perform or have performed the public functions listed in Articles 16 and 17 of the Instructive of the UIF.
12. Digital Asset Service Providers (DASPs)/Bitcoin Service Providers (BSPs): A natural or legal person that provides for itself or for third parties bitcoin/digital asset-related services such as, but not limited to, custodians, exchanges and payment processors or wallets.
13. **Customer Reports:** these are the reports that Virtual Asset Service Providers must maintain in relation to active, inactive and disconnected customers with whom the referred Provider has had interaction during each calendar month.
14. **Supplementary Reports:** these are those international or local transactions that must be reported by those entities that are subject to the supervision and regulation of the Superintendence of the Financial System regarding local or foreign transactions greater than US$1,000.00 or family remittances greater than US$200.00.
15. **Warning signs:** Facts, situations, events, quantitative and qualitative indicators, financial ratios and other information that is considered relevant, from which the possible existence of an Unusual or Suspicious Operation that may be related to an illicit activity such as ML/TF/ FPWMD can be inferred.
16. **Suspicious Transaction Attempt:** Any unusual operation that is not legally justified and that is intended to be carried out by a natural or legal person and, due to withdrawal or impossibility of execution, due to the controls established by the Company, cannot be carried out or completed.
17. **Financial Investigation Unit (FIU):** Office attached to the Attorney General's Office, created for the investigation of crimes related to ML/TF/ FPWMD.

IV. Introduction

The Company adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

The company adopts a risk-based approach in the design and implementation of this Manual with a view to managing and mitigating the risks associated Money Laundering (ML), Financing of Terrorism (TF) and Financing for Proliferation of Weapons of Mass Destruction (FPWMD). A qualified Compliance Officer has been appointed to implement appropriate AML/CTF policies and procedures.

IV.I. Company's Key Objectives

In the course of its business activity, the Company pursues the following objectives in relation to AML/CTF:

- implement an AML/CTF Manual for the prevention of ML/TF/FPWMD, with a risk-based approach;
- apply mechanisms capable of ensuring that the measures for prevention, mitigation, control and reporting of activities are consistent and proportional to the previously identified risks to which the Company is exposed to;
- ensure compliance with the applicable laws, regulations, instructions, technical standards and guidelines issued by the competent authorities and with the Recommendations issued by the Financial Action Task Force (hereinafter referred to as "FATF"), regarding the prevention of ML/TF/FPWMD;
- establish and communicate the responsibilities, attributions and roles of the different areas of the Company with respect to the risks of ML/TF/FPWMD;
- define the measures for the identification, evaluation and management of risks related to ML/TF/FPWMD to which the Company may be exposed, in order to establish and implement controls, measures and adequate due diligence to mitigate such risks in the processes or procedures in which the Company is involved.

IV.II. Company's Compliance Manual

The Company has established this Manual to ensure that any ML/TF/FPWMD risks identified by the Company are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the Company being used to facilitate any financial crimes. This Manual is designed to represent the basic standards of AML and CTF procedures and standards, which will be strictly observed by Company.

The Manual is based upon applicable AML/CTF laws, regulations and regulatory guidance from the Government Institutions of El Salvador. This Manual is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation.

Among other things, this Manual:

- forms part of its wider compliance regime, and is designed to meet the requirements of its legislative environment;
- ensures that the Company is able to detect irregular activities associated with ML/TF/FPWMD and report them to the appropriate authorities;
- focuses not only on the effectiveness of internal systems and controls developed to detect money laundering, but on the risk posed by the activities of customers with which Company does business;
- is built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organisation.

IV.III. Review of the Manual

This Manual is the subject of a review by the General Shareholders Meeting or the higher Administrative Body at least annually. The proposal for a review and the review of this Manual may be scheduled more often by the decision of the Company's Compliance Officer. The Company must review and, where necessary, update this Manual and its annexes (incl. the risk assessment policy and risk assessment made thereof) in the each of the following cases:

- publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment or updated National Policy for the Prevention of Money Laundering and Terrorism Financing;

- upon receipt of an order from the FIU strengthen the applicable internal procedures;
- upon significant events or changes in the Company's management and operations;
- such necessity arises during periodic monitoring of the implementation and adequacy of the Company's internal policies.

This Manual's review (incl. regular annual review) shall be confirmed and approved by the General Shareholders Meeting or the higher Administrative Body.

IV.IV. Governance Principles and Code of Ethics

The Company's employees and the service providers (third parties) involved in the Company's business should act in accordance with this Manual and the Code of Ethics. The obligations of the Company as defined in this Manual must be understood as the duties of all employees of the Company unless it is provided that certain duties must be performed by a specially designated employee of the Company (e. g. the Compliance Officer, etc.). The Code of Ethics of the Company is aimed at increasing the awareness of all employees by establishing criteria to place ethical principles that must be followed before the achievement of the Company's objectives and business interests.

All employees of the Company, depending on the functions performed by them, shall be introduced to this Manual and the Code of Ethics. They should be aware of their subordination to other structural units of the Company. If the Company has more than 1 Employee in a structural unit, the higher Administrative Body shall appoint a responsible employee whose task is, among other things, to perform daily supervision over the performance of the tasks of the structural unit (or part of it).

The day-to-day management of the Company takes place through the Sole Director. The Sole Director is responsible for assigning tasks to the Company's structural units and controlling the performance of tasks assigned. In addition to day-to-day management, the Sole Director organizes meetings and, if necessary, discusses decision-making with experts (incl. employees, advisors and external service providers).

IV.V. Company's Services

The Company's main economic activity is provision of services related to digital assets (incl., Bitcoin) including wallet and exchange services as it is specified in a regulatory framework for Bitcoin (as legal tender), and a regulatory framework for digital assets other than Bitcoin of El Salvador.

The Company has developed **services description** (annex 2) as separate document, which establishes the following in regards of each service:

- conditions to be fulfilled for provision of the service;
- service provision flow, incl. possible assets flows.

Before using new digital asset or any changes in way of the services provision, the Company shall update services description document and assess risks related to such changes, including, but not limited to, risks which may affect the digital asset users' anonymity. In regards of new digital asset at least the transactions flow and blockchain structure shall be assessed, as well as other important circumstances.

All of the Company's services of digital assets (incl., Bitcoin) wallet and exchange are provided electronically through the mobile application and platform operated by the Company.

IV.VI. Money Laundering

The term "money laundering" (ML) or asset laundering is defined in chapter III of the LCLDA and means:

1) the deposit, withdrawal, conversion or transfer of funds, goods or related rights that come directly or indirectly from criminal activities, in order to hide or cover up their illicit origin, or to help evade the legal consequences of their acts to whoever has participated in the commission of such criminal activities, inside or outside the country;
2) any operation, transaction, action or omission aimed at concealing the illicit origin and legalizing the proceeds of criminal activities committed inside or outside the country;
3) the concealment or disguise of the nature, origin, location, destination, movement or apparently legal ownership of funds, assets or rights related thereto, which proceed directly or indirectly from criminal activities;
4) the acquisition, possession or use of funds, goods or rights related thereto, knowing that they derive from criminal activities with the purpose of legitimizing them;
5) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points 1, 2, 3 and 4.

There are three common stages in ML, and they frequently involve numerous transactions. The Bitcoin Service Providers (BSP), as well as Digital Assets Service Providers (DASP) should be alert to any such sign for potential criminal activities. These stages are:

1) Placement – the physical disposal of assets proceeds derived from illegal activities;
2) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail, and provide anonymity; and
3) Integration – creating the impression of apparent legitimacy to criminally derived wealth. In situations when the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

- Illicit funds are physically placed in the financial institution

- Multiply transactions
- Wire transfers between domestic and foreign accounts

- Real estate investment
- Purchase of luxury assets
- Investments in Securities Markets

IV.VI.I. Money Laundering using Digital Assets

Money Laundering using Digital Assets follows the above-described general pattern of placement-layering-integration with some specificities stemming from specifics of Digital Assets, including their anonymous nature and the speed at which transactions may be carried out (incl. cross-border transactions).

There are different types of technologies related to Digital Assets which can be misused for Money Laundering purposes, for example:

- Use of privacy coins offers a higher level of anonymous blockchain transactions as they are anonymous and untraceable by design. Some of the techniques used in the privacy coins include hiding a person's real Digital Asset wallet balance and address and mixing multiple transactions with each other to exclude blockchain analysis.
- Mixer/tumbler services enable sending potentially traceable Digital Asset to a required address with the purpose of obscuring the source of origin, thus making them untraceable. This is done through first sending Digital Assets from multiple addresses to one address, where the Digital Asset is mixed/tumbled together. The Digital Asset is then split into several portions and sent to different addresses. This process may be repeated several times before the Digital Asset reaches its final destination address.

The following list (non-exhaustive) provides examples of possible scenarios describing how the services of Digital Asset wallet and exchange may be used to conduct Money Laundering:

Example 1

Placement – A criminal has obtained cash as result of conducting illicit activities (e.g. selling drugs) which he then deposits via several ATMs to several bank accounts of the criminal and his accomplices in small amounts over a long period of time.

Layering – Digital Asset is then purchased from a BSP/DASP via several accounts in amounts which remain little under the reporting limit (some of them may share personal data e.g. IP address) using the fiat currency deposited to the bank accounts in the placement stage.

Integration – The Digital Asset is then sent shortly after to a single Digital Asset wallet in a BSP/DASP located in a different jurisdiction and sold for fiat currency, which is sent to the bank account of the criminal.

Example 2

Placement – A criminal sends from country A to country B using the hawala system funds obtained from illicit activity (e.g. human trafficking)

Layering – The criminal's accomplice who owns a company which activity is cash intensive (e.g. hotel chain) in country B receives the funds and claims them as business profits by performing invoice fraud and integrating both illicit and legally acquired funds.

Integration – The company then exchanges the funds to Digital Asset and issues a private loan to the criminal in Digital Asset and they agree for cash payments for repayment of the loan. Criminal receives the funds through a BSP/DASP, and never makes the repayment.

Example 3

Placement – A criminal conducting illicit activity through dark web (e.g. sale of weapons) accepts payments in Digital Asset from his clients using a mixer/tumbler service to a Digital Asset wallet in a BSP/DASP.

Layering – The criminal then purchases luxury goods (e.g. art pieces, designer handbags) using the Digital Asset.

Integration – After some time, the criminal sells the purchased luxury goods and asks the buyers to send the funds to his bank account.

IV.VII. Terrorist Financing

The term "terrorist financing" (TF) is defined in article 29 of the Special Law Against Acts of Terrorism of El Salvador and means an offence committed by any person who by any means, directly or indirectly, provides, collects, transports or possesses funds or attempts to provide or collect funds, dispenses or attempts to dispense financial or other services with the intention that such funds be used, in whole or in part, to commit any of the offences covered by this Special Law. According to the abovementioned article, it also means an offence committed by any person who, directly or indirectly, places funds, financial or material resources or financial or related services of any nature, at the disposal of a person or entity for the commission of any of the offenses provided for in this Special Law.

Similar to money laundering, terrorist financing generally consists of three stages:

1) Raising – generating the funds intended for a terrorist or terror organization. The funds can originate from a variety of sources (incl. from illicit activity as well as legal business operations);
2) Moving – upon raising required amount of funds, the funds are moved to a place where they can be accessed and used by a terrorist or terror organization;
3) Using funds – some examples of the use of funds in terrorism include using it for the terrorist or terror organization to pay for weapons, material, equipment, overheads, media, messaging, training, and salaries.

Despite the different stages, the ways in which terrorist financing is done is similar and, in some cases, may be identical to the methods used for money laundering.

Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

IV.VIII. Proliferation of Weapons of Mass Destruction

Under UN Security Council Resolution No. 687, the weapons of mass destruction (WMD) include nuclear, chemical and biological weapons and their delivery systems. The term "proliferation of weapons of mass destruction" (PWMD) in the context of FATF Recommendation 1 refers strictly and exclusively to the possible non-compliance, non-implementation or evasion of the obligations related to targeted financial sanctions referred to in FATF Recommendation 7 and means the act of providing funds or financial services which are used, in whole or in part, for the following[1]:

- illegal manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, supply, stockpiling or use of entire manufactured systems of weapons of mass destruction; or
- illegal manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, supply stockpiling or use of components for use in WMD; or
- acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of means of delivery of manufactured systems of WMD; or
- supply or sale of components for the means of delivery of weapons of mass destruction; or supply or sale of related materials/goods or services (such as technologies, software, dual-use goods or expertise) for the construction of manufactured systems of weapons of mass destruction, their components or the means of delivery of weapons.

Proliferation activities and procurement processes require financing and, therefore, financial transactions. Proliferation of weapons of mass destruction also includes three stages:

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP%20on%20Recommendation%202%20Sharing%20among%20domestic%20competent%20authorities%20re%20financing%20of%20proliferation.pdf.coredownload.inline.pdf

1) Raising – a proliferator raises funds to finance a WMD. The funds can originate from a variety of sources (incl. from illicit activity as well as legal business operations);
2) Disguising the funds – upon raising required amount of funds, a proliferator transfers these funds into the international financial system for e.g. trade purposes;
3) Procurement of materials and technology – for example, a proliferator or its agents uses those funds to pay for goods and services related to WMD.

V. AML/CTF systems

V.I. Primary Legislation Governing AML/CTF

The Company shall comply with the rules and regulations set out in Law Against Money Laundering and Asset Laundering of Republic of El Salvador (in Spanish „Ley Contra el Lavado de Dinero y Activos" or LCLDA)[2]. In addition, the following legal acts are relevant to the Company's activity (non-exhaustive list):

- Executive Decree No. 2 dated January 21, 2000, Regulation of the Anti-Money Laundering and Anti-Money Laundering Law[3];
- Agreement No. 380, dated October 22, 2021, Financial Investigation Unit Instructive for the prevention of Money Laundering and Asset Laundering[4];
- Legislative Decree No 108 dated October 17, 2006, Special Law Against Acts of Terrorism[5];
- Legislative Decree No. 57 dated June 09, 2021, Bitcoin Law[6];
- Executive Decree No. 27, dated August 27, 2021, Regulation of the Bitcoin Law[7];
- Legislative Decree No. 126 dated October 30, 1997, Central American Convention for the Prevention and Repression of Crimes of Money and Assets Laundering Related to the Illicit Trafficking of Drugs and Related Crimes[8];
- Legislative Decree No. 643 dated January 11, 2023, Law on Issuance of Digital Assets[9];
- Digital Asset Service Providers Regulations approved by the National Commission of Digital Assets dated August 10, 2023[10];
- Guide for AML/CFT/CPF risk management for the Digital Assets Industry dated December 22, 2023[11];
- The FATF Forty Recommendations[12];

[2] https://www.uif.gob.sv/wp-content/uploads/leyes/leyclda.pdf
[3] https://www.uif.gob.sv/wp-content/uploads/instructivos/Reglamento-de-la-Ley-contra-el-Lavado-de-Dinero-y-de-Activos.pdf
[4] https://www.uif.gob.sv/wp-content/uploads/instructivos/InstructivoUifDiarioOficial2021.pdf
[5] https://www.uif.gob.sv/wp-content/uploads/leyes/Ley-Especial-contra-Actos-de-Terrorismo.pdf
[6] https://www.uif.gob.sv/wp-content/uploads/leyes/Ley-Bitcoin.pdf
[7] https://www.uif.gob.sv/wp-content/uploads/instructivos/Reglamento-de-la-Ley-Bitcoin.pdf
[8] https://www.uif.gob.sv/wp-content/uploads/convenciones/04-Convenio-C-A-para-la-prevencion-la-represion-delitos-lavado-dinero-activos.pdf
[9] https://cnad.gob.sv/wp-content/uploads/2023/10/LEY-DE-ACTIVOS-DIGITALES-2023-ESP.pdf
[10] https://cnad.gob.sv/wp-content/uploads/2023/10/Reglamento-de-Proveedores-de-Servicios-de-Activos-Digitales-2023.08.11-ESP.pdf
[11] https://cnad.gob.sv/wp-content/uploads/2024/01/GuiaPSAD-LDA-FT-ADM-Espanol.pdf
[12] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

- NRP-36 dated October 10, 2022, Technical Standards for Managing the Risks of Money Laundering, Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction[13].

Company firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The Company is, therefore, committed to the highest standards of AML/CTF measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

V.II. Control Bodies

El Salvador has two main regulatory frameworks relevant to digital assets:

- a regulatory framework for Bitcoin (as legal tender); and
- a regulatory framework for digital assets other than Bitcoin.

With regards to the Bitcoin framework, the Company is subject to registration and further control with the Central Reserve Bank (BCR) and whose supervision falls under the Superintendence of the Financial System (SSF).

With regards to the framework for digital assets other than Bitcoin, the Company is subject to registration and further control through the National Commission for Digital Assets (NCDA). The NCDA controls if the DASPs adhere to specific financial and operational requirements to safeguard investors and promote responsible development.

[13] https://www.bcr.gob.sv/regulaciones/upload/NRP-36.pdf

V.III. Supervisory Authority

For the purpose of AML/CTF, BSPs and DASPs registered with control bodies they are subject to are supervised by the state authority with the following details:

- Unidad de Investigación Financiera, Fiscalía General de la República (UIF), in English – Financial Investigation Unit (FIU) of the Attorney General's Office;
- address: Urbanización Madre Selva IV Etapa, prolongación Calzada El Amate, N.° 4, Antiguo Cuscatlán, La Libertad, El Salvador, C.A.;
- phone: (503) 2593-7800;
- email: solicitud.info@uif.gob.sv.

The same authority also performs supervision under implementation of international and domestic sanction regimes.

V.IV. Effective Controls

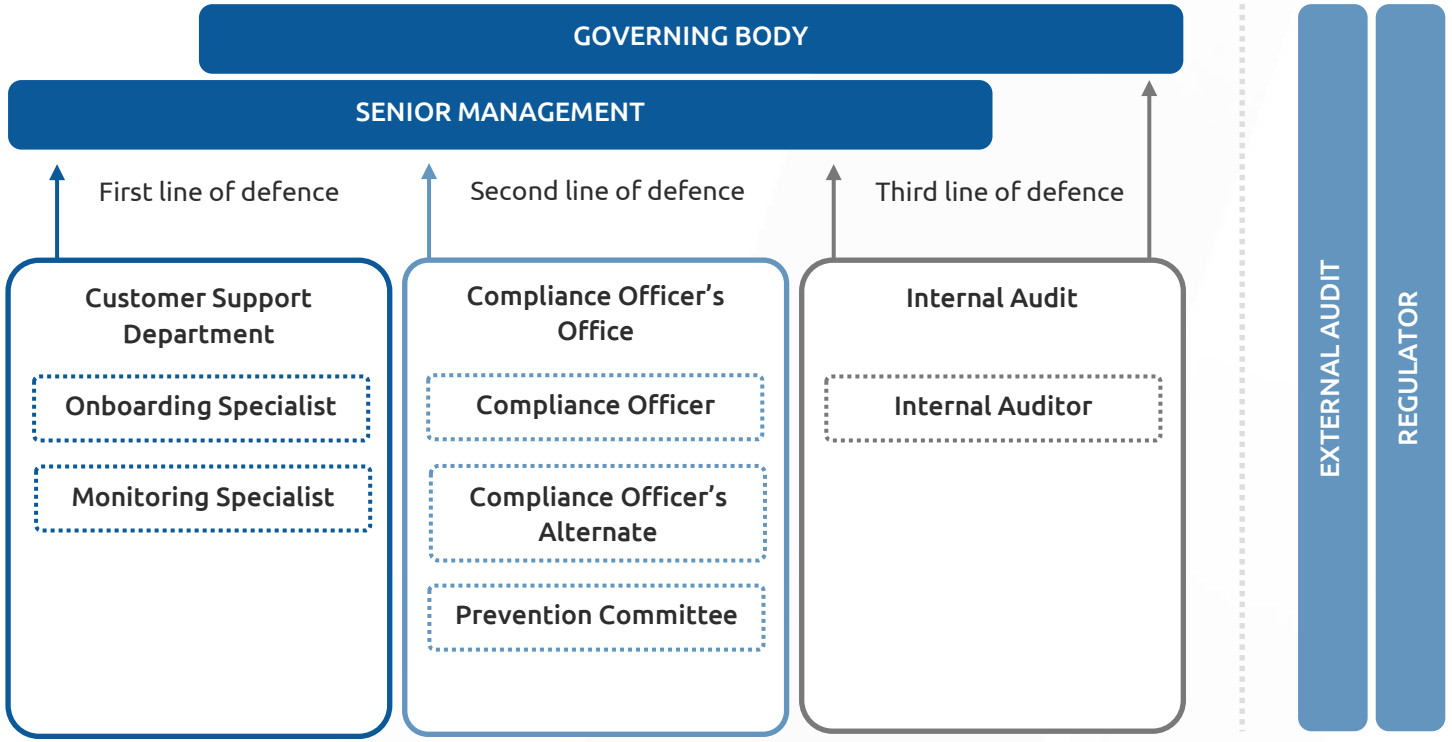
To ensure proper implementation of AML/CTF procedures and controls, Company has effective controls covering:

- effective AML/CTF Compliance Manual;
- Sole Director and Committee oversight;
- appointment of the Compliance Officer and other employees with certain responsibilities;
- compliance and audit function;
- staff training.

The Sole Director of Company is responsible for managing the business effectively and for the oversight of internal AML/CTF controls and systems. The Sole Director appoints the Compliance Officer who has overall responsibility for the establishment and maintenance of Company' AML/CTF systems and is the central reference point for suspicious transaction reporting.

V.V. Three Lines of Defence

The Company follows the three lines of defence framework when managing ML/TF/FPWMD risks. The three lines of defence is an industry model for managing risks. It is used to structure roles, responsibilities and accountabilities for decision making, risk and control management, and independent assurance. The three lines of defence are used as the fundamental guiding principle when performing the AML/CTF obligations.



V.VI. Governing Body Responsibilities

The higher Administrative Body, which might be compose of a Sole Director or a Board of Directors, is the primary governing body of the Company. In accordance with Article 5 of the FIU Instruction, the Company's Sole Director is responsible for approving, promoting and implementing the internal policies and procedures for the prevention of ML/TF/FPWMD, as well as control and detection of unusual or suspicious transactions and reporting of such transactions. In addition to approving the abovementioned internal policies and procedures, the Sole Director's responsibilities include but are not limited to:

- maintaining compliance with effective laws of El Salvador;
- creating the Compliance Officer's Office for coordinating activities related to ML/TF/FPWMD prevention;
- establishing the responsibilities of the Senior Management, the Compliance Officer and personnel of the Compliance Officer's Office, the internal audit personnel related to ML/TF/FPWMD prevention work, the personnel involved in business generation and customer service areas, as well as of the rest of the employees and collaborators of the Company;
- appointing and approving the appointment of the Compliance Officer and his or her alternate;
- approving the AML/CTF Compliance Manual and its updates;
- approving the Code of Ethics;
- approving the Compliance Officer's annual work plan;
- approving of the annual ML/TF/FPWMD prevention training plan;
- being aware of the reports and statistics of the management performed by the Compliance Officer or the Compliance Officer's Office, leaving a record in the respective minutes;
- being aware of the reports submitted by internal and external audits or whoever performs similar functions related to ML/TF/FPWMD prevention work and following up on the observations or recommendations adopted;
- supporting the work of the Compliance Officer and his or her team in their work;
- communicating the appointment, dismissal or resignation of the Compliance Officer, both incumbent and alternate, to the FIU and the respective control, supervision or oversight agencies, in accordance with the established deadlines;
- establishing the consequences of non-compliance with the procedures for the control and detection of suspicious or unusual transactions and reporting of such transactions, for the whole Company.

The Sole Director of the Company has approved this AML/CTF Compliance Manual, the appointment of the Compliance Officer and have assigned responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CTF requirements.

V.VII. Senior Management Responsibilities

The Company's Sole Director is responsible for overseeing the performance of the Senior Management (incl., General Manager, Legal Manager, Operations Manager etc.) and their functions. The Company's Senior Management responsibilities include but are not limited to:

- ensuring that all business activities that are conducted by the Company's personnel with customers are carried out in accordance with established laws, regulations and ethical standards in order to prevent ML/TF/FPWMD risks;
- ensuring that the AML/CFT Compliance Manual and its procedures for prevention of ML/TF/FPWMD is approved by the Sole Director and communicated to all the Company's personnel, facilitating access to them through the existing technological means or others considered pertinent;
- ensuring the implementation of the annual training plan on ML/TF/FPWMD prevention approved by the Sole Director;
- creating or establishing communication channels that facilitate the Company's personnel to inform the Compliance Officer of any irregularity that puts the Company at risk and that is considered to be in violation of the legal provisions applicable to the prevention of ML/TF/FPWMD;
- ensuring that the Compliance Officer reports to the Sole Director the results of its assessments related to ML/TF/FPWMD prevention, at least quarterly within three months following the reporting period;
- providing timely support to the Compliance Officer.

V.VIII. KYC Agents

KYC Agents comprise the first line of defence, which is a part of the risk management system that is related to the structural units with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures.

The first line of defence must have good knowledge of the customer and the specific features of their activities and business activities.

Principal functions of the KYC Agents include in particular:

- performing of the Customer's onboarding procedure (as defined below) and application of CDD/EDD measures before the establishment of the Business Relationship with the Customer;
- performing of the ODD/EDD measures in the course of the established Business Relationship with the Customer (incl. the monitoring of transactions and periodically updating the Customer's information);
- identifying transactions in the customer's activities that are suspicious or unusual or do not correspond to reasonable economic objectives, or transactions that refer to such circumstances, and referring such transactions to the second line of defence (Compliance Department) for analysis and if necessary, directly to the Senior Management;
- perform other functions which are assigned to the KYC Agents under the applicable law, internal policies, job description.

V.IX. Compliance Officer's Office

The Compliance Officer's Office is a compliance unit within the Company whose main objective is to coordinate activities related to AML/CTF and to routinely monitor due compliance with internal policies and procedures for the prevention of ML/TF/FPWMD, with a risk-based approach.

V.IX.I. Compliance Officer

The Compliance Officer acts as the focal point within the Company for the oversight of all activities relating to the prevention and detection of ML/TF/FPWMD and providing support and guidance to the Senior Management to ensure that ML/TF risks are adequately managed.

The Compliance Officer is sufficiently independent and has a direct reporting line to the Company's Senior Management. The Compliance Officer has access to sufficient resources and information to be able to ensure Company's compliance with effective laws and regulations of El Salvador.

In particular, the Compliance Officer is responsible for:

- monitoring of due compliance with policies and procedures for the prevention of ML/TF/FPWMD, with a risk-based approach and, in addition, the implementation of controls and procedures that facilitate the detection of unusual or suspicious transactions and the reporting of such transactions;

- submitting, at least every six months, written reports, in person or through remote connections to the Manager, which must include the work performed;
- promoting the adoption of modifications to the policies and procedures for the prevention of ML/TF/FPWMD and for the detection and reporting of unusual or suspicious transactions and report the results of the corrective actions requested by the Senior Management;
- designing the AML/CTF Compliance Manual and proposing the update of the procedures to the Committee;
- collaborating on the development of methodologies, qualitative indicators and/or quantitative methods of recognized technical value for the timely detection of unusual or suspicious transactions;
- analysing and implementing corrective measures for the observations detected in the reports submitted by the internal and external audit;
- evaluating compliance with the applicable laws, regulations, instructions and other rules related to the ML/TF/FPWMD prevention;
- performing an analysis of transactions or operations to determine whether or not to prepare a suspicious transaction report;
- validating that Regulated Transaction (RT) reports are sent to FIU through the means established by it;
- providing timely response to the information requested by the FIU, keeping a file of the same with the appropriate confidentiality;
- preparing and coordinating the execution of the annual training plan;
- participating as a member of the Committee, following up and properly documenting the issues discussed;
- establishing and coordinating permanent monitoring mechanisms to monitor the transactions carried out by customers in course of the business relationship, in order to ensure that the transactions being executed are consistent with their profile;
- establishing and coordinating permanent implementation of additional or enhanced monitoring mechanisms for operations of customers located in countries or jurisdictions designated by the FATF as high risk or non-cooperative, or that have business with persons located in those territories; likewise, operations of customers that conduct financial business in countries considered as zero or low taxation or qualified as “tax havens”;
- issuing reports or opinions on the existence of ML/TF/FPWMD risks in the launching of new products, channels and services of the Company, or in modifications thereof, prior to their launching or putting into production;
- Other functions as defined in the internal policies and procedures of the Company.

The minimum requirements to be appointed as the Compliance Officer within the Company are the following:

- certification in money laundering and terrorist financing prevention and a minimum of two years of experience in this field;
- hold a managerial position;

- legal, business and controls skills and knowledge;
- to have a university degree and basic knowledge of the administrative and legal aspects of the business or activity in question.

The appointment of the Compliance Officer does not exempt the other employees from the obligation to apply, in the performance of their duties, the procedures for the prevention and control of ML/TF/FPWMD risks.

The Company shall appoint the Alternate Compliance Officer who shall comply with the same requirements that are imposed on the Compliance Officer.

V.X. Compliance Committee

The Compliance Committee (hereinafter – the Committee) shall support the performance of Compliance Officer and be oriented to strengthen the control mechanisms and the prevention of ML/TF/FPWMD risks. In particular the Committee is responsible for the following:

- instructing by means of agreements, modifications or improvements to AML/CTF Compliance Manual, in compliance with the national and international legal framework;
- following up on the management of the Compliance Officer;
- being aware of the deficiencies in the AML/CTF Compliance Manual detected by the Compliance Officer's Office, as well as the corrective actions or measures that have been implemented for such purposes;
- reviewing the implementation of the annual training plan that involves all employees of the Company and also includes specialized training for the Compliance Officer's staff on AML/CTF/FPWMD issues;
- reviewing that the Compliance Officer's approach is oriented to ML/TF/FPWMD risk prevention and management;
- reviewing at least every three years the organizational structure of the Compliance Officer's Office in terms of human resources, in proportion to the size of the institution, number of clients, products and services, as well as its operational capacity, to determine the need for greater resources to mitigate ML/TF/FPWMD risks;
- promoting and guaranteeing the independence and autonomy of the Compliance Officer in an institutional manner;
- ensuring that the Compliance Officer has unrestricted access to all information and documentation handled by the Company related to AML/CTF/FPWMD.

The Committee shall be composed of at least five members, who shall preferably hold the following positions:

- Sole Director;
- General Manager;
- Legal Manager;
- Operations Manager;
- Compliance Officer.

At the first meeting of the Committee, the members shall elect the following persons with the following responsibilities:

- Chairman who will be in charge of chairing the Committee's meetings, maintaining order in the participation of each member and proposing the agenda items to be addressed at each of the meetings;
- Vice-Chairman who shall be in charge of communicating to the Sole Director and the Compliance Officer the recommendations, observations or comments made by the Committee, may propose the agenda items deemed necessary for each of the Committee's meetings and shall be in charge of performing the functions of the Chairman in the event of his/her absence;
- Secretary who shall be responsible for summoning the members to the Committee meeting, verifying the attendance of the members, safeguarding the physical or digital books in which the minutes are recorded, taking notes and preparing the respective minutes, issuing certifications of the items of the minutes and forwarding them to the Vice President for external communication when necessary;
- Two Members who shall be in charge of gathering the necessary information (obtained mainly from the Compliance Officer, Internal and/or External Audit and other sources internal to the Company, incl., the FIU, the BCR Standards Committee, the National Virtual Assets Commission or any other official and public source related to ML/TF/FPWMD prevention issues) and processing it for its presentation to the Committee.

Once the Committee has been formed and the positions have been designated, the operation of the Committee shall be governed by the following rules:

- *Quorum: the* Committee shall validly meet with the majority of its members present and resolutions shall be approved by simple majority, the presence of the Sole Director being indispensable at all meetings;

- *Preferential vote:* the Chairman of the Committee, or when the Vice-Chairman assumes the role of Chairman in the absence of the latter, shall have the casting vote when there is a tie in those sessions in which four of the five members of the Committee participate;
- *Sessions:* Sessions may be held either virtually or in person, which shall be recorded in the minutes of the respective session;
- *Minutes:* the minutes of the meeting must contain at least the number of the minutes, time and date of the meeting, members of the Committee present, details of the agenda and any amendments thereto, a summary of each of the points discussed at the meeting and the favorable and/or unfavorable votes on each of the points addressed;
- *Certifications of minute items:* when it is necessary to issue a certification of a minute item, it shall be issued by the Secretary of the Committee, who shall expressly state the use to which it is to be put.

V.XI. Audit Function

Audit function shall be established to perform regularly reviews of the AML/CTF systems to ensure their effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF/FPWMD and the size of the Company's business, as well as regulatory requirements. Where appropriate, Company will seek a review from external auditors. Independent audit functions include the following principles:

- compliance and audit functions are independent in practice;
- the regular review is performed at a frequency of once a year;
- external party is leveraged to perform the auditing;
- availability of communication hierarchically to Senior Management and Sole Director through the means of direct communication.

The performing of audit functions shall be ensured by the Sole Director, which should be adopted, at least, on annual basis.

VI. Risk-based approach (RBA)

By adopting a risk-based approach, the Company is able to ensure that measures to prevent or mitigate ML, TF and FPWMD threats are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

The inherent risk is assessed in course of identification of the specific products, services, customers, entities, and geographic locations. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered.

Risk assessment during on-boarding stage of the new customer provides the Company with an opportunity to gain an insight into the type and nature of its potential customers, their geographic locations and business activities, whereas ongoing determination of the customer's risk profile allows the Company to ensure, that correct risk level is assigned to the customer throughout the established relationship.

The Company determines the extent of its CDD measures and ongoing monitoring, using a risk-based approach (RBA) depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified.

The RBA enables the Company to subject its customers to proportionate controls and oversight by determining:

- the extent of the due diligence to be performed on the direct customer;
- the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;
- the level of ongoing monitoring to be applied to the relationship;
- measures to mitigate any risks identified.

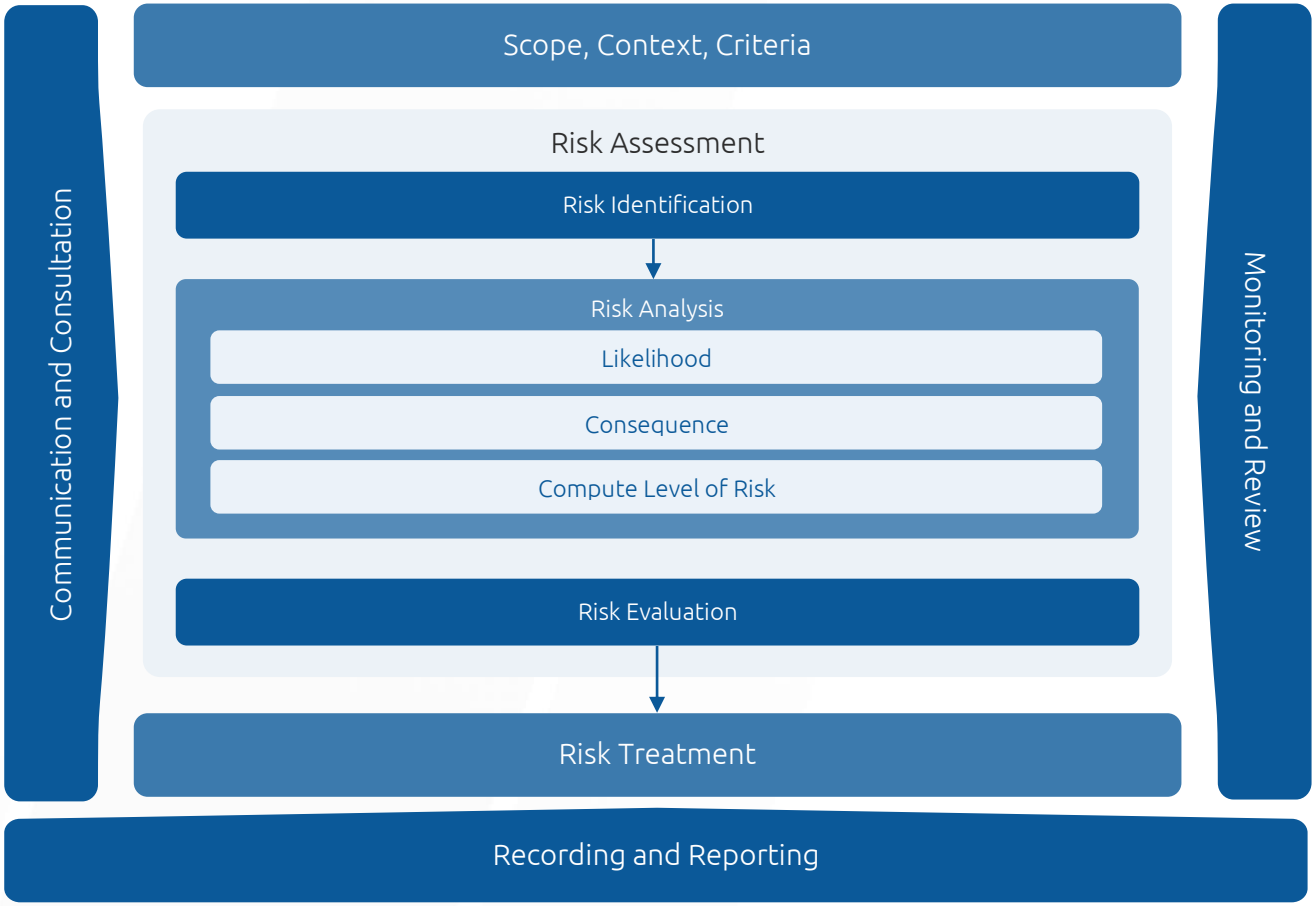
An RBA involves identifying and categorizing ML/TF/FPWMD risks at the customer level and establishing reasonable measures based on risks identified. An RBA does not refrain Company from engaging in transactions with customers or establishing business relationships with potential customers, but rather it assists Company to effectively manage potential ML/TF/FPWMD risks.

VI.I. Risk Assessment and Risk Categories

The Company prepares and regularly updates the risk assessment in order to identify, assess, analyse and manage ML/TF/FPWMD risks. The process of risk assessment, executed by the Company shall include at least the following stages:

- risk factors identification;
- risks factors analysis;
- risks factors evaluation.

Risk assessment is an integral part of the risks management process within the RBA.



In the course of risk assessment, the Company uses at least the following sources:

- applicable regulatory requirements (El Salvadoran laws, FIU Instructions, etc.);
- last national risk assessment;
- guidelines of authorities (incl. international organizations);
- the knowledge previously obtained when performing activities similar to the Company.

As part of the Company's ML/TF/FPWMD risk assessment, the Company addresses the full spectrum of the Company's risks on enterprise-wide level by maintaining and continuously updating the **Risk Matrix** (annex 3) taking into consideration the internal and external factors.

The Company assess the ML/TF/FPWMD risks of its customers by assigning a ML/TF/FPWMD risk rating taking into consideration the risk categories as specified below.

VI.I.I. Customer risk

Customer risk factors are related to the customer's or its beneficial owner's personality, their behaviour and other circumstances directly related to the specific person. Factors in this category include customer's legal status, its structure, information previously known about the customer, etc. When identifying risk factors in this category, the Company considers the following:

- the customer's status, such as entity listed on a regulated market, governmental authority or entity regulated by public law, credit or financial institution;
- the customer's PEP status, as well as known connection to PEPs (family members, close associates, etc.);
- complexity of the customer's organizational structure, including use of corporate structures, trusts and the use of nominee directors/shareholders and bearer shares;
- negative information about the customer or related persons (e. g. adverse media, warnings from regulatory bodies, criminal records, etc.);
- the customer's behaviour and personalities (e. g. education or knowledge in certain field, age, etc.);
- the customer's area of activity (e. g. cash intensive or other business vulnerable to a ML/TF/FPWMD);
- origins of the customer's wealth and opportunities to verify their soundness.

VI.I.II. Country or geographic region risk

Country or geographic region risk factors are related to specific jurisdiction or region. Factors in this category include the customer's citizenship, place of residence, location of business as well as location of transaction's counterparty (relevant country). When identifying risk factors in this category, the Company defines if the relevant country meets the following facts about jurisdiction and region:

- is the Company's domestic country;
- have been identified by the FATF as jurisdictions with strategic AML/CTF deficiencies;
- is subject to sanctions, embargoes or similar measures issued by the United Nations Security Council (UN);
- has the status of high-risk third country as established by the FATF;
- is vulnerable to corruption or other criminal activity;
- believed to have strong links to terrorist activities.

VI.I.III. Product and/or services risk

Product and/or services risk factors are related to specific service being provided. Such factors include volume of services being provided to the customer, specific transactions patterns used and other circumstances, which may affect risk of a ML/TF/FPWMD occurrence in the course of services provision. When identifying risk factors in this category, the Company considers the following facts about products and services:

- volume of products and/or services requested or provided;
- specific transactions patterns (e. g. FATF Red flags indicators);
- intended purpose of product and/or service, as well as identified purpose;
- product and/or service possible (and identified) use in activities vulnerable to a ML/TF/FPWMD and in illicit (prohibited) activities;
- product and/or service ways to promote anonymity.

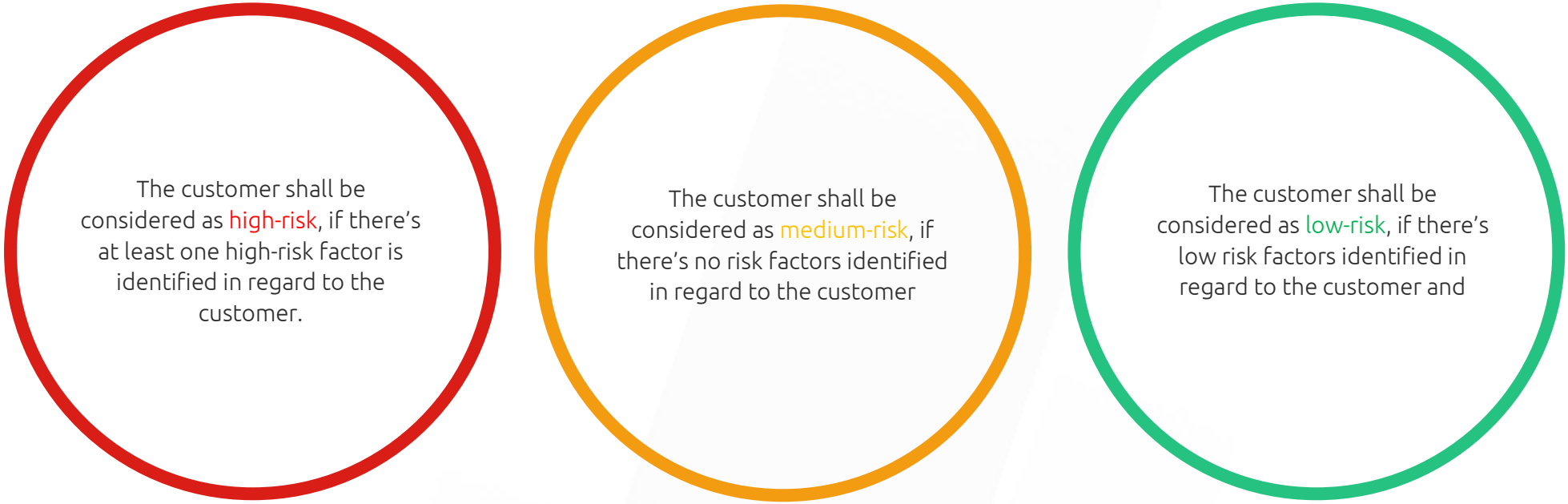
VI.I.IV. Delivery / distribution channel risk

Delivery and/or distribution channels risk factors are related to channels used for provision of the services. Such factors include specific ways for identity verification, performing transactions and authentication methods. When identifying risk factors in this category, the Company considers the following facts about delivery / distribution channel:

- the method using which the customer's and its representative's identity has been verified (e. g. via face-to-face meeting, remotely, use of qualified electronic signature);
- credit institution, financial institution, paying institution or payment channel used by the customer;
- IP address(es) and device ID(s) used by the customer;
- use of solutions which promote anonymity by the Customer (e. g. VPN, encrypted email, TOR browser, one-time wallets, etc.).

VI.II. Determination of the customer's risk profile

The Company establishes and maintains the **list of risk factors** as separate document (annex 4), which is used for determination of the customer's risk profile.



The Company identifies risk factors in the course of customer due diligence as described below.

VI.III. Maintaining of the customer's risk profile

The Company reviews the business relationship with each customer as per the schedule below to ensure if the risk profile determined is still applicable or should be modified based on any changes of the identity of the customer, the nature of the customer's business, the customer's

country of residence, the actual volume of transactions and other facts, which may affect the customer's risk assessment. Only the Compliance Officer is permitted to alter a customer's risk profile. The Compliance Officer will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to customers.

Low Risk

The Compliance Officer performs reviews of every low-risk every 3 years.

Medium Risk

The Compliance Officer performs reviews of every medium-risk customer that is no longer a new relationship every 2 years (i.e., every 12 months after the customer's onboarding).

High Risk

Due to the high-risk nature of these relationships, the Compliance Officer performs annual reviews of every high-risk customer including a transactional review.

Each high-risk customer will require Enhanced Due Diligence before the relationship and additional facts will be gathered to learn more about the customer. For any non-individual customer whose business has been identified as a "high-risk business", the Compliance Officer must also additionally verify the existence of the business and purpose of the business relationship with the Company.

VI.IV. Non-acceptable customers

The Company has created the **list of prohibited risk factors** (annex 4) in the presence of which the customer will not meet the Company's risk appetite. In case, when such risk factor has arisen in the course of the customer's onboarding or before making occasional transaction – the Company refuses to establish the business relationship or perform transaction with such customer. If prohibited risk factor is identified in the course of the business relationship established – such relationship shall be terminated in accordance with this Manual.

Prohibition of anonymous accounts

The Company is prohibited from opening anonymous accounts or accounts under obviously fictitious names, as well as from opening accounts or otherwise starting business relationship without requesting data confirming the identity of the customer or if there is a reasonable suspicion that the data recorded in these documents is fake or falsified.

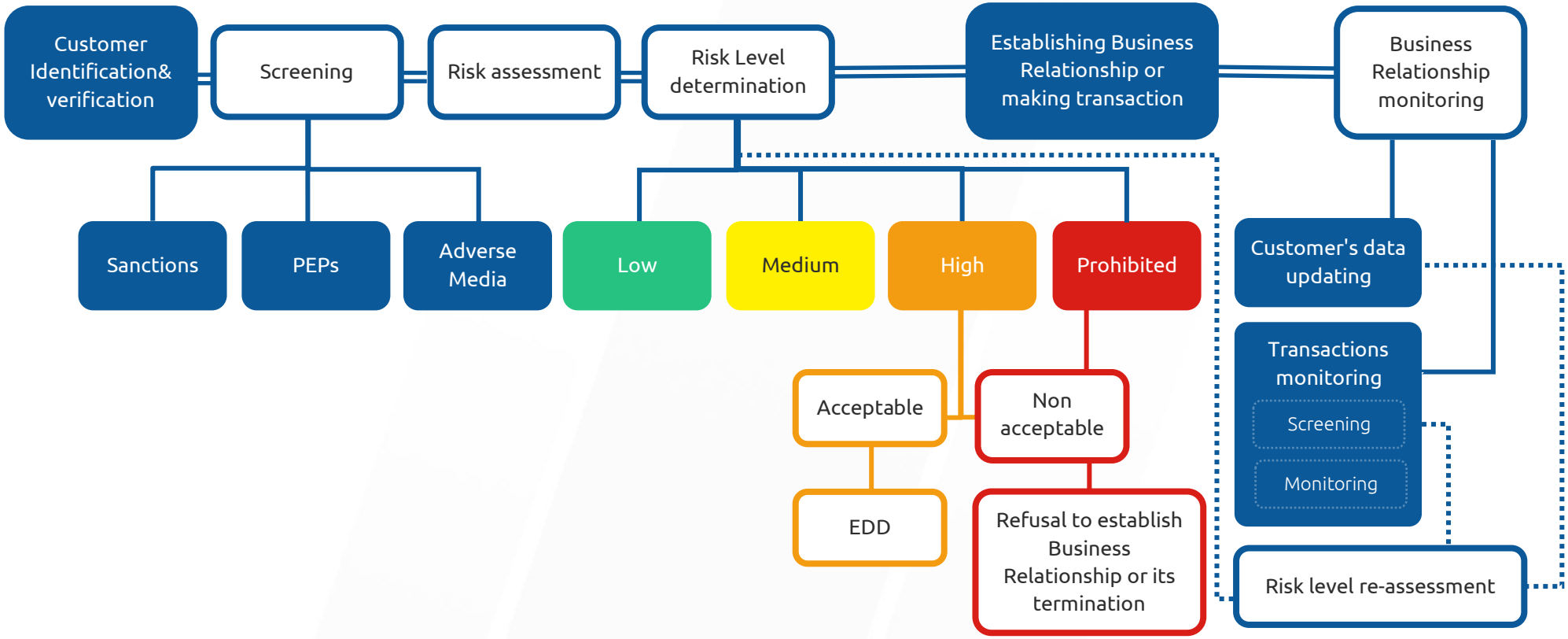
Prohibition of shell banks

The Company does not maintain correspondent relationships with shell banks, which is defined as a financial institution or an institution that carries out activities equivalent to those carried out by a financial institution, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, organizational structure and internal control systems, and which is unaffiliated with a financial group supervised by the competent authorities.

VII. Customer due diligence

Customer due diligence (CDD) is central to an effective AML/CTF regime. The Company takes CDD measures to identify and verify each of its customers (incl., counterparties) so it can:

- determine the ML/TF/FPWMD risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.



The Company applies the following CDD measures:

- identification of the customer and verification of the customer's identity using documents, data or information from reliable and independent source;
- identification and taking reasonable measures to verify the beneficial owner's identity so that Company is satisfied that it knows who the beneficial owner is, including in the case of a legal entity or trust, measures to enable Company to understand the ownership and control structure of the legal entity or trust;
- identification and taking reasonable measures to verify if the customer is a PEP or a person connected to PEP ((family members, close associates, etc.);
- obtaining an information on the purpose and intended nature of the business relationship or transaction unless the purpose and intended nature are obvious;
- monitoring of the business relationship.

If a person purports to act on behalf of the customer, Company takes measures to:

- identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information;
- verify the person's authority to act on behalf of the customer.

CDD requirements should apply:

- upon establishment of the business relationship;
- upon executing or mediating of occasional transaction(s) where the value of the transaction(s) exceeds $1,000 (or an equal amount in other assets) within 24 hours;
- upon suspicion of ML/TF/FPWMD, regardless of any derogations, exceptions or limits provided for in this Manual and applicable legislation.
- when the Company doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

VII.I. Verification of the customer's identity

In the course of CDD measures implementation, the Company shall verify the customer's identity by using reliable and independent source to confirm that the data directly related to the customer is true and correct. The Company identifies the customer and verifies the customer's identity by reference to documents, data or information provided by a reliable and independent source, including:

- a governmental body or other relevant authority;
- an authority in a place outside El Salvador that performs functions similar to those of a governmental body or other relevant authority;
- which has been issued by or received from a third party or a place that has no interest in or connections with the customer or the Company, i. e. that is neutral (e.g. information obtained from the Internet is not such information, as it often originates from the customer themselves or its reliability and independence cannot be verified) and the reliability and independence of which can be determined without objective obstacles and reliability and independence are also understandable to a third party not involved in CDD implementation.

VII.II. Timing of CDD and Maintenance of Business Relationship

The Company completes the CDD process before establishing any business relationship or before carrying out a specified occasional transaction.

The customer identification information (as well as information on any beneficial owners and PEP status) and information about the purpose and intended nature of the business relationship or transaction shall be obtained before the business relationship is entered into or occasional transaction is performed.

Where Company is unable to comply with relevant CDD requirements and the ongoing due diligence requirements, the Company shall terminate the business relationship, refrain from establishing business relationship, refuse from performing the transaction or refuse from providing the service.

Prior to terminating the business relationship with the customer, the Company must inform the FIU of its intention and may only proceed with the termination of the business relationship after the period allowed by the FIU (10 working days) has expired and no response has been received from the FIU. This decision must be informed to the customer until a pronouncement has been issued by the FIU or when the term to do so has expired.

VII.III. Occasional Transactions

Occasional transaction is a transaction between the Company and a customer who does not have a business relationship with the Company. Occasional transactions may include:

- one-time exchanges carried out with digital assets
- one-time transfers carried out with digital assets;
- opening and maintaining digital wallets.

The Company takes measures to ensure, that certain services are provided in the course of occasional transactions without violation of applicable legislation. These measures include:

- specifying if certain service described may be provided in the course of occasional transaction(s);
- applying a customer's identification procedure before concluding of occasional transaction.

In addition, the Company establishes certain limits for number and value of occasional transactions within certain period and applies screening and monitoring measures for such limits. In case when any of such limits is exceeded – the Company considers this fact as intention to establish the business relationship and applies CDD accordingly.

VII.IV. Keeping customer information up to date

The Company takes steps from time to time to ensure that the customer information that has been obtained is up-to-date and relevant. To achieve this, Company undertakes periodic reviews of existing records of customers.

An appropriate time to do so is upon certain trigger events such as:

- specific time period has passed and the customer's risk profile shall be reviewed;
- the customer notifies about changes in the customer´s information;

- when a significant transaction (not only of a big amount, but also unusual) is to take place;
- when a material change occurs in the way the customer's account is operated;
- when the customer's documentation standards change substantially;
- when the Company is aware that it lacks sufficient information about the customer concerned.

In addition to aforementioned, the customers are continuously (when any of watchlists is updated) screened against watchlists (incl. PEP, Sanctions and Adverse Media). In case of match – the Company is notified and shall apply CDD accordingly.

VIII. Know Your Customer: on-boarding principles

The Company has established customer's onboarding procedure as separate document (annex 5), which contains the steps, which should be performed for application of CDD measures in the course of customer's onboarding, as well as certain requirements for documents and data to be provided. The customer's onboarding procedure established follows the abovementioned requirements.

VIII.I. Identification of the Customer – natural person

The Company identifies the Customer who is a natural person and, where relevant, their representative and retains the following data on the Customer and their representative:

- name(s) and surname(s);
- date of birth;
- nationality;
- citizenship;
- photograph.

The following valid identity documents which contain data specified above may be used as the basis for the identification of a natural person:

- an identity document of the Republic of El Salvador (incl., Salvadoran passport or DUI);
- an identity document of a foreign state;
- a residence permit in the Republic of El Salvador;
- a national driving license or foreign driver's license along with an International Driving Permit (IDP).

VIII.II. Identification of the Customer – legal entity

The Company identifies the Customer which is a legal entity and their representative and retains the following data on the Customer:

- business name or name;
- legal form;
- registration number if such number has been issued;
- name(s) and surname(s), personal number (in the case of a foreigner – date of birth or where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification) and citizenship of the director(s) or member(s) of the management director(s) of another equivalent body, and their authorities in representing the Customer;
- an extract of registration and its date of issuance;
- head office (address) and address of actual operation.

The following documents issued by a competent authority or body not earlier than six months before their use may be implied for identification of the Customer:

- registry card of the relevant register; or
- registration certificate of the relevant register; or
- a document equivalent with an aforementioned documents or relevant documents of establishment of the Customer.

The Company verifies the correctness of the Customer's data specified above, using information originating from a credible and independent source for that purpose. Where the Company has access to the relevant register of legal entities, the submission of the documents specified above do not need to be demanded from the Customer.

The identity of legal entity and the right of legal entity's representation can be verified on the basis of a document specified above, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

VIII.III. The identification of the Customer's representative and their right of representation

The representative of the customer who intends to act on the customer behalf shall be identified as the customer, who is a natural person in accordance with aforementioned onboarding requirements. The Company must also identify and verify the nature and scope of the right of representation of this representative. The name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained, except in case, when the right of representation was verified using information originating from the relevant register and information about such verification is saved.

In case when the Customer is a legal entity, the following persons may be deemed as the Customer's representative:

- the natural person, whom right to represent the Customer arises from law (e. g. management board member, director, manager, or similar position; hereinafter – lawful representative);
- the natural person to whom the relevant power of attorney is issued by the person specified in previous point (hereinafter – contractual representative).

The Company must observe the conditions of the right of representation granted to the legal entity's representatives and provide services only within the scope of the right of representation.

The authorisation has to be in line with the requirements of the Civil and Commercial Procedure Code. The authorisation issued abroad has to be legalized for use in El Salvador. In case the right of representation of the customer (legal person) is evident from the registry extract, articles of association or equivalent documents evidencing the identity of the customer (legal person), a separate document of authorisation (e.g. a power of attorney) should not be required.

VIII.IV. Customer's remote onboarding requirements

In case the Customer and where relevant, their representative is identified without their physical presence via remote onboarding, the Customer and the representative shall be identified only via using the methods specified below.

The methods specified below may only be used only in case when the customer and the beneficial owner that is a natural person and the representative of the customer who is a legal entity has been identified on the basis of the relevant documents.

VIII.IV.I. Remote onboarding through direct video streaming

The customer can use electronic means allowing direct video streaming (if any) for the onboarding if the facial image of the customer and the original of the identification document shown by the customer is recorded at the time of direct video streaming. The customer's onboarding shall be performed continuously during live video transmission and shall be part of the single customer's onboarding process.

This method of the Customer's onboarding can be used only if all the following requirements are fulfilled:

- the Company has established and approved by the Senior Management and the Compliance Officer list of electronic means, which may be used by the Company for the customer's onboarding via direct video streaming;
- the Company has established the customer's onboarding procedure which allows this method of onboarding and verification to be used;
- the Company has established adequate internal control measures to ensure fulfilment of aforementioned requirements.

VIII.V. The identification of the Customer's Beneficial Owner

The beneficial owner means any natural person who owns the customer (a legal person or a foreign undertaking) or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted.

The Company shall identify the beneficial owner of the customer and take measures to verify the identity of the beneficial owner to the extent that allows the Company to make sure that they know who the beneficial owner is. The Company collects the following data regarding the customer's beneficial owner(s):

- name(s) and surname(s);

- personal number[14].

The Company shall request from the customer information about the customer's beneficial owner (e. g. providing the customer with an opportunity to specify their beneficial owner when collecting data about the customer). The customer must provide this information by means of a document signed by its representative.

If the documents used for the legal entity´s identification or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) is registered on the basis of the document provided and signed by the representative of the legal entity.

The Company shall apply reasonable measures to verify the accuracy of the information provided in a document (e.g., by making inquiries in the relevant registers), requiring the submission of the legal entity's annual report or other relevant document. If the Company has doubts about the accuracy or completeness of the relevant information, the Company shall verify the information provided from publicly available sources and, if necessary, request additional information from the customer.

Where the Company establishes the business relationship with the Customer whose information on beneficial owners must be submitted to the state or be registered there, the Company shall obtain a relevant registration certificate or registry extract upon identification of the Customer´s beneficial owner.

VIII.VI. Identification of the purpose and nature of the business relationship or a transaction

The Company shall understand the purpose and nature of the establishing Business Relationship or performing transaction. Depending on the Company risk assessment of the situation, measures required may include:

- the customer confirming that the Company’s terms of services provision are accepted;

[14] in the case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification);

- the customer providing additional information in regards of transaction(s) performed (e. g. in the course of EDD measures or monitoring of the business relationship as specified below).

The Company shall apply additional measures and collect additional information to identify the purpose and nature of the Business Relationship or an Occasional Transaction in cases where:

- there is a situation that refers to high value or is unusual;
- where the risk and/or risk profile associated with the customer and the nature of the business relationship gives reason for the performance of additional actions in order to be able to appropriately monitor to business relationship later (e. g. if the customer is residing or established in high-risk third countries as identified by the FATF.

VIII.VII. Political Exposed Person's identification

Domestic Politically Exposed Persons (PEP) are considered to be those specified in article 9(B) of LCLDA and referred to in articles 236 and 239 of the Constitution of the Republic of El Salvador, article 2 literals "a", "b" and "c" and article 52 of the United Nations Convention Against Corruption clauses (2), (3), and (5):

- The President, Vice President of the Republic and those appointed to the presidency;
- Congressmen;
- The Ministers, Vice-Ministers of State, Secretaries, and the Departmental Governors;
- The President and Magistrates of the Supreme Court of Justice and of the Chambers of Second Instance, the Judges of First Instance and the Judges of the Peace;
- Mayors and other members of the Municipal Councils;
- The President and Magistrates of the Court of Accounts of the Republic;
- The Attorney General of the Republic, the General Prosecutor of the Republic, the General Prosecutor for the Defense of Human Rights
- The President and Magistrates of the Supreme Electoral Tribunal;
- The Diplomatic Representatives;
- Heads of autonomous institutions;

- Director and Deputy Directors of the National Civilian Police, and of the Armed Forces its Chief and Deputy Chief of the Joint military high command.

Persons designated as domestic PEPs shall continue to be subject to enhanced due diligence for a period equal to the duration of their functions, not exceeding five years after the termination of their functions.

Foreign Politically Exposed Persons are individuals who perform or have been entrusted with prominent public functions in this or another country, for example:

- Heads of State or Government;
- high-level politicians;
- high-level foreign governmental, judicial or international organization public officials;
- high-ranking military personnel;
- high-level Executives of state corporations;
- high-level Officials of political parties;
- Ambassadors and Consuls of other countries accredited in El Salvador; and
- individuals fulfilling or entrusted with prominent functions by an international organization.

In addition, domestic or foreign PEPs include close family members or close associates of such persons.

Close Family Member means the spouse, the person with whom partnership has been registered (i.e., the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.

Close Associate means:

- a natural person who, together with the Politically Exposed Person, is a member of the same legal entity or of a body without legal personality or maintains other business relationship;
- a natural person who is the only Beneficial Owner of the legal entity or a body without legal personality set up or operating de facto with the aim of acquiring property or another personal benefit for the Politically Exposed Person.

The Company takes measures to ascertain whether the customer, the beneficial owner of the customer or the representative of the customer is a PEP, their family member or close associate or if the customer has become such a person. For that purpose, the Company:

- asks the customer about their status in the course of the customer's onboarding applicable to all customers;
- makes reference to publicly available information;
- screens relevant persons against commercially available databases and lists for determining whether a customer or a beneficial owner of a customer is a PEP.

In case the person is identified as a PEP, close family member or close associate to PEP, he/she shall be classified as high risk and the enhanced due diligence measures shall be applied. In addition, authorization is requested from the Sole Director to establish or continue contractual relationships with such person.

In the event that a PEP, close family member or close associate to PEP is involved in cases of corruption or any crime that may generate ML/TF/FPWMD, or its risk classification changes to such an extent that it cannot be mitigated by the Company, the Compliance Officer shall follow the following procedure:

- the Compliance Officer shall immediately and within 3 business days, notify the Sole Administrator to authorize the continuity or initiation of the commercial relationship with this person.
- the notification to the Sole Administrator shall be accompanied by all the necessary information and the corresponding risk analysis evidencing the Critical Risk that cannot be mitigated by the Company.
- the Sole Director shall have up to 3 business days to decide on the authorization of the continuity or initiation of the business relationship with the customer identified as a PEP, close family member or close associate to PEP.

In the event that the Sole Director does not provide the approval on the establishment or continuity of the business relationship, the Compliance Officer may refuse to initiate the contractual relationship or terminate it.

IX. Simplified customer due diligence

Simplified customer due diligence (SDD) foresees that application of full CDD measures is not required and may be applied where the customer's risk profile indicates low risk level of ML/TF/FPWMD. The Company needs to have reasonable grounds to support the use of SDD in each particular case.

When applying SDD measures, the Company must only obtain the following data of the Customer who is a natural person:

- name(s) and surname(s);
- personal number or date of birth;
- contact details.

In case of the Customer, which is a legal entity, the following data:

- business name or name;
- legal form;
- registration number if such number has been issued;
- head office (address) and address of actual operation; and
- the Customer´s representative name(s), surname(s) and personal number or date of birth.

SDD measures include, for example:

- verification of the identity of the and the beneficial owner after the establishment of the business relationship.
- reduction in the frequency of updates of customer or counterparty identification.
- reduced degree of ongoing monitoring and review of transactions, based on a reasonable threshold.
- no collection of specific information to understand the purpose and intended nature of the business relationship, but rather the purpose and nature is inferred from the type of transactions or business relationship established.

SDD measures shall not be applied in the circumstances where EDD measures (as described below) must be carried out or where in the course of performing ongoing monitoring of the business relationship, it is established that the risk of ML/TF/FPWMD is no longer low, and the Company must apply the relevant level of CDD measures.

X. Enhanced due diligence measures

The Company applies Enhanced Due Diligence (EDD) measures where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high-risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product the Company provides or from a customer of the Company.

What the EDD actually entails will be dependent on the nature and severity of the ML/TF/FPWMD risk.

X.I. High-risk situations

In any situation that by its nature presents a higher risk of ML/TF/FPWMD, Company takes additional measures to mitigate the risk of ML/TF/FPWMD. The Company always applies EDD measures, when:

- the customer's risk profile indicates high risk level of ML/TF/FPWMD;
- upon identification of the customer or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
- in the case of performance of transaction or business relationship with the PEP (either domestic or foreign), the family member of the PEP or a person known to be the close associate of the PEP;
- where transaction or business relationship are carried out with natural persons residing or legal persons established in high-risk countries as identified by FATF;
- the customer is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CTF systems that are in accordance with the recommendations of the FATF.

Prior to applying EDD measures, the Company ensures that the business relationship or transaction has a high risk and that a high-risk rate can be attributed to such business relationship or transaction. Above all, the Company assesses prior to applying the EDD measures whether the features

described above are present and applies them as independent grounds (that is, each of the factors identified allows application of EDD measures with respect to the customer).

X.II. Scope of EDD measures

In case when EDD measures must be applied, the amount of EDD measures and the scope shall be determined by the Company's employee, who is applying such measures.

The following additional and relevant due diligence measures may be followed for **natural persons**:

- obtaining additional information about the origin of their assets and/or funds, their net worth and their business relationships with other regulated entities;
- conducting an interview with the customer and a visit to their facilities by the business unit with a written report of the result of the interview.

The following additional and relevant due diligence measures may be followed for **legal persons**:

- obtaining additional information about the origin of assets, equity and source of funds;
- conducting an interview with customer and a visit to their facilities by the business unit with a written report of the result of the interview;
- identifying the managers of the potential customer;
- obtaining Senior Management approval to establish or continue business relationships with those customers rated as high risk or categorized as PEP;
- conducting enhanced ongoing monitoring of the business relationship, increasing the number and duration of controls applied, and selecting transaction patterns that need further scrutiny;
- obtaining additional information about the customer and update customer and beneficial owner identification data;
- obtaining additional information about the intended nature of the business relationship;
- obtaining information on the reasons for the transactions attempted or carried out;
- any other enhanced measure that is effective and proportionate to the risks identified by the Company.

The Company establishes **procedure for application of EDD measures** as separate document (annex 6), which specifies criteria for application of certain EDD measures, as well as procedure for such measures' application.

X.II.I. High-Risk third countries

With respect to business relationships or transactions involving natural persons residing or legal persons established in high-risk third countries as identified by FATF, the Company applies the following EDD measures:

- obtaining additional information on the customer and on the beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner;
- obtaining information on the reasons for the intended or performed transactions;
- obtaining the approval of Compliance Officer for establishing business relationships with these customers or continuing business relationships with them;
- conducting enhanced monitoring of the business relationship with these by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

When applying EDD in the cases where transactions and business relationships are carried out with natural persons residing or legal persons established in **high-risk third countries** (identified according to lists of jurisdictions with strategic deficiencies in their frameworks to combat ML/TF/FPWMD published by the FATF), and in the cases where higher risk of ML/TF/FPWMD is identified based on the risk assessment made by the Company, the Company shall apply one or several additional measures to identify the customer and of the beneficial owner to decrease the risks posed and must:

- obtain approval from the Compliance Officer for establishing business relationships with such customers or continuing business relationships with these customers;
- take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
- perform enhanced ongoing monitoring of the business relationships with such customers.

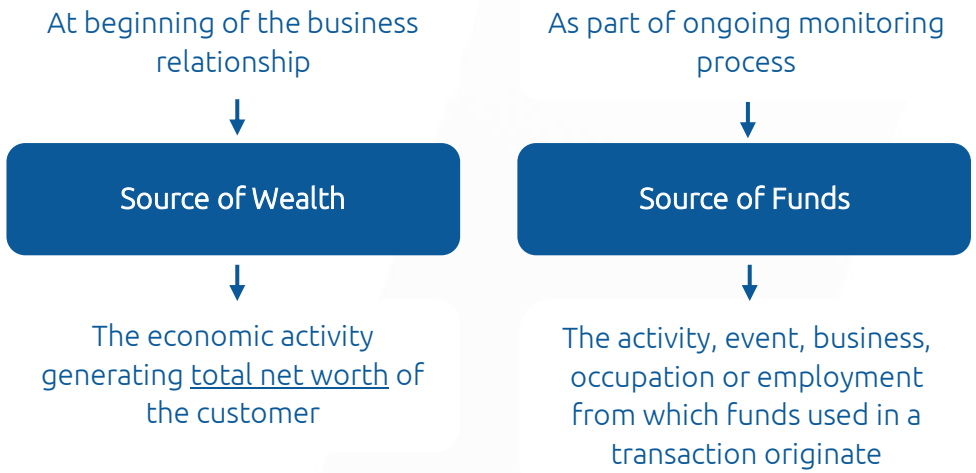
X.III. Source of Wealth and Funds

Establishing the Customer's source of wealth (SoW) and source of funds (SoF) is a core requirement of EDD.

Source of Wealth refers to the origin of the customer's entire body of wealth (i.e. total assets). SoW explains activities the customer participates in and their geographical location. This information will usually give an indication as to the volume of wealth the customer could be expected to have, and a picture of how the customer acquired such wealth. When establishing SoW, there is no need to establish funds used in specific transaction. The goal of SoW establishment is to understand and verify, that customer´s SoW corresponds with data given by the Customer when onboarding and volume of the customer´s wealth allows them to perform transactions with expected turnover specified by the customer.

Source of Funds refers to origin of funds being deposited, received, or transferred with the Company. SoF tells where the assets is coming from, which can be proven through bank statements, tax returns or the customer´s financials, etc. Typically, SoW is requested when establishing business relationship or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to the Company. The Company collects information relating to SoW or SoF of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.



The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to Company.

The following documents, data, or information could be considered reliable and independent:

- government-issued or registered documents or data;
- full bank and other investment statements;
- full payslips or wage slip or other documents confirming salary;
- inheritance (stamped grant of probate, stamped grant of letters of administration);
- audited financial accounts;
- letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;

- a copy of a will;
- sales and purchase agreements.

For customers who conduct their business with Company there is a range of documents that Company can use to verify how funds have been acquired (e.g., balance statements and other accounting documents, contract with counterparties, invoices, proof(s) of work, etc.).

The company establishes limits on the volume of transactions, after which the source of funds must be requested, in the requirements for transactions monitoring (as specified below).

XI. Employee Awareness

In order to ensure the proper functioning of the Company and guarantee the preservation of the moral and ethical quality of the Company's employees, there are personnel selection mechanisms that allow to know in a comprehensive manner the aspects that are part of the employees (specifically those related to the personal, professional, family etc.). For this purpose, the person in charge of hiring, in the process of application and selection of personnel, will request the information and documentation considered relevant, which will be filed in the file that will be kept for each employee.

Prior to any hiring, the Human Resources Manager may document, through the Criminal Record, National Civil Police Solvency and others deemed necessary, that the candidate has not been convicted of crimes related to ML/TF/FPWMD. Likewise, the Human Resources Manager shall confirm with the Compliance Officer that the applicant is not mentioned in the list of the UN, OFAC or the list issued by the FIU.

The following minimum information and documents shall be collected from the candidate and kept in the respective employee file once their hiring has been formalized:

- evidence of consultation on caution and blacklists;
- staff engagement form;
- resume (CV);
- copy of identity document;

- copy of NIT or tax identification number;
- copy of social security or social security documents;
- copy of main titles
- original of Police Clearance Certificate
- criminal record.
- for key positions, a home visit, as applicable.

In addition, prior to any hiring, the person in charge of hiring must verify the candidate or employee on the lists previously mentioned. Evidence of this verification must be filed in the employee's file. The information and documents of the employee's file must be updated at least once every two years.

XII. Ongoing monitoring

In the course of the **ongoing monitoring of the business relationship**, the Company monitors the transactions concluded during the business relationship in such a manner that the Company can determine whether the transactions to be concluded correspond to the information previously known about the customer (i.e., what the customer declared upon the establishment of the business relationship or what has become known in the course of the business relationship).

The Company also monitors the business relationship to ascertain the customer's activities or facts that indicate criminal activities, ML/TF/FPWMD or the relation of which to ML/TF/FPWMD is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question. In the course of the business relationship, the Company constantly assesses the changes in the customer's activities and assesses whether these changes may increase the risk level associated with the customer and the business relationship, giving rise to the need to change the customer's risk level assigned and to apply EDD measures.

The Company establishes and maintains the **requirements for transactions monitoring** as separate document (annex 7), which contains set of measures shall be applied in the course of ongoing monitoring of the business relationship.

XII.I. Risk-based approach to monitoring

The extent of ongoing monitoring is linked to the determined customer's risk profile. The Company takes additional measures when monitoring the business relationships posing a higher risk. High-risk customers, for example PEPs, require more frequent and intensive monitoring.

The Company conducts ongoing monitoring on a risk-based approach and considers:

- the nature and type of transactions (e.g., abnormal size or frequency);
- the nature of a series of transactions (e.g., a number of transfers);
- the amount of any transactions, paying particular attention to particularly substantial transactions;
- the geographical origin/destination of a deposit or withdrawal;

- the customer's normal activity or turnover;
- specific transactions patterns, published by relevant authorities (e. g. FATF);
- the results provided by the third-party solutions used..

The Company is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of the customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

Where the nature of the business relationship changes significantly, the Company carries out applies relevant measures to ensure that the ML/TF/FPWMD risk involved, and nature of the business relationship are fully understood by the Company. Ongoing monitoring procedures take account the above changes.

XII.II. Methods and procedures

When considering how to monitor its business relationship with the customer, the Company takes into account the following factors:

- the size and complexity of the Company's business;
- its assessment of the ML/TF/FPWMD risks arising from the Company's business;
- the nature of the Company's systems and controls;
- the monitoring procedures that already exist to satisfy other business needs of the Company;
- the nature of the products and services (which includes the means of delivery or communication).

The Company takes the four steps systemic approach for ongoing monitoring of the business relationship:

Measures, used by the Company for ongoing monitoring of established business relationships is divided into two following categories.

Screening – monitoring transactions in real-time in real time on the basis of the parameters or characteristics previously determined. Screening measures are applied to the transaction before or immediately after completion of the transaction and may require the following actions:

- transaction suspension;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;
- sending an internal report to the Compliance Officer;
- sending an external report to the FIU.

Monitoring – analysis of transactions after their performance for the purpose to identify transactions and circumstances that could not be identified in real time or that, due to the nature of the transaction, did not appear in the parameters of screening. Monitoring measures may require the following actions:

- account suspension;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;
- sending an internal report to the Compliance Officer;
- sending an external report to the FIU.

In both cases (screening & monitoring), the Company uses technological solutions (incl. third-party solutions), as well as appoints employees responsible for the ongoing monitoring of the business relationships in according with requirements established.

XII.III. Suspicious Transactions Warning Signs

When establishing and maintaining requirements for ongoing monitoring of the business relationship, the Company takes into account the Technical Standards for managing the risks of ML/TF/FPWMD, as well as other sources, incl. guidelines of international organizations (e. g. FATF). The following are some of the suspicious activity warning signs most commonly associated with ML/TF/FPWMD:

- frequent and unexplained account movements to different persons;
- frequent and unexplained movements of funds between individuals in various geographic locations;
- suspicious activity based on transaction pattern, i.e.
  - account used as a temporary repository for funds;
  - a period of significantly increased activity amid relatively dormant periods;
  - "structuring" or "smurfing" i.e. many lower value transactions conducted when one, or a few, large transactions could be used;"
  - U-turn" transactions, i.e. funds pass from one person to another, and then back to the original person or company;
  - excessive transactions just below established thresholds (e. g. reporting, CDD/EDD limits, etc.);
  - excessive transfers between several counterparties.

- involvement of one or more of the following entities which are commonly involved in ML/TF/FPWMD:
  - shelf or shell companies;
  - company registered in a known "tax haven" or “offshore” financial centre;
  - casinos and gambling entities;
  - money remittance companies;
  - banks or financial institutions that do not have a physical presence in any country;
  - financial cooperatives;
  - pawnshops;
  - non-governmental organizations and foundations;
  - arms manufacturers, traders and brokers;
  - DNFBPs;
- the customer refuses or is unwilling to provide documents or information necessary to determine the customer’s or the beneficial owner’s identity or submits documents or information that raise doubts about their veracity, authenticity, etc.;
- the customer refuses or is unwilling to provide information or documents necessary for the business relationship monitoring (e.g. explanation of their activity, information about their SoW/SoF) or submits documents or information that raise doubts about their veracity, authenticity, etc.;
- activity is incommensurate with that expected from the customer considering the information already known about the customer (e.g. SoW, country of residence or establishment) and the customer’s previous activity;
- deposits from or withdrawals to a digital wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports;
- currencies, countries or residents of countries, commonly associated with international crime or drug trafficking or identified as having serious deficiencies in their anti-money laundering regimes;
- currencies, countries or residents of countries, commonly associated with terrorist activities or the persons or organizations designated as terrorists or their associates;
- PEPs and close family members or close associates of such persons.

XIII. Sanctions policies

In addition to AML/CTF framework, this Manual also covers the Company's obligations related to implementation of sanctions legally binding to the Company. The Company follows the FIU Instructions and takes measures to ensure compliance with the relevant regulations and legislation on sanctions in El Salvador. It is particularly vital that the Company is able to identify sanction subjects and transactions violating sanctions, which may arise in the course of the Company's business activity. The Company takes into account, at least, the following sanctions regimes:

- United Nations Security Council;
- Office of Foreign Assets Control.

By the decision of the Compliance Officer, the Company may follow other sanction regimes and restrictive measures.

XIII.I. Procedure for identifying the subject of sanctions and a transaction violating sanctions

The Company verifies whether the customer or their beneficial owner is a subject of Sanctions in the course of the customer's onboarding procedure.

To avoid establishing business relationship or conducting transactions with any subjects of sanctions, the Company implements an effective screening mechanism, which includes:

- screening customers and beneficial owners of customers against sanctions watchlists at the establishment of the Business Relationship;
- screening the Customers and the Beneficial Owners of the Customers against sanctions watchlists as soon as practicable (i.e., when any of watchlists has been updated);
- screening of transactions for the purpose to identify connection to subjects of sanctions.

To verify that the persons' names resulting from the inquiry are the same as the persons listed in the document imposing sanction(s), their personal data shall be used, the main characteristics of which are, for a legal entity, its name or trademark, registry code or registration date, and for a natural person, their name and date of birth. In order to establish the identity of the persons specified in the relevant legal act or notice being the same as

those identified as a result of the inquiry from databases, the Company analyses the names of the persons found as a result of the inquiry based on the possible effect of factors distorting personal data (e. g. transcribing foreign names, different order of words, substitution of diacritics or double letters etc.).

If sanctions subject is identified – the relevant notice must be sent to the Compliance Officer. If the Company's employee has doubts that a person is a subject of sanctions, this employee shall immediately notify the Compliance Officer. In this case the Compliance Officer shall decide on whether to ask or acquire additional data from the person or notify the FIU immediately of their suspicion.

XIII.II. Actions when identifying the sanctions subject or a transaction violating sanctions

If the Company becomes aware that the customer which is in the business relationship with the Company, as well as a potential customer intending to establish the business relationship or to perform a transaction with the Company, is the subject of sanctions, the Company's employee shall immediately notify the Compliance Officer about the identification of the subject of sanctions, or the doubt thereof.

The Company will not establish business relationship with potential customers subject to Sanctions.

In case the customer is subject of the lists of persons designated by virtue of the resolutions of the United Nations Security Council, the following actions must be taken:

- the Company shall refrain from carrying out operations until the receipt of instructions from the competent judicial authority, including refraining from terminating business relations with the persons designated by the resolutions of the United Nations Security Council;
- the Company shall report it to the FIU via email within 3 working days;
- the Company shall wait for further instructions from the FIU regarding actions that shall be taken.

When identifying the subject of the sanctions, it is necessary to identify the measures that are taken to sanction this person. These measures are described in the legal act implementing sanctions; therefore it is necessary to identify the exact sanction what is implemented against the person to ensure legal and proper application of measures.

XIV. Reporting

XIV.I. Internal reporting

Any employee of the Company who becomes aware of information about unusual or suspicious activity in the operations of any customer, is obliged to notify the Compliance Officer as soon as possible as provided below. Employees must not delay any disclosures unnecessarily.

In case when necessity to notify the Compliance Officer arise, such notification shall be performed by filling internal report in the form approved (annex 8). Internal report shall be prepared and signed by the employee. Signed internal report shall be sent to the Compliance Officer physically or electronically as soon as possible but not later than 24 hours after necessity to send report has arisen. In addition to the above, the employee must leave a record of the analysis of the unusual or suspicious operation, with its respective conclusion.

It should be note that if the necessity of internal report arises, the Company must immediately postpone the transaction (if possible).

The Compliance Officer shall have a term of fifteen working days to analyse (e. g. sending external report, terminate the transaction or the business relationship, perform further investigation, etc.) the internal report. This period is extendable only once, for the same period, upon request to the FIU through email.

As a result of the analysis carried out, the Compliance Officer shall take the following actions:

- conclude that it is a suspicious transaction and proceed to prepare the Suspicious Transaction Report (STR) which must be sent to the FIU;
- conclude that this is a normal operation and close the case.

In both cases, all analyses and supporting information justifying the action to be taken in each case must be recorded.

XIV.II. External suspicious transaction reporting (STR)

The Company must suspend the transaction disregarding the amount of the transaction (except for the cases where this is objectively impossible due to the nature of the transaction, the manner of execution thereof or other circumstances) and the Compliance Officer must report to the FIU on the activity or the circumstances that they identify in the course of economic activities and whereby the Company has established that the Customer is carrying out a suspicious operation or transaction.

Suspicious monetary operations or transactions shall be identified:

- by noting the activities of customers which, by their nature, may be related to ML/TF/FPWMD;
- when conducting the customer's and the beneficial owner's identification;
- when conducting ongoing monitoring of the business relationship, including the investigation of transactions that have occurred during that relationship.
- in accordance with the minimal characteristics of suspicious transactions or operations performed by the customer provided in the Technical Standards for Managing the Risks of ML/TF/FPWMD.

The mere fact that the customer of the Company, after the application of CDD measures and/or establishment of business relationship, appears in any adverse media, relating it to an investigation or criminal activity, is not a cause for submitting a STR, unless a substantiated analysis has been made on such customer, which supports the submission of such report.

STR shall be sent to the FIU within a maximum period of five working days, counted from the moment when, according to the analysis carried out, there are sufficient elements of judgment to consider the transaction or operation irregular, inconsistent or unrelated to the type of economic activity of the customer. In addition, the report of suspicious transaction shall be sent to the FIU when there are reasonable grounds to believe that the money or assets are related to or could be used for terrorist acts or terrorist organizations, organized crime, drug trafficking and any of its variant.

The amount of the operations or transactions is irrelevant for the purposes of sending STR.

The Company shall submit STR through the corresponding form of the technological platform developed by FIU for such purpose, the information of those transactions or operations it considers suspicious related to the crimes of money laundering financing of terrorism and proliferation.

XIV.II.I. Tipping off

In general, the information obtained in the execution of the procedures and practices (incl., reporting) of this AML/CTF Manual is confidential, which means that it may only be disclosed to the competent authorities, upon request. Therefore, all employees who have responsibilities assigned by this Manual and the procedures derived from it, are obliged to safeguard and limit the use of this information to the strictly established purposes.

When the customer is the subject of an external reporting, there must be taken careful steps while communicating with the customer and additional advice should be taken from the Compliance Officer in order not to accidentally disclose investigative actions to the customer. Under no circumstances may the Compliance Officer and his or her alternate disclose the suspicious transaction reports, their analysis or support documents and annexes, the notices sent by the FIU and the answers given to these requirements.

The Company's employees are prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the FIU, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FIU or about the commencement of criminal proceedings.

XIV.III. External suspicious transaction attempt report

The suspicious transaction attempt covers situations where the suspicious transaction was not perfected because whoever tried to carry it out desisted from it or because of the controls established, refusal to be carried out or the Company prevented its realization. When it is known that a natural or legal person intends or have made an attempt to carry out an unusual or suspicious transaction, the situations covered under the attempt must be reported to FIU as an attempted suspicious transaction, using the form defined by FIU.

In cases where the customer refuses to be identified or is found to be presenting presumably false documents, the latter must be reported as an attempted suspicious transaction, attaching the documentation that has been presented.

This report must be made within five business days from the moment in which, according to the analysis performed by the Compliance Officer, it is concluded that the attempted transaction is suspicious.

XIV.IV. Reporting of regulated transactions

The Compliance Officer shall monitor the daily transactions of customers in order to identify transactions that exceed the thresholds established by the law (i.e., Regulated Transactions) and make the following respective reports to FIU:

- individual cash transaction report in case of single cash transaction that exceeds $10,000 or its equivalent in foreign currency within five business days from the day after the transaction was carried out;
- multiple cash transactions report in case of multiple cash transactions that cumulatively during one calendar month exceed $10,000 or its equivalent in foreign currency within five working days from the day following the end of the calendar month;
- individual transaction with other means report in case of single transaction with security other than paper money or cash, such as checks or credit card payments, that exceeds $25,000 or its equivalent in foreign currency within five business days as of the day following the day of the transaction;
- multiple transactions in another medium report in case of multiple transactions in other media and cash that cumulatively during the calendar month exceed $25,000 within 5 business days from the day following the end of the calendar month.

According to the article 9 of the LCLDA, the Regulated Transactions reports shall be sent by the Compliance Officer to FIU in writing via email or by any electronic means.

XIV.V. Supplementary transactions reporting

The Compliance Officer, as applicable, shall report the following supplementary transactions:

- international wire transfers of funds equal to or greater than $1,000 or its equivalent in foreign currency;
- local wire transfers generated through electronic devices or applications, equal to or greater than $1,000 or its equivalent in foreign currency.

- family remittances equal to or greater than US$200 or its equivalent in foreign currency.

DASPs must report individual customer transactions equal to or greater than $1,000 according to the conversion rate to U.S. Dollars on the day the transaction takes place. Such reports must be submitted through one of the 8 forms designated by the FIU, which can be found in the respective platform.

XV. Data retention

The Company must retain certain data and documents about its customers and transactions. Documents and data must be retained in a manner that allows for exhaustive and immediate response to the request from the Compliance Officer, queries made by the FIU or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

The Company shall implement all rules of protection of personal data upon the requirements arising from the applicable legislation. The Company is allowed to process personal data gathered upon CDD measures implementation only for the purpose of preventing ML/TF/FPWMD and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

In order to guarantee a greater degree of collaboration with the authorities, the Company will keep the identification data, files, analysis of unusual or suspicious transactions and correspondence with customers during Business Relationship in an electronic form for a period of no less than **five years**, counted from the date of the completion of each transaction or from the termination of the business relationship. In addition, the Company will maintain all documentation and information supporting the opening of accounts or business relationships, copies of identification documents and transactions for a period of not less than **fifteen years** in accordance with article 12 of LCLDA.

XVI. Confidentiality

The information obtained in the execution of the procedures and practices that make up a part of this AML/CTF Manual is confidential, which means that it may only be disclosed to the competent authorities, upon request. Therefore, all employees who have responsibilities assigned by this

AML/CTF Manual and the procedures derived from it, are obliged to safeguard and limit the use of this information to the strictly established purposes.

Given the nature of the information handled by the Company, the sensitivity of the data residing in the information systems is subject to proper control and limited access specified in the **data processing file** (annex 9).

XVII. Training

Each year, the Compliance Officer must design an annual training plan for all personnel hired or subcontracted by the Company, which must include all ML/TF/FPWMD risk prevention and control issues, to support the identification of unusual or suspicious situations in the handling of operations of the Company. The Company developed a **draft of the annual training plan** (annex 10), which must be updated and redesigned annually in accordance with the training needs. The annual training plan shall be submitted for approval to the Sole Director no later than December 31 of each year, for implementation in the year immediately following its approval.

Training for personnel hired and subcontracted by the Company may be done **externally** by attending training events or hiring expert facilitators in the respective field, as well as **internally** by the Compliance Officer.

The training content shall include, at least, the following fundamental aspects, depending on the characteristics of the target group of employees:

- raising awareness of AML/CFT in the corporate culture;
- regulatory standards, requirements and fundamental concepts of ML/TF/FPWMD
- organizational and control structure of the Company for the prevention of ML/TF/ FPWMD
- knowledge of customers, counterparties and the market;
- implementation of policies and procedures for the prevention of ML/TF/FPWMD;
- knowledge of ML/FT/FPWMD warning signs;
- detection of unusual or suspicious transactions and reporting of suspicious transactions;
- information management,
- knowledge of the employee.

All training provided to personnel of the Company should be documented in a file, whether the training is provided by in physical or digital form that shall include the following documents:

- documents used for the development of the annual training plan;
- the duly signed **training attendance protocol** (annex 11);
- evidence of evaluation of the training or workshops by the employees.

XVII.I. Induction

All newly hired employees or outsourced personnel must receive a mandatory induction on ML/FT/FPWMD prevention within 30 days of joining the Company. The human resources area or its equivalent, in coordination with the Compliance Officer, is responsible for scheduling the induction of employees and outsourced personnel.

The following aspects must be complied with in the induction process for new personnel:

- Presentation of generalities and consequences of ML/FT/FPWMD offenses and sensitization of the culture of prevention of these offenses.
- Knowledge of policies and procedures for the prevention, control and detection of suspicious transactions.
- Examination of knowledge of the policies and procedures for the prevention, control and detection of suspicious operations.

The induction of all employees and outsourced personnel must be documented in a physical or electronic form.

XVIII. Review and controls of the Compliance Manual

XVIII.I. Internal Audit

The performance of this Manual shall be reviewed by the Auditor, or whoever performs similar functions within the Company, in order to ensure effectiveness of AML/CTF Compliance Manual (hereinafter – the Internal Control). The Auditor must have the required competency, tools, and access to the relevant information in all structural units of the Company. The internal audit must be carried out in accordance with the activities, nature, size, operations and risk level of the Company, in accordance with the risk-based approach. The Internal Control shall be performed on the basis of an annual plan for the verification of compliance with policies and procedures for the prevention of ML/TF/FPWMD.

In course of Internal Control performed by the Auditor, or whoever performs similar functions within the Company, at least the following controls shall be applied on annual basis:

- evaluation of compliance and effectiveness of the rules applicable to the policies and procedures for the prevention and control of ML/TF/FPWMD.
- evaluation of the procedures for detection of unusual or suspicious operations and reporting;
- validation of the sending of reports by means of a sampling.

The internal Control over the obligation to report suspicious transactions and transactions that exceed the threshold of Regulated Transactions established by the law shall be performed through the access to administrative and statistical information and, as appropriate, the acknowledgement of receipt or confirmation of sending, which allows to verify, on a sample basis, whether the duty to make the aforementioned reports is being complied with.

An opinion should be issued regarding the adequacy and operation of AML/CTF Compliance Manual adopted to prevent ML/TF/FPWMD offenses, indicating any materially significant deficiencies or omissions, the recommendations made to overcome them, and the corrective measures adopted. The outcome of the review shall be communicated to the Sole Director, Senior Management and the Compliance Officer for appropriate follow-up.

XVIII.II. External Audit

The external auditors that are required by law to have their own control body, shall verify compliance with the rules to which the Company is subject, must evaluate this AML/CTF Compliance Manual and issue a report on compliance with the rules and instructions and with the policies and procedures for the prevention of ML/TF/FPWMD (hereinafter – the External Control), with a risk-based approach.

The External Control shall include annual work plans, the evaluation of the management and legal provisions applicable to the prevention of ML/TF/FPWMD risks and shall inform the Sole Director and the Compliance Officer in a timely manner, of any matter of which they shall be aware in relation to ML/TF/FPWMD risks.

XVIII.III. Compliance Officer review

The Company performs a review of this AML/CTF Manual, on an annual basis, which shall be the responsibility of the Compliance Officer, in which the application of the procedures and their effectiveness shall be evaluated. In addition, an opinion shall be issued regarding the adequacy and operation of the policies and procedures adopted to prevent ML/TF/FPWMD, indicating the materially significant deficiencies or omissions, the recommendations made to overcome them, and the corrective measures adopted or to be adopted, including the need for investment in technological development to make the work of the Compliance Officer more efficient.

The result of such review shall be communicated to the Sole Administrator for due follow-up within the first quarter of each calendar year. It should be noted that this review is independent of the internal and external audit work to which the Company is subject.

XIX. Annexes

Annex title	Document description
1. Resolution of approving the AMLCTF Compliance Manual	The Company´s CEO´s draft for approving this AMLCTF Compliance Manual
2. Services Description	Description of the services provided by the Company.
3. Risk Matrix	Table used for prioritizing and tracking risks on the enterprise-wide level.
4. List of Risk Factors	List of risk factors which are used for determination of the Customer's risk profile.
5. Customers' Onboarding Procedure	Description of the procedure which shall be applied in the case the Customer shall pass the onboarding procedure.
6. Procedure for Application of EDD Measures	Description of EDD measures which shall be applied to the high-risk Customers.
7. Requirements for Transactions Monitoring	List of ODD measures which shall be applied by the Company for the monitoring of transactions.
8. Internal Report Form	Internal reporting form which should be filled by the Onboarding Specialist and/or Monitoring Specialist when notifying the Compliance Officer
9. Data processing file	List of data collected about the customers and transactions and information about its processing.

10. Annual Training Plan Draft	Draft of annual training that sets out the training recipients, strategies, curriculum, and methods for training employees across the Company.
11. Training Attendance Protocol	Form which should be signed if the Employee has passed the relevant training.

Version Control Table

Approval date	Changes description
27.08.2025	First issue