AML / CTF/ CFPWMD Guideline

CORNERSTORE DIGITAL LIMITADA.

REPUBLICA DE COSTA RICA

June 2026

- This AML/CTF/CFPWMD Guideline (Guideline) has been adopted to serve as guidance for CORNERSTORE DIGITAL LIMITADA. (Company) to follow the good practices and the international standards on the prevention of ML, TF and FPWMD.
- This Guideline 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 Guideline 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 Costa Ricaand abroad.
- This Guideline shall be accepted and approved by the resolution of the Senior Management.

Administrative information

Company name: CORNERSTORE DIGITAL LIMITADA.;

World Trade Center 200-B, Suite 62;

Calle 53 Este, Marbella

Ciudad de Panama, PA

Republica de Panama.

Glossary

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFPWMD	Countering the Financing of the Proliferation of Weapons of Mass Destruction
CTF	Counter-terrorist financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FAU	Financial Analysis Unit
FPWMD	Financing of the Proliferation of Weapons of Mass Destruction
ML	Money Laundering
PEP	Politically Exposed Person
RBA	RBA Risk-Based Approach
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
TF	Terrorist Financing
UN	The United Nations
VASP	Virtual Asset Service Provider
VC	Virtual Currency

Table of Contents

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 Guideline with a view to managing and mitigating ML/TF/FPWMD risks. A qualified AML Officer has been appointed to implement appropriate AML/CTF/CFPWMD policies and procedures.

Company's key AML/CTF/CFPWMD Principles

In the course of its business activity, the Company implements the following principles:

- to comply with AML/CTF/CFPWMD legislation in the countries in which it operates;
- to strive to fulfil international standards as detailed by the Financial Action Task Force (FATF) recommendations;
- to work in conjunction with the governments of the countries the Company operates in, as well as support their objectives in relation to the prevention, detection and control of ML/TF;
- the Company may decide not to provide products or services based upon decisions guided by ML/TF/FPWMD risk appetite and corporate social responsibility;
- to comply with primary legislation of Costa Rica on AML/CTF/CFPWMD.

Company's Compliance Guideline

The Company has established this Guideline 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 Guideline is designed to represent the basic standards of AML and CTF procedures and standards, which will be strictly observed by Company.

The Guideline is based upon applicable AML/CTF/CFPWMD laws, regulations and regulatory guidance from the Government Institutions of Costa Rica. This Guideline 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 Guideline:

- forms part of its wider compliance regime;
- ensures that the Company is able to detect unusual and suspicious activities associated with money laundering, fraud, terrorist financing, 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 with;
- is built on a strong foundation of understanding of the best practices and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organisation.

Review of the Guideline

This Guideline is the subject of a review by the Senior Management at least annually. The proposal for a review and the review of this Guideline may be scheduled more often by the decision of the Company's AML Officer. The Company must review and, where necessary, update this Guideline 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 ML/TF/FPWMD Risk Assessment;
- upon receipt of an order from the relevant government authorities to 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 Guideline’s review (incl. regular annual review) shall be confirmed with the relevant resolution signed by the Senior Management.

Governance Principles

The Company's employees and the service providers (third parties) involved in the Company's activity should act in accordance with this Guideline. The obligations of the Company as defined in this Guideline 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 Senior Management, the AML Officer, etc.).

All employees of the Company, depending on the functions performed by them, shall be introduced to this Guideline. 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 Senior Management 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 Company's Senior Management must ensure that all newly recruited employees are made aware of this Guideline and the Company's structure.

The day-to-day management of the Company takes place through the Senior Management.

The Senior Management is responsible for assigning tasks to the Company's structural units and controlling the performance of tasks assigned. In case when the relevant Employee or third party is not appointed for performing of structural unit's functions, the Senior Management shall be responsible for this structural unit's functions. In addition to day-to-day management, the Senior Management organizes meetings and, if necessary, discusses decision-making with experts (incl. employees, advisors and external service providers).

Company's Services

The Company's main economic activity is services of VC exchange and VC wallet services.

Before using of new virtual currency 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 virtual currency users' anonymity. In regards of new virtual currency at least the virtual currency transactions flow and blockchain structure shall be assessed, as well as other important circumstances.

All of the Company's services of virtual currency exchange and wallet operator are provided electronically [through the website operated by the Company].

Money Laundering

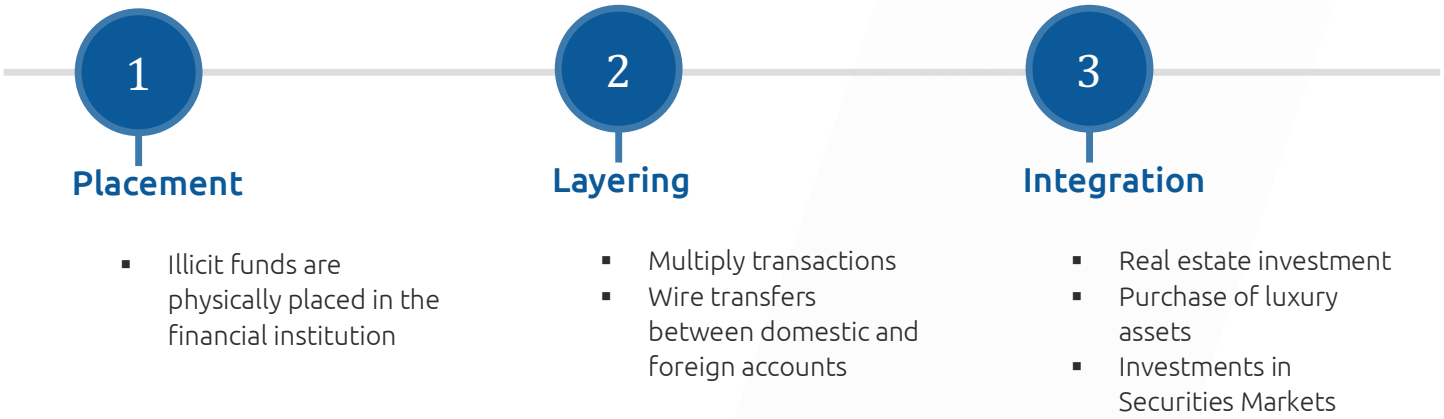
The term “money laundering” (ML) is defined as a predicate offense typified in articles 250 and 251 of the Criminal Code, meaning:

1) personally or through an intermediary, receiving, depositing, negotiating, transferring or converting money, titles, securities, goods or other financial resources, reasonably foreseeing that they come from activities related to international bribery, crimes against Copyrights and Related Rights, against Industrial Property Rights or against Humanity, drug trafficking, illicit association to commit drug-related crimes, qualified fraud, financial crimes, illegal arms trafficking, human trafficking, kidnapping, extortion, embezzlement, homicide for price or reward, against the environment, corruption of public servants, illicit enrichment, acts of terrorism, financing of terrorism, pornography and corruption of minors, trafficking and commercial sexual exploitation, theft or international trafficking of vehicles, with the purpose of hiding, concealing or disguising its illicit origin, or helping to evade the legal consequences;
2) without having participating, but knowing its origin, concealing, covering up or impeding the determination, origin, location, destination or ownership of money, goods, securities or other financial resources, or helping to ensure their profit, when these come from or have been obtained directly or indirectly from any of the illicit activities indicated in the preceding article or, in any other way, helps to ensure their profit;
3) personally or through an intermediary person, natural or juridical, in a banking, financial, commercial or any other type of establishment, with money, securities or other financial resources coming from any of the activities foreseen in point 1;
4) personally or through an intermediary, natural or juridical person, provides false information to another person or banking, financial, commercial or any other type of establishment, for the opening of a bank account or for carrying out transactions with money, securities, goods or other financial resources, coming from any of the activities foreseen in point 1.

There are three common stages in ML, and they frequently involve numerous transactions. A VASP 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.



Money Laundering using Virtual Currencies

Money Laundering using Virtual Currencies follows the above-described general pattern of placement-layering-integration with some specificities stemming from specifics of Virtual Currencies, 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 Virtual Currencies 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 Virtual Currency wallet balance and address and mixing multiple transactions with each other to exclude blockchain analysis.

- Mixer/tumbler services enable sending potentially traceable Virtual Currency to a required address with the purpose of obscuring the source of origin, thus making them untraceable. This is done through first sending Virtual Currencies from multiple addresses to one address, where the Virtual Currency is mixed/tumbled together. The Virtual Currency is then split into several portions and sent to different addresses. This process may be repeated several times before the Virtual Currency reaches its final destination address.

The following list (non-exhaustive) provides examples of possible scenarios describing how the services of VC exchange operator and custodian VC wallet operator 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 – Virtual Currency is then purchased from a VASP 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 Virtual Currency is then sent shortly after to a single VC wallet in a VASP 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 Virtual Currency and issues a private loan to the criminal in Virtual Currency and they agree for cash payments for repayment of the loan. Criminal receives the funds through a VASP, and never makes the repayment.

Example 3

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

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

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

Terrorist Financing

The term "terrorist financing" (TF) is typified as the financing of the crimes defined as "terrorism" specified in articles 289-291 of the Criminal Code, meaning:

- with the purpose of disturbing the public peace, causing panic, terror or fear in the population or in a sector of it, using radioactive material, weapon, fire, explosive, biological or toxic substance or any other means of mass destruction or element having such potential, against living beings, public services, goods or things;
- knowingly financing, subsidizing, concealing or transferring money, goods or other financial resources or of any other nature, to be used in the commission of terrorism as described above even if the person does not intervene in its execution or it is not consummated;
- using the Internet to teach how to build bombs or recruit people to carry out acts for terrorist purposes.

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.

Financing of the Proliferation of Weapons of Mass Destruction

The term "financing of the proliferation of weapons of mass destruction" (FPWMD) is defined by the FATF as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials.

TF and FPWMD are interconnected based on the fact that FPWMD might be a means for supporting the undertaking of terrorist activities. Therefore, its countering is essential for the prevention of terrorist acts. FPWMD often uses the same channels as terrorist financing, meaning that the measures to be applied for CFPWMD purposes would therefore often be similar to the measures applied in the case of CTF.

AML/CTF/CFPWMD systems

Effective Controls

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

- effective AML/CTF/CFPWMD Guideline;
- Senior Management oversight
- appointment of the AML Officer and other employees with certain responsibilities;
- compliance and audit function;
- staff training.

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

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 risk. 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/CFPWMD obligations.

Senior Management Responsibilities

The Company's Senior Management is responsible for all Senior Management functions. The Company's Senior Management responsibilities include but are not limited to:

- maintaining compliance with effective laws of Costa Rica;
- monitoring and overseeing the compliance activities of the Company to ensure they are in accordance with the applicable laws, regulations and internal policies and procedures;
- reviewing the AML/CTF/CFPWMD Compliance Guideline to ensure it is comprehensive, adequate and viable;
- approving the AML/CTF/CFPWMD Compliance Guideline;
- ensuring that the AML/CTF/CFPWMD Compliance Guideline is effectively implemented by the Company's AML Officer and other employees;
- Designating a qualified employee to serve as the Company's AML Officer;
- Reviewing the performance of the AML Officer;
- Ensuring that the AML Officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CTF/CFPWMD Compliance Guideline based on the Company's risk profile;
- Periodically receiving and reviewing reports presented by the AML Officer to ensure that the compliance Guideline is being executed as approved and that it is, in fact, serving its intended purpose of maintaining the integrity, safety and soundness of the Company;
- Annually reviewing changes proposed to be made to AML/CTF/CFPWMD Compliance Guideline, and, if satisfied that the modifications are desirable, approving the modifications/changes;
- Designating and contracting the services of a competent entity to perform independent compliance audits of the Company to test for the Company's level of adherence to the applicable AML/CTF/CFPWMD laws and regulations.

The Senior Management of the Company have approved this AML/CTF/CFPWMD Compliance Guideline and the designation of the AML Officer and have assigned responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CTF/CFPWMD requirements.

Customer Support Department

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.

Compliance Department

AML Officer

The AML 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/FPWMD risks are adequately managed.

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

In particular, the AML Officer assumes responsibility for:

- developing and/or continuously reviewing the AML/CTF/CFPWMD systems (incl. risk assessment made thereof) to ensure they remain up-to-date and meet current statutory and regulatory requirements;
- the oversight of all aspects of the AML/CTF/CFPWMD systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
- reviewing all internal disclosures and exception reports and determining whether or not it is necessary to refuse to perform a transaction or refuse to conclude/terminate a business relationship;
- maintaining all records related to such internal reviews.

In addition, the AML Officer:

- organizes conducting of on-going monitoring of the Company's relationships with it customers and reviews of monitoring conducted on a regular basis;
- identifies suspicious transactions and activities;
- monitors changes of best practices and regulatory requirements with respect to ML/TF/FPWMD prevention and counteraction; communicates all AML/CTF/CFPWMD relevant issues to the Senior Management;
- develops internal training Guidelines and materials, as well as receives relevant trainings.

- perform other functions which are assigned to the AML Officer under the applicable law, internal policies, job description.

Investigation Unit

Investigation Unit works Under the auspice of the AML Officer. The following functions shall be performed by the Investigation Unit:

- assistance of the AML Officer regarding reviewing received internal disclosures and exception reports;
- perform other functions which are assigned to the Investigation Unit under the internal policies and job description.

Internal Audit

Internal Auditor

Audit function shall be established to perform regularly reviews of the AML/CTF/CFPWMD 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;
- availability of direct communication to Senior Management through regular committees (compliance committee) or other means of direct communication.

The performing of audit functions shall be ensured by the decision of Senior Management, which should be adopted, at least, on annual basis. The Senior Management may decide to avoid performing of audit for specific period if such decision doesn't affect the Company's exposure to ML/TF/FPWMD risks and it is confirmed by the AML Officer.

Risk-based approach (RBA)

Risk based approach is the process by which the Company, according to its understanding of the risks, adopt the preventive measures corresponding to the nature of these risks in order to focus efforts more effectively; that is, the greater the risks the more extended or reinforced the measures applied to manage, mitigate and in the event of minor risks, simplified measures shall be allowed. 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.

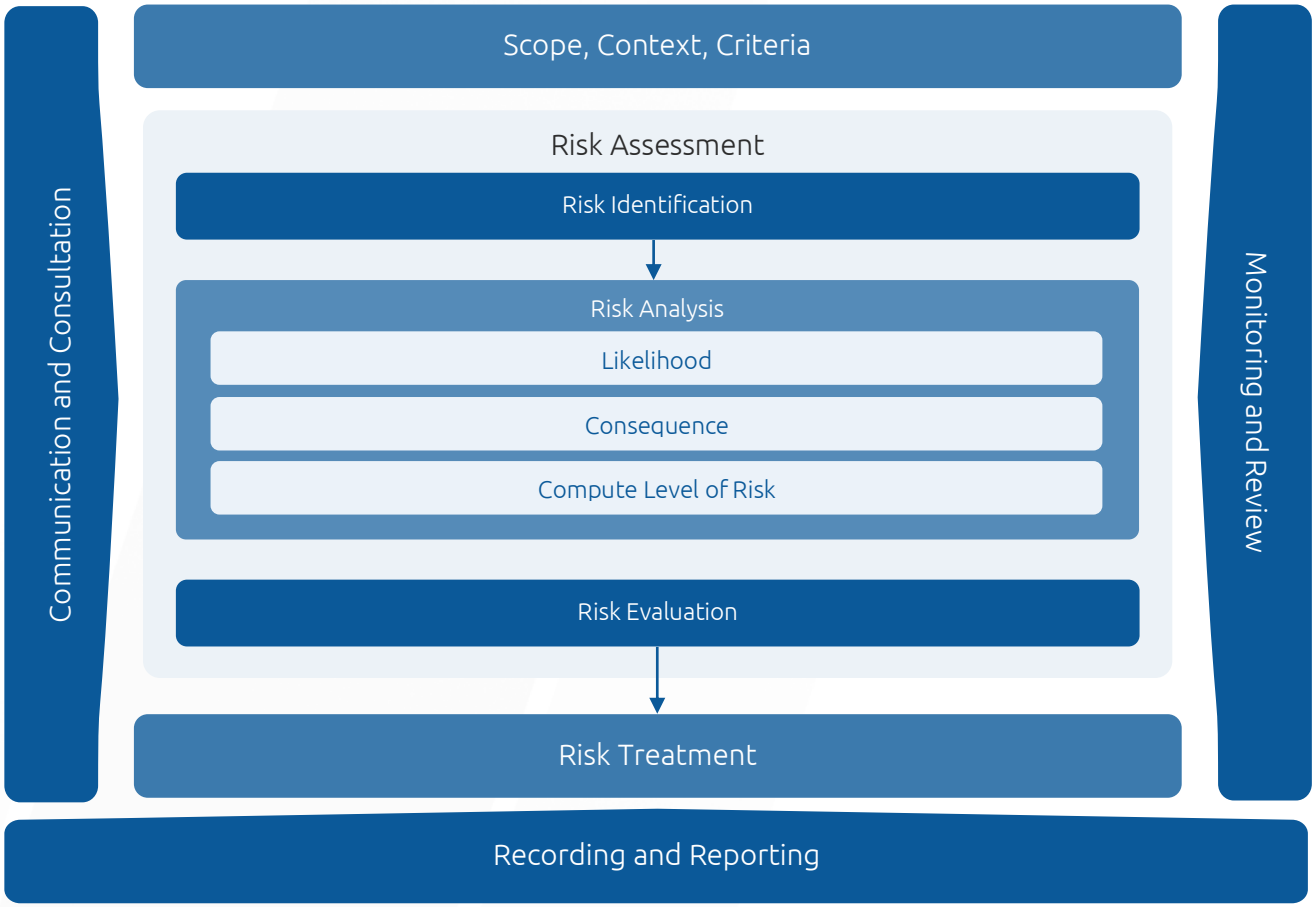
An RBA involves identifying and categorizing ML/TF/FPWMD risks at the customer level and establishing reasonable measures based on risks identified. An RBA does not refrain Company from engaging in transactions with customers or establishing business relationships with potential customers, but rather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

Risk Assessment and Risk Categories

The Company prepares and regularly updates the risk assessment in order to identify, assess, analyse and manage ML and TF 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 (laws of Costa Rica, FAU guides and manuals, etc.);
- last national risk assessment;
- last supra-national (UN-wide) risk assessment;
- guidelines of authorities (incl. international organizations);
- the knowledge previously obtained when performing activities similar to the Company.

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.

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 ML, TF or FPWMD);
- origins of the customer's wealth and opportunities to verify their soundness.

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 located in European Economic Area;
- have been identified by the FATF as jurisdictions with strategic AML/CTF/CFPWMD deficiencies;
- is subject to sanctions, embargoes or similar measures issued by UN;
- has the status of high-risk third country as established by the relevant EU regulation;
- is vulnerable to corruption or other criminal activity;
- believed to have strong links to terrorist activities.

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 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 ML, TF, FPWMD and illicit (prohibited) activities;
- product and/or service ways to promote anonymity.

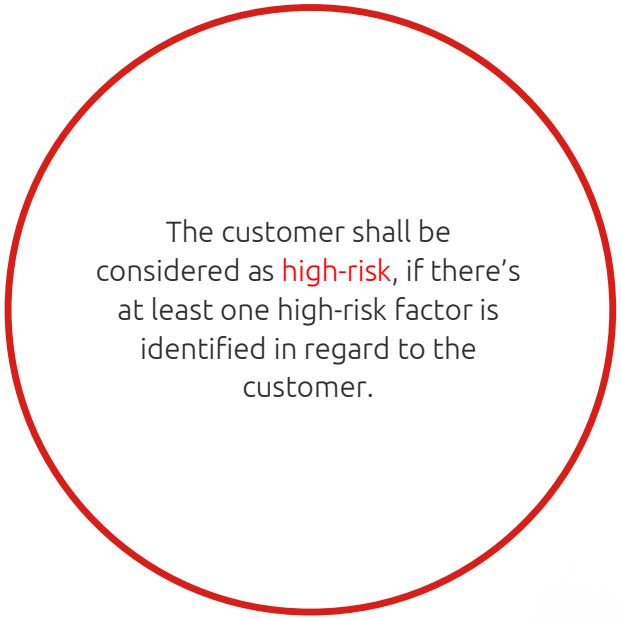
Delivery / distribution channel risk

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.).

Determination of the customer's risk profile

The Company establishes and maintains the **list of risk factors** as separate document (annex 2), 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.

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 AML Officer is permitted to alter a customer's risk profile. The AML Officer will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to customers.

Low Risk

The AML Officer will engage in annual reviews of each low-risk customer.

Medium Risk

The AML Officer performs annual reviews of every medium-risk customer that is no longer a new relationship (i. e. every 6 months after the customer's onboarding).

High Risk

Due to the high-risk nature of these relationships, the AML Officer performs monthly 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 AML Officer must also additionally verify the existence of the business and purpose of the business relationship with the Company.

Non-acceptable customers

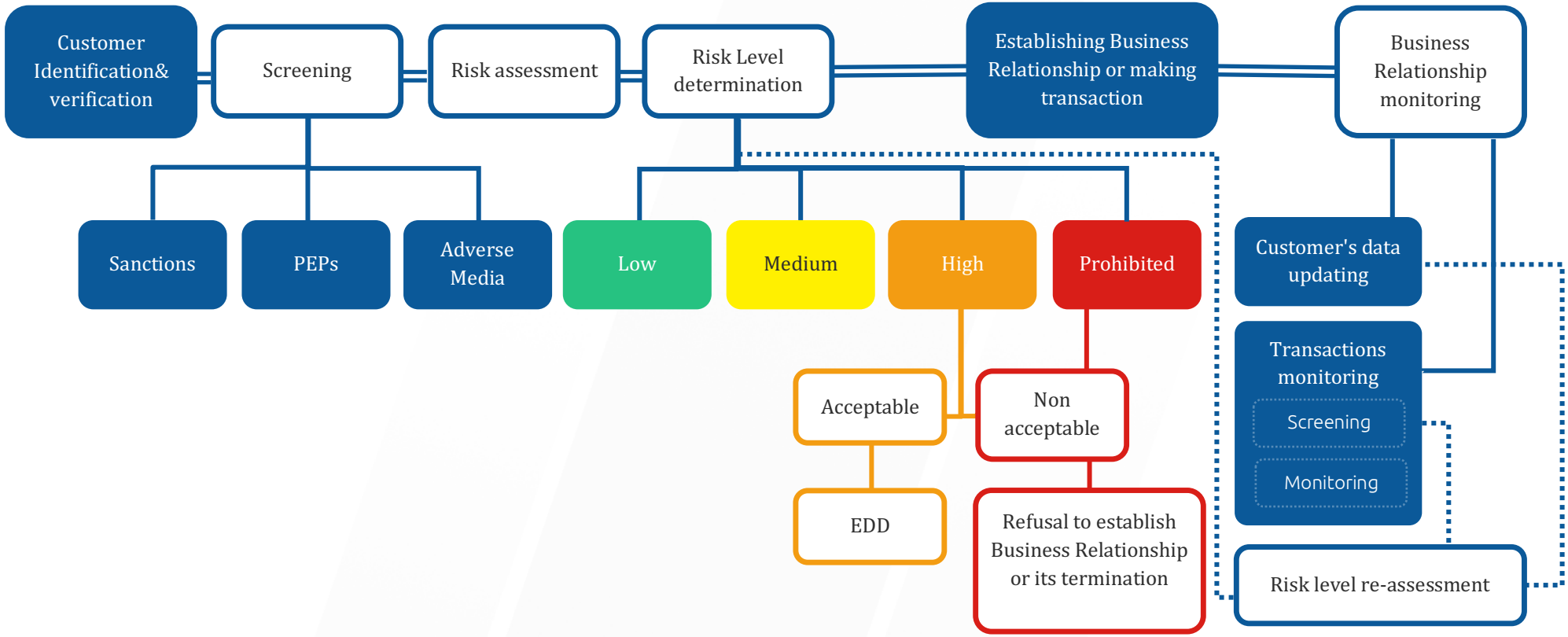
The Company has created the list of prohibited risk factors (annex 2) in the presence of which the customer will not meet the Company's risk appetite. In case, when such risk factor has arisen in the course of the customer's onboarding or before making occasional transaction – the Company refuses to 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 Guideline.

The Company may not establish a business relationship or conduct a transaction and shall terminate the business relationship where the customer does not facilitate compliance with the relevant due diligence measures.

Customer due diligence

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

- determine the money laundering and terrorism financing 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 verification of the customer's identity;
- identification and taking reasonable measures to verify the beneficial owner's identity;
- 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 information and documentation related to the financial and transactional profile of the customer;
- 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 suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in this Guideline 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.
- 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.

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 Costa Rica 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.

Timing of CDD

The Company completes the CDD process before establishing any business relationship.

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.

Where Company is unable to comply with relevant CDD requirements and the ongoing due diligence requirements, it must not establish a business relationship or carry out any occasional transaction with that customer, or must terminate business relationship as soon as reasonably practicable (where applicable).

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 virtual currency exchanges;
- one-time virtual currency transfers;
- opening and maintaining virtual currency wallets.

The Company does not provide services in the course of occasional transactions and a business relationship shall be established prior conducting any transactions.

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. In the case of customers identified as high-risk, updating of all records of due diligence information and documentation should be performed **at least annually**.
- 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.

Know Your Customer: on-boarding principles

Identification of the customer – natural person

The Company does not accept natural persons as customers.

Identification of the customer – legal entity

The Company applies the following CDD measures for the customer, who is a legal entity, to identify the customer:

- request the corresponding certifications evidencing the incorporation and validity of the customer, as well as the identification of officers, directors, attorneys-in- fact, signatories and legal representatives of such legal entities, as well as their identification, verification and domicile;
- identify and take reasonable steps to verify the beneficial owner using relevant information obtained from reliable sources[1];
- conduct the due diligence required for natural persons acting as administrators, representatives, attorneys-in-fact, beneficiaries and signatories of the customer.

The identification of the customer's representative and their right of representation

The representative of the customer who intends to act on the customer's 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.

[1] •When the beneficial owner is a legal entity, due diligence shall extend to the natural person who is the owner or controller.

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 local Law and National Constitution of Costa Rica. The authorisation issued abroad has to be legalized for use in Costa Rica 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.

The identification of the customer's Beneficial Owner

Beneficial owner is a person or natural persons who ultimately, directly or indirectly, own, control and/or exercise significant influence over the customer and/or business relationship, or the person or natural persons who exercise ultimate control over a legal person or legal structure.

The Company shall identify the beneficial owner with ownership or control, directly or indirectly, of 10% or more of the shares or participations for the customer who is a financial obligated subjects and 25% or more for the customer who is a non-financial obligated subjects.

The Company shall identify and know who the beneficial owner is, with the firm purpose of knowing the nature of the customer's activities, financial behavior and relationship with other accounts or contracts.

Identification of the nature of the customer's business

The Company shall collect information from the customer in order to understand the nature of the customer's professional or business activity and verify this information.

The Company shall request from the customer information about the customer's professional or business activity (e. g. providing the customer with an opportunity to specify their professional or business activity when collecting data about the customer).

Political Exposed Person's identification

Politically exposed person (PEP) means national or foreign persons who perform prominent public functions at a high level or with command and jurisdiction in a state, such as (but not limited to) heads of state or government, high-profile politicians, senior government, judicial or military officials, senior executives of state-owned companies or corporations, public officials holding elected office, among others who exercise decision-making in public entities; persons performing or entrusted with important functions by an international organization, such as members of senior management, i.e. directors, deputy directors and members of the board of directors or equivalent functions. Individuals holding middle or junior positions in the aforementioned categories shall not be considered as PEPs.

Close Relatives means the spouse, parents, siblings and children of the PEP.

Close Associate means a person known to have an intimate relationship with respect to the PEP, this includes those who are in a position to carry out financial, commercial or any other type of transaction, whether local or international, on behalf of the PEP.

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;
- makes reference to publicly available information;
- screens relevant persons against commercially available databases for determining whether a customer or a beneficial owner of a customer is a PEP.

The Company may not discriminate against persons who qualify as PEPs, provided that the customer complies with the requirements of the EDD measures.

Where the customer who is a PEP ceases to perform the functions and duties for which he was originally qualified as a PEP, the Company shall at least within 24 months take into account the risks that remain related to the customer and apply relevant and risk-based measures as long as it is certain that the risks characteristic of PEPs no longer exists in the case of the customer.

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.

High-risk situations

In any situation that by its nature presents a higher risk of ML/TF, 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;
- the transactions or activity of the customer does not correspond with its declared activity, financial profile, transactional profile or its background;
- 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, the close relative of the PEP or a person known to be the close associate of the PEP;
- the customer is from a country that according to the FATF do not apply sufficient measures for the crimes of ML, TF and FPWMD.

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).

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:

- examining the background and purpose of transactions and documenting findings in writing;
- obtaining the approval of Senior Management for establishing or continuing the business relationship;
- obtaining information on the SoW and SoF of the customer and their beneficial owner;
- improving the monitoring of the Business Relationship by increasing the number and frequency of the applied control measures and by increasing the number of transactions selected for further examination.

Obtaining the approval of Senior Management

The Company shall obtain the approval of Senior Management for establishing or continuing the business relationship in the case where any of the following factors is detected about the customer:

- the customer is subject to negative news related to ML , TF, violation of Sanctions and/or other offences (Adverse Media);
- the customer is a citizen of or the customer's place of residence, establishment, location (incl. location in specific region), place of business of specific infrastructure location is in or the customer's main business partners or transactions' counterparties are related to a country or jurisdiction which, based on the trustworthy sources in the country like mutual assessments, detailed assessment reports or published follow-up reports, has no valid and efficient systems of the prevention of money laundering and terrorist financing;
- the customer is a citizen of or the customer's place of residence, establishment, location (incl. location in specific region), place of business of specific infrastructure location is in or the customer's main business partners or transactions' counterparties are related to a high-risk third country as determined by the EC.

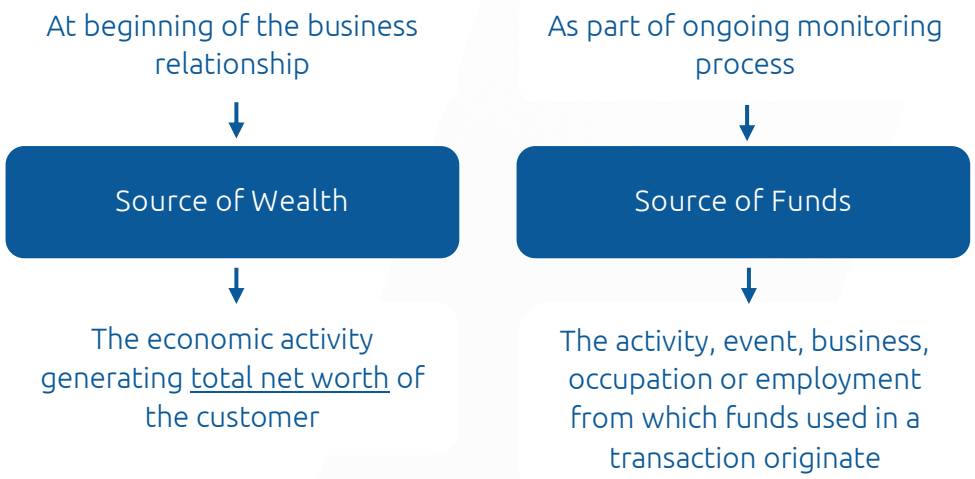
Source of Wealth and Funds

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 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 from a chartered accountant or Charities Services;
- 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).

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.

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. FAU or FATF);

- results provided by VC wallets scoring 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.

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 AML Officer;
- sending an external report to the FCIS.

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 AML Officer.

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.

Sanctions policies

The Company is not authorized to implement Sanctions (incl. to freeze assets). However, for the assessment of customer's risk level, the Company shall verify whether the customer, their beneficial owner or representative is a subject of Sanctions during the customer's onboarding and during the ongoing monitoring during the business relationship. The check for all customers is performed when any of watchlists is updated.

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 (incl. scoring of VC wallets) 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 analyzes 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 AML Officer. If the Company's employee has doubts that a person is a subject of sanctions, this employee shall immediately notify the AML Officer.

The Company must not establish a Business Relationship, refuse the established Business Relationship or terminate the business relationship upon the establishment that the customer, their Beneficial Owner or representative, is the subject of Sanctions.

Suspicious Transactions

Suspicious Transactions Indicators

When establishing and maintaining requirements for ongoing monitoring of the business relationship, the Company takes into account relevant sources, incl. guidelines of international organizations (e. g. FATF). The following are some of the suspicious activity indicators most commonly associated with ML:

- large or frequent deposits or withdrawals;
- 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:
  - shelf or shell company;
  - company registered in a known "tax haven" or "off-shore" financial center;
  - company formation agent, or secretarial company, as the authorized signatory of the bank account;

  - money service operator;
  - casino;
- 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 virtual currency address or 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 co-workers of such persons.

Internal reporting

The employees shall disclose to the AML Officer any fact, transaction or operation that has been carried out, including attempts to carry out operations, in which it is suspected that they may be related to the crimes of ML, TF and FPWMD, regardless of the amount, that cannot be justified or supported.

In case when necessity to notify the AML Officer arise, such notification shall be performed by filling **internal report in the form** approved (annex 3). Internal report shall be prepared and signed by the employee. Signed internal report shall be sent to the AML Officer's email as soon as possible but not later than 24 hours after necessity to send report has arisen. Employees must not delay any disclosures unnecessarily.

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

The AML Officer shall immediately analyze the report received and take necessary actions (e. g. terminate the transaction or the business relationship, perform further investigation, etc.).

Data retention

The Company must retain certain data and documents about its customers and transactions. Documents and data shall be retained in a manner that allows for exhaustive and immediate response to the request from the AML Officer and queries made by 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 following data and documents shall be retained for **5 years** after the termination of the relevant Business Relationship with the relevant customer:

- due diligence of the customer and the beneficial owner;
- operations performed.

The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure or receives the instruction from competent authority to extent the retention periods. The deletion of data is responsibility of the AML Officer.

Employee knowledge

The Company ensures that its employees (incl. the Senior Management and the AML Officer) have the relevant qualifications for their work tasks. When the employee is recruited or engaged, the employee's qualifications are checked as part of the recruitment/appointment process. The

Company shall adequately select and supervise the conduct of the Company's employees, especially those who hold positions related to the handling and analysis of clients, receipt of funds or VC, control of information and key controls.

The Company shall establish an employee profile, which shall be updated for the duration of the employment relationship upon the occurrence of any changes of the information in the employee profile.

Employees should be trained to understand the risks to which they are exposed, the controls that mitigate those risks, and the personal and institutional impact of their actions.

Training

In accordance with the requirements applicable to the Company on ensuring the suitability of the employees, the Company makes sure that such employees receive appropriate training and information on an ongoing basis to be able to fulfil the Company's obligations in compliance with the applicable legislation. It shall be ensured through training that the employees are knowledgeable within the area of AML/CTF/CFPWMD to an appropriate extent considering the Employee's tasks and functions.

The training is structured on the basis of the risks identified through the Company's risk assessment. For new Employees, the training consists at least of a review of the content of the applicable rules and regulations, the Company's internal policies (incl. this Guideline) and other relevant procedures.

The content and frequency of the training is adapted to the employee's tasks and function on issues relating to AML/CTF/CFPWMD measures. If this Guideline and/or any of its annexes are updated or amended in some way, the content and frequency of the training is adjusted appropriately.

The employees receive training on an ongoing basis under the management of the AML Officer in accordance with the following training plan:

- periodicity: **at least annually**;
- scope:
  - review of applicable rules and regulations;
  - specific information relating to new/updated features in the applicable rules and regulations;

- review of this Guideline and other relevant procedures and information that should facilitate such employees detecting suspected ML and TF;
- specific information on all the most contemporary ML, TF FPWMD methods and risks arising therefrom;
- report and exchange of experience relating to transactions reviewed since the previous training.

The training held is to be documented electronically and confirmed with the employee's signature on the **training protocol** (annex 4). This protocol should include the content of the training, names of participants and date of the training.

In addition to the above, the employees are kept informed by the AML Officer on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of ML, TF and FPWMD.

Internal Control of Execution of the Compliance Guideline

The performance of this Guideline shall be internally controlled by the Internal Auditor appointed by the Senior Management for performing relevant functions (hereinafter in this chapter – Internal Auditor). The Internal Auditor must have the required competency, tools, and access to the relevant information in all structural units of the Company.

The Internal Auditor shall perform internal control functions at least in the following fields:

- the Company´s compliance with established risk assessment policy and risk appetite;
- CDD/EDD measures implementation;
- the Company´s obligation to refusal to the transaction or business relationship and their termination;
- the Company´s training obligation regarding the AML/CTF/CFPWMD requirements;
- the Company´s data retention obligation.

The exact measures for performing internal control shall be determined by the Internal Auditor and shall correspond to the Company's size and their nature, scope and level of complexity of the activities and services provided. The Internal Auditor must consider at least examination fields specified above. The internal control measures shall be performed at the time determined by the Internal Auditor with the frequency set by him or her, **at least annually**, if the nature of measure does not expressly provide otherwise.

The results of internal control measures implementation (hereinafter in this chapter – the Internal Control Data) shall be saved separately from other data. Only the Senior Management and the Internal Auditor may have access to the Internal Control Data. Internal Auditor may provide access to the Internal Control Data to other Employees or third parties (e. g. advisors, other auditors, etc.) only with prior consent of the Senior Management. The persons have access to the Internal Control Data must not disclose it to anyone without prior consent of the Senior Management.

The Internal Control Data shall be saved in chronological order with format, which allows to analyze this and understandable connect this to other relevant data.

The Internal Auditor shall provide the **internal control report** (annex 5) to the Senior Management periodically and to the general meeting of the Company's shareholders at least annually. The provided internal control report shall include at least the following:

- period of exercising the internal control;
- name of the person executing the internal control;
- description of the internal control measures that has been performed;
- results of the internal control;
- general conclusions from the exercised internal control;
- determined deficiencies, which were eliminated in the period of exercising the internal control;
- determined deficiencies, which were not eliminated at the end of period of exercising the internal control;
- measures that are required to implement for elimination of determined deficiencies.

The Senior Management shall review the internal control report provided and make resolution regarding it. The Internal Auditor shall be notified about the essence of such resolution in format which can be reproduced in writing. For this reason, the Senior Management is obliged to:

- analyze the results of performed internal control;
- implement actions to eliminate deficiencies occurred.

In case, when the Internal Auditor has not been appointed by the Senior Management in accordance with this chapter, the Senior Management is responsible for performance of the Internal Auditor's duties.

In addition to internal control procedure described below, control over the performance of this Guideline should be performed in the course of internal audit, if the Company has appointed internal auditor.

Risk assessment and risk appetite

The target of the implementation of internal control measures for Company's compliance with established risk assessment policy (incl. established risk appetite) is examination of the following circumstances:

- the Company establishes and uses risk-based approach when providing services to the customers (e.g., CDD measures implemented in accordance with risk level);
- the Company determined factors which affecting the arise of ML/TF/FPWMD risks and determined factors are relevant;
- the Company determined and assessed ML/TF/FPWMD of all services which Company provides;
- the Company composed the risk profile of the customer prior the performing transactions or creating business relationship;
- the Company updates risk profile of the customer on regular basis;
- the Company follows established risk appetite;
- the Company keeps records of all incidents in accordance with established risk assessment policy;
- risk assessment policy was reviewed during the last year.

Customer due diligence measures implementation

The target of the implementation of internal control measures for Company's compliance with CDD measures implementation is an examination of the following circumstances:

- the Company apply CDD measures prescribed by this Guideline to all relevant customers;
- the Company collects proper documents and information when applying CDD measures;
- the Company properly verifies data and documents collected when applying CDD measures;
- the Company applies the relevant level of CDD measures (e. g. EDD measures, etc.);
- the Company applies proper EDD measures to specific customers (e. g. PEP, high-risk country, etc.);
- the Company performs customers´ onboarding in accordance with established procedure;
- the Company properly identifies customers´ representative(s);
- the Company properly identifies customers´ beneficial owners;
- the Company properly identifies customers´ PEP status;
- the Company understands purpose and nature of business relationship or transaction;
- the Company properly monitors business relationships with customers;
- the Company properly reports suspicious transactions to the AML Officer.

Obligation to refusal of transaction or business relationship and their termination

The target of the implementation of internal control measures for Company's compliance with obligation to refuse the transaction or business relationship and their termination is an examination of the following circumstances:

- the Company refuses or terminates transaction or business relationship if it´s obligatory in accordance with this Guideline.

Training obligation

The target of the implementation of internal control measures for Company's compliance with training obligation in AML/CTF/CFPWMD field is an examination of the following circumstances:

- all Employees (incl. the AML Officer and the Senior Management) have relevant training;
- each Employee (incl. the AML Officer and the Senior Management) has been training for the last 360 days.

Obligation of data retention

The target of the implementation of internal control measures for Company's compliance with obligation of collection and preservation of data is an examination of the following circumstances:

- all data which shall be saved in accordance with this Guideline (hereinafter in this chapter – the Saved Data) have been properly saved in chronological order with format, which allows to analyze this and understandable connect the Saved Data to other relevant data;
- only Employees (incl. the AML Officer and the Senior Management) or authorized third parties have access to the Saved Data;
- the Saved Data in electronic format has backup;
- the Saved Data in other formats (e. g. on paper) has backup in electronic format;
- the Saved Data is irrevocably deleted if it's obligatory.

Annexes

Annex title	Document description
1. Resolution of approving the AMLCTF Compliance Guideline	The Company´s Senior Management´s draft for approving this AML/CTF/CFPWMD Guideline
2. List of Risk Factors	List of risk factors which are used for determination of the customer's risk profile.
3. Internal Report Form	Internal reporting form which should be filled by the KYC Agent when notifying the AML Officer
4. Training Protocol	Form which should be signed if the Employee has passed the relevant training.
5. Internal Control Report Form	Report form which should be filled and provided by the Internal Auditor to the Senior Management and to the general meeting of the Company's shareholders periodically

Version Control Table

Approval date	Changes description	Approved by	Signature
12/06/2026	First issue	Aleksander Feldman, Director