

- This anti money laundering counter financing of terrorism and counter financing of proliferation of weapons policy (AML/CFT/CFP Policy) shall apply to all branches and subsidiaries of **Esti Technologies N.V.** (Company).
- This AML/CFT/CFP Policy consists of the 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 AML/CFT/CFP Policy 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 Curaçao and abroad.
- The AML/CFT/CFP Policy is accepted and approved by the resolution of the Company's senior management or the board of directors.

Administrative information

Company name: Esti Technologies N.V.;

Registration number: 157981;

Address: Schottegatweg Oost 10 Unit 1-9, Bon Bini
Business Center;

Email: info@estitechnologies-nv.com

March 2025

Glossary

AML	Anti-Money Laundering	PEP	Politically Exposed Person
BRA	Business Risk Assessment	RBA	RBA Risk-Based Approach
CDD	Customer Due Diligence	SDD	Simplified Due Diligence
CFT	Counter Financing of Terrorism	SoF	Source of Funds
CFATF	Caribbean Financial Action Task Force	SoW	Source of Wealth
CFP	Counter Financing of Proliferation of Weapons	UN	The United Nations
CRA	Customer Risk Assessment		
EU	The European Union		
EDD	Enhanced Due Diligence		
FATF	Financial Action Task Force		
FIU	Financial Investigation Unit Curaçao		
FT	Financing of Terrorism		
FP	Financing of Proliferation of Weapons		
GCB	Curaçao Gaming Control Board		
ML	Money Laundering		

Table of Contents

GLOSSARY	2
TABLE OF CONTENTS	3
INTRODUCTION	7
COMPANY'S KEY AML/CFT/CFP PRINCIPLES	7
COMPANY'S AML/CFT/CFP POLICY	7
REVIEW OF THE AML/CFT/CFP POLICY	8
GOVERNANCE PRINCIPLES	9
COMPANY'S SERVICES	9
MONEY LAUNDERING	10
FINANCING OF TERRORISM	10
FINANCING OF PROLIFERATION OF WEAPONS	11
AML/CFT/CFP SYSTEMS	11
PRIMARY LEGISLATION GOVERNING AML/CFT/CFP IN CURAÇAO	11
SUPERVISORY AUTHORITIES	13
EFFECTIVE CONTROLS	13
THREE LINES OF DEFENSE	14
SENIOR MANAGEMENT RESPONSIBILITIES	15
KYC AGENTS	16

COMPLIANCE DEPARTMENT.....	17
Compliance Officer.....	17
Investigation Unit.....	18
AUDIT FUNCTION.....	18
RISK BASED APPROACH (RBA).....	19
RISK ASSESSMENT.....	20
BUSINESS RISK ASSESSMENT	21
CUSTOMER RISK ASSESSMENT	22
Determination of the customer's risk profile	22
Maintaining of the customer's risk profile	23
High Risk.....	23
Medium Risk	23
Low Risk.....	23
NON-ACCEPTABLE CUSTOMERS	24
Anonymous accounts	24
Prohibited countries.....	24
Inability to complete CDD.....	25
RISK FACTORS SPECIFIC TO THE GAMBLING SECTOR.....	25
Customer risk.....	25
Geographical risk.....	26
Product, service and transaction risk	26

Distribution channels risk	27
TECHNOLOGICAL DEVELOPMENTS RISK ASSESSMENT	28
CUSTOMER ACCEPTANCE POLICY	28
CUSTOMER DUE DILIGENCE.....	29
Timing of CDD Measures	30
Minimum level of CDD measures	31
Identification and verification of the customer	32
Identification and verification of the Beneficial Owner	34
Obtaining information on the Purpose and Intended Nature of the Business Relationship	34
Politically Exposed Persons identification.....	35
Reliance on Third Parties and Outsourcing	36
SIMPLIFIED DUE DILIGENCE	37
ENHANCED DUE DILIGENCE.....	38
Politically Exposed Persons	39
Source of Wealth and Funds	40
ONGOING DUE DILIGENCE	42
Ongoing monitoring of identity.....	42
Ongoing monitoring of transactions.....	42
<i>Risk-based approach to monitoring</i>	43
<i>Methods and procedures</i>	43
REFUSAL OR TERMINATION OF THE BUSINESS RELATIONSHIP	45

TARGETED FINANCIAL SANCTIONS.....	46
PROCEDURE FOR IDENTIFYING THE SUBJECT OF SANCTIONS AND A TRANSACTION VIOLATING SANCTIONS.....	46
ACTIONS WHEN IDENTIFYING THE SANCTIONS SUBJECT OR A TRANSACTION VIOLATING SANCTIONS	47
REPORTING OBLIGATIONS.....	47
RECOGNITION OF UNUSUAL TRANSACTIONS.....	47
Objective indicators.....	48
Subjective indicators.....	48
INTERNAL REPORTING OF UNUSUAL TRANSACTIONS	49
EXTERNAL REPORTING OF UNUSUAL TRANSACTIONS	50
BLOCKING/FREEZING ACCOUNTS.....	50
TIPPING OFF.....	51
RECORD KEEPING	51
TRAINING AND SCREENING OF EMPLOYEES	53
INDEPENDENT AUDIT OF THE AML/CFT/CFP POLICY	55
EXAMINATION BY THE GAMING CONTROL BOARD	56
ANNEXES.....	ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.
VERSION CONTROL TABLE.....	ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.

Introduction

The Company adopts appropriate, sufficient measures aimed at 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 AML/CFT/CFP policy with a view to managing and mitigating ML/FT/FP risks. A qualified Compliance Officer has been appointed to implement appropriate AML/CFT/CFP policies and procedures.

Company's key AML/CFT/CFP Principles

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

- to comply with AML/CFT/CFP 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 FIU and 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/FT/FP;
- the Company may decide not to provide products or services based upon decisions guided by ML/FT/FP risk appetite and corporate social responsibility;
- to comply with the primary legislation of Curaçao on AML/CFT/CFP.

Company's AML/CFT/CFP Policy

The Company has established this AML/CFT/CFP Policy to ensure that any ML/FT/FP 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 AML/CFT/CFP Policy is designed to represent the basic standards of AML and CFT procedures and standards, which will be strictly observed by the Company.

The AML/CFT/CFP Policy is based upon applicable AML/CFT/CFP laws, regulations and regulatory guidance from the Government Institutions of Curaçao. This AML/CFT/CFP Policy 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 AML/CFT/CFP Policy:

- 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 suspicious activities associated with money laundering, fraud, and 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 also on the risk posed by the activities of customers with which the 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 organization.

Review of the AML/CFT/CFP Policy

The AML/CFT/CFP Policy is subject to a review by the senior management or the board of directors at least annually. The proposal for a review and the review of these Guidelines may be scheduled more often by the decision of the compliance officer or the Internal Control Officer. The Company must review and, where necessary, update this AML/CFT/CFP Policy and its annexes (incl. the risk assessment policy and risk assessment made thereof) in each of the following cases:

- publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment;
- upon receipt of an order from the FIU 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 AML/CFT/CFP Policy's review (incl. regular annual review) shall be confirmed with the relevant resolution signed by the senior management or the board of directors.

Governance Principles

The Company's employees and the service providers (third parties) involved in the Company's business should act in accordance with this AML/CFT/CFP Policy. The obligations of the Company as defined in this AML/CFT/CFP Policy 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 Compliance Officer, etc.).

All employees of the Company, depending on the functions performed by them, shall be introduced to this AML/CFT/CFP Policy. 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 AML/CFT/CFP Policy 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 to perform 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 is operating as an online casino as it is specified in Curaçao legislation. The Company provides services to a customer allowing for the wagering of a stake with monetary value in a game of chance. In doing so the Company opens an account for their customers. This is considered to be indicative of a relationship that is expected to have an element of duration and is therefore considered a business relationship between the Company and the customer. The Company provides the services only via electronic channels.

Before any changes in way of the services provision, the Company shall assess risks related to such changes.

Money Laundering

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Most people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for ML such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

Financing of Terrorism

Financing of terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act. The most basic difference between the financing of terrorism and money laundering involves the origin of the funds. FT uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

Financing of Proliferation of Weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

AML/CFT/CFP systems

Primary Legislation Governing AML/CFT/CFP in Curaçao

The Company shall comply with the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction¹ (Regulation) issued in the implementation of NOIS, NORUT, Sanctions National Ordinance and Kingdom Sanctions Act. In addition, the following legal acts are relevant to the Company's activity (non-exhaustive list):

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92) (hereinafter – NOIS)²;
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99) (hereinafter – NORUT)³;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73)⁴;
- Sanctions National Ordinance (N.G. 2014, no. 55)⁵;

¹ https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_regulations_for_the_combating_of_money_laundering_and_financing_of_terrorism_version_january_10_2025.pdf

² NOIS: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_92_landsverordening_identificatie_bij_dienstverlening_gt.pdf

Amendments of NOIS: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240517_pb.pdf

³ NORUT: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_99_landsverordening_melding_ongebruikelijke_transacties_gt.pdf

Amendments of NORUT: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240517_pb.pdf

⁴ Indicators for recognizing unusual transaction: https://gamingcontrol.spin-cdn.com/media/pdf_files/20191108_pb_2015_no_73_regeling_indicatoren_ongebruikelijke_transacties.pdf

Amendment of the Indicators for recognizing unusual transactions: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240611_60_mrmaw_tot_wijz_regeling_indicatoren_ongebruikelijke_transacties_1.pdf

⁵ Dutch version of UNSC Resolutions: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2014_55_sanctions_national_ordinance.pdf

English versions of UNSC Resolutions can be found here: <https://main.un.org/securitycouncil/en>

- Kingdom Sanction Act (N.G. 2016, no. 54)⁶;
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29)⁷;
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28)⁸;
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)⁹;
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)¹⁰;
- National Decree for general measures, of the 21st September 2016, for the implementation of article 7 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolution 2231 (20 July 2015) (Sanctions Decree Islamic Republic of Iran) (N.G. 2016 no. 71)¹¹;
- National Decree for general measures, of the 21st April 2017, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions 2140 (2014) and 2216 (2015) on Yemen (Sanctions Decree Yemen) (N.G. 2017 no. 46)¹²;
- GCB Requirements for Compliance Officer based on NOIS/NORUT (hereinafter – Requirements for Compliance Officer)¹³;
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

⁶ https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_wettennl_regeling_rijkssanctiewet_bwbr0038211.pdf

⁷ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_29_sanction_decree_al_qaida_taliban_isil_anf_etc.pdf

⁸ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_28_sanction_decree_libya.pdf

⁹ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_30_sanction_decree_dpr_of_korea_2015.pdf

¹⁰ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2018_34_continuance_pbs_2015_28_29_30.pdf

¹¹ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2016_71_sanction_regulation_islamic_republic_iran.pdf

¹² https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_46_sanction_decree_yemen.pdf

¹³ https://gamingcontrol.spin-cdn.com/media/aml_cft/20250115_gcb_requirements_for_compliance_officer_final.pdf

The 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 the 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/CFT/CFP 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.

Supervisory Authorities

For the purpose of compliance with AML/CFT/CFP legislation and regulation, casinos and providers of other online games registered in Curaçao are supervised by the state authority with the following details:

- name: Curaçao Gaming Control Board (GCB, also referred to as the Curaçao Gaming Authority - GCA);
- address: Scharlooweg 172-174, Willemstad, Curaçao;
- phone: +(599 9) 737-2299;
- email: info@gcb.cw.

For the purposes of unusual transaction reporting, the Curaçao Financial Intelligence Unit with the below details; acts as an independent buffer between the private sector and the criminal justice system, in the joint combat against ML, FT and FP:

- name: Curaçao Financial Intelligence Unit (FIU);
- address: Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao;
- phone: + (599 9) 462 6588;
- emails: info@fiucuracao.cw, supervision@fiucuracao.cw.

Effective Controls

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

- effective AML/CFT/CFP compliance program;

- senior management oversight;
- appointment of the Compliance Officer and other employees with certain responsibilities;
- compliance and audit function;
- staff screening and training.

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

Three Lines of Defense

The Company follows the three lines of defense framework when managing ML/FT/FP risks. The three lines of defense 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 defense are used as the fundamental guiding principle when performing the AML/CFT/CFP obligations.



Senior Management Responsibilities

The Company's Senior Management responsibilities include but are not limited to:

- maintaining compliance with effective laws of Curaçao;
- 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/CFT/CFP Policy to ensure it is comprehensive, adequate and viable;

- approving the AML/CFT/CFP Policy;
- ensuring that the AML/CFT/CFP Policy is effectively implemented by the Company's Compliance Officer and other employees;
- Designating a qualified employee to serve as the Company's Compliance Officer;
- Reviewing the performance of the Compliance Officer and assign responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CFT/CFP requirements;
- Ensuring that the Compliance Officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CFT/CFP Policy based on the Company's risk profile;
- Periodically receiving and reviewing reports presented by the Compliance Officer to ensure that AML/CFT/CFP Policy 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/CFT/CFP Policy, 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/CFT/CFP laws and regulations.

KYC Agents

KYC Agents comprise the first line of defense, 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 manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures.

The first line of defense 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 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 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 defense (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

Compliance Officer

The Company shall formally designate a senior officer at the management level and independent from the games operations, responsible for the detection and deterrence of ML/FT/FP (hereinafter – the Compliance Officer) using the **decision for the Compliance Officer appointment** (annex 1). The Compliance Officer must demonstrate professional experience, competence and integrity and comply with the requirements specified in the Requirements for 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/FT/FP and providing support and guidance to the senior management to ensure that ML/FT/FP risks are adequately managed. The Compliance Officer shall be assigned at least the following responsibilities:

- to design and implement the AML program;
- to verify adherence to Curaçao laws and regulations regarding the detection and deterrence of ML, FT and FP;
- to review compliance with the Company's policy and procedures;
- to organize training sessions for the employees on various compliance-related issues;
- to analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- to review all internally reported unusual transactions for their completeness and accuracy with other sources;
- to keep records of internally and externally reported unusual transactions;
- to design an internal procedure about when reporting unusual transactions will lead to blocking/ freezing of accounts, taking into account the risk of tipping off the player;
- to execute closer investigation of unusual transactions if necessary;
- to prepare the external report of unusual transactions;

- to make necessary changes to the AML program;
- to remain informed on the local and international developments on ML, FT and FP and to make suggestions to management for improvements; and
- to prepare periodic information on the Company's efforts against ML, FT and FP.

The above-mentioned responsibilities shall be included in the job description of the Compliance Officer. The job description shall be signed off and dated by the Compliance Officer, indicating his/her acceptance of the entrusted responsibilities. The Compliance Officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The Compliance Officer must be able to act independently.

Investigation Unit

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

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

Audit Function

Audit function shall be established to perform regularly reviews of the AML/CFT/CFP systems to ensure their effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/FT/FP and the size of the Company's business, as well as regulatory requirements. Where appropriate, the 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**;

- adequately resourced internal audit department or an outside independent party is leveraged to perform the auditing;
- 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 an annual basis**.

Risk Based Approach (RBA)

Based on the FATF Recommendations, the Company shall apply a risk-based approach (hereinafter – RBA) when designing policies, procedures and controls to combat ML, FT and FP. By adopting an RBA, the Company is able to ensure that measures to prevent or mitigate ML, FT and FP are commensurate with the risks identified. That means the higher the risk, the more measures the Company has to take to mitigate the risk. Where the risks are lower the Company may take simplified measures, provided that this is consistent with the country's assessment of its ML, FT and FP risks.

Applying a Risk-based Approach means that the Company shall:

- assess the risks that ML/FT/FP may occur within the Company beforehand;
- design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- monitor and improve the effective operation of these policies, procedures and controls;
- document the risk assessments, including everything that has been done and the reason for this being done.

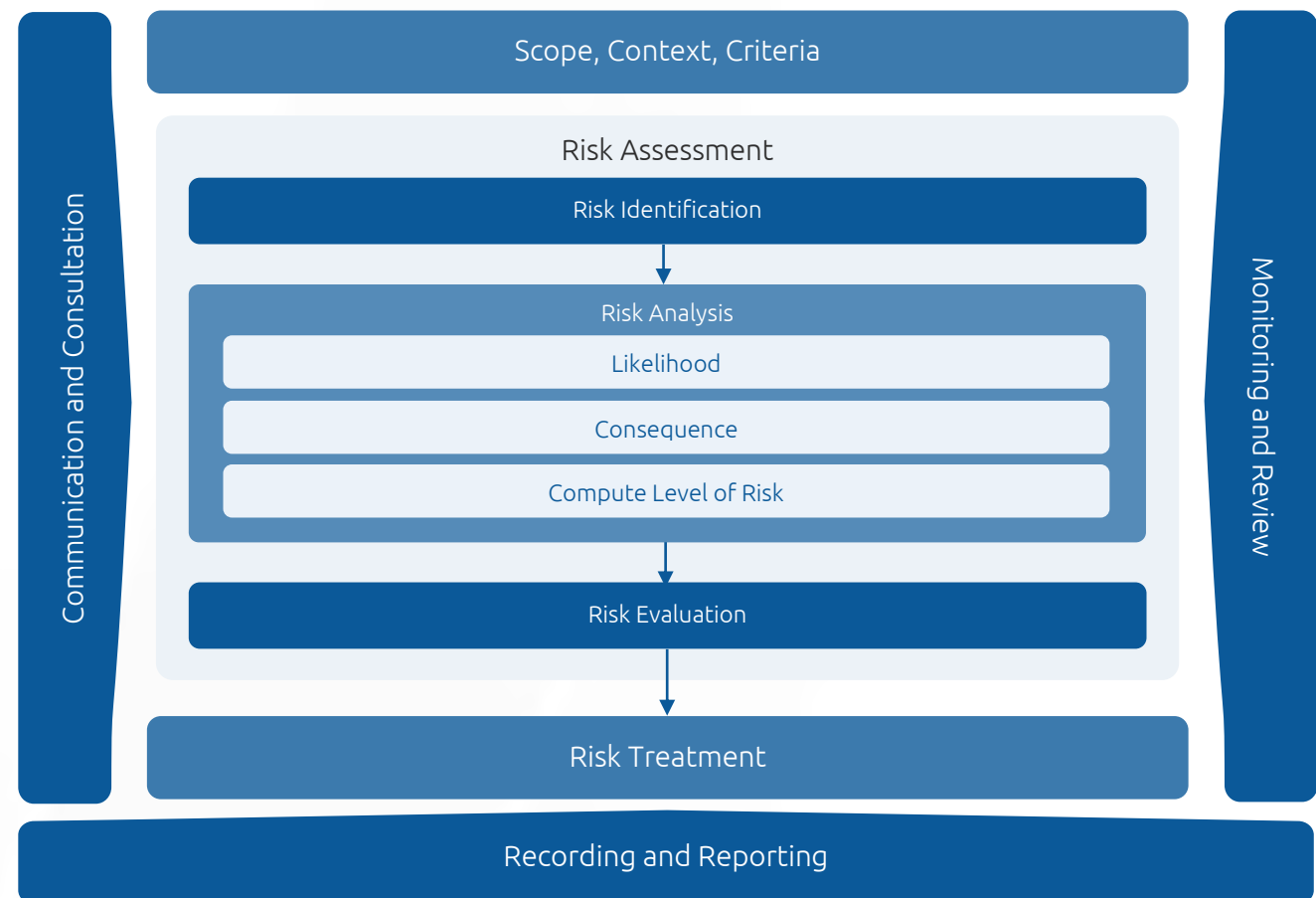
The Company document their policies, procedures and controls relative to their applied RBA. Since risks are dynamic, the Company must, on an on-going basis, monitor the effective operation of the policies, procedures and controls concerning their RBA and, when needed, make the necessary amendments to these policies, procedures and controls. The risk assessment should also be made available to the GCB upon request.

Risk Assessment

The Company prepares and regularly updates the risk assessment in order to identify, assess, analyze and manage ML, FT and FP 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. The risk assessment has to be documented and approved by the **board of directors** of the Company. It should also be made available to the GCB upon request.



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

- applicable regulatory requirements (Curaçao laws, decrees, etc.);
- last national risk assessment of the jurisdictions where they operate;
- 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/FT/FP risks of its customers by assigning an ML/FT/FP risk rating taking into consideration the risk categories as specified below.

Business Risk Assessment

The Company shall carry out a business risk assessment (hereinafter – BRA) to identify the ML/FT/FP risks the Company is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment should address the ways in which the Company's products and services could be used for ML, FT and FP and the extent of the risk that this will happen. All factors that may have an impact on the risks of ML, FT and FP must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors. Once the BRA has been conducted, the Company can set a risk appetite: it decides how much risk it is prepared to accept.

The Company shall revise their BRA whenever there are changes to the environment within which they are operating and within its business activities, such as the introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, the Company shall assess their business risk **at least annually**, to evaluate whether any changes thereto are necessary.

The aspects of the BRA should cover, including:

- the methodology adopted;
- the reasons for considering a risk factor as presenting a low, medium or high risk;
- the outcome of the BRA;
- any information sources used.

In order to work risk-based, it is also important that the Company continuously follows the latest reporting requirements regarding ML, FT and FP.

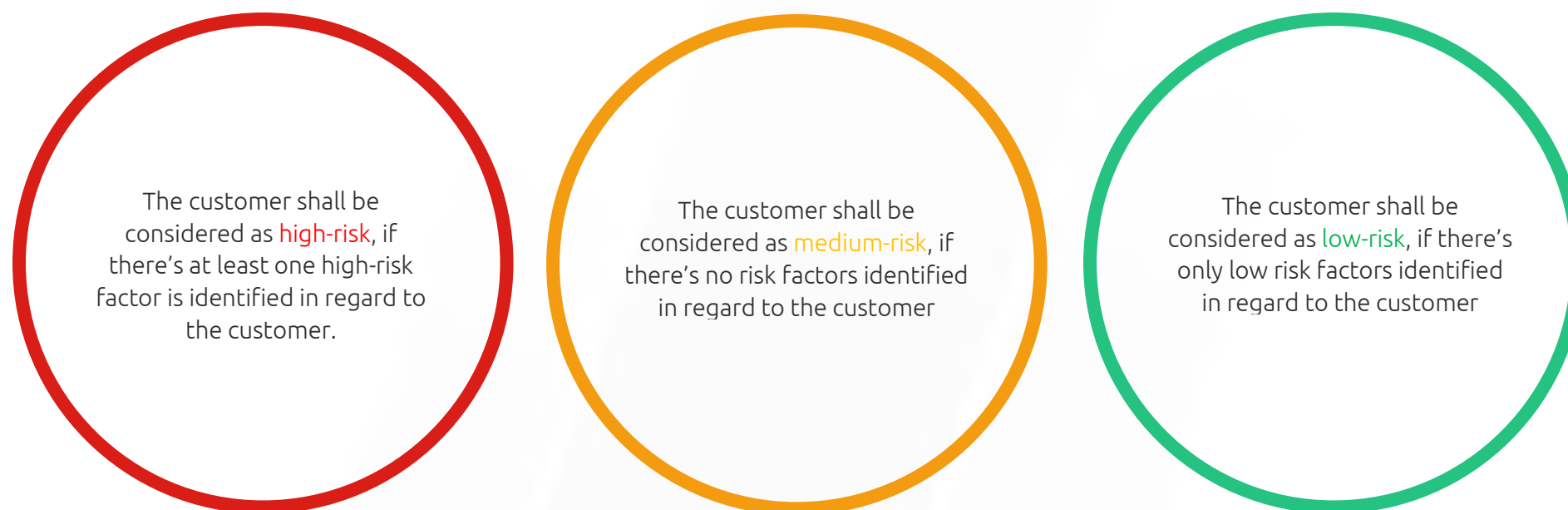
Customer Risk Assessment

The customer specific risk assessment (hereinafter – CRA) has to be carried out either **prior to the carrying out of an occasional transaction, or during establishing a business relationship**. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The CRA will assess the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied.

Determination of the customer's risk profile

The Company establishes and maintains the **list of risk factors** as a separate document (annex 3), which is used for the determination of the customer's risk profile.



The Company identifies risk factors in the course of CDD 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 that the risk profile determined is still applicable or should be modified based on any changes in the identity of the customer, the nature of the customer's economic activity, the customer's country of residence, the actual volume of transactions and other facts, which may affect the CRA. 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 will engage in annual reviews of each low-risk customer.

Medium Risk

The Compliance 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 Compliance Officer performs monthly reviews of every high-risk customer including a transactional review.

Each high-risk customer will require EDD before the conclusion of business relationship and additional facts will be gathered to learn more about the customer.

Non-acceptable customers

The Company has created a list of prohibited risk factors (annex 3) in the presence of which the customer will not meet the Company's risk appetite. In case, when such a risk factor has arisen in the course of the customer's onboarding or before making an occasional transaction – the Company refuses to establish a business relationship or perform a transaction with such a customer. If a 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.

The Company has to make an unusual transaction report to the FIU if the presumption of ML/FT/FP exists.

Anonymous accounts

The Company is prohibited from keeping anonymous accounts or accounts with obviously fictitious names. The Company must identify the customer and ask for the customer's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions.

Prohibited countries

Curaçao prohibits its own residents to access Curaçao-based online gaming operators. Additionally, the Company cannot accept customers from territories as determined by the GCB from time to time. There are countries that have treaties in place with Curaçao that include restrictions prohibiting persons from such countries to access to Curaçao-based online gaming operators.

Inability to complete CDD

Where unable to comply with the CDD requirements the Company must not open the account, commence business relations or perform the transaction. If the Company already has a business relationship with the customer the Company should terminate the business relationship.

Risk Factors Specific to the Gambling Sector

There are four risk areas that the BRA and CRA have to cover, these are:

Customer risk

Customer risk is the risk of ML/FT/FP that arises from maintaining relations with a given customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers' whose activities may indicate a higher risk include:

- customers who have multiple sources of income;
- customers with irregular income streams;
- PEPs;
- high spenders (money can be derived from illegal activities);
- disproportionate spenders (inconsistent with the Company's information about the customer's known source of income/assets);
- casual customers like locals/tourists, especially when spending pattern changes;
- improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- customers using multiple casino player rating accounts to hinder the Company to track their gambling activities;
- unknown customers (redeeming large amounts of chips);
- junkets (junket operators monitor customer activity and issues and collect credit).

The Company must set a value which represents the upper value of a typical customer's transactions.

The Company has a list of customer related factors that are considered as high risk and those that are considered low risk provided in the list of risk factors (annex 3).

Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the Company itself, the customer and the source of wealth of the business relationship. The nationality, residence and place of birth of the customer have to be taken into account as well as these might be indicative of a heightened geographical risk. It is advisable to take into account a variety of sources of information, including:

- countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- countries on the FATF list of Jurisdictions under Increased Monitoring;
- countries on the CFATF Public Statement;
- countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT/CFP regime;
- countries sanctioned by the OFAC;
- countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- countries on the Corruption Perception Index compiled by Transparency International.

The Company has a list of countries that are considered as high risk and those that are considered low risk provided in the list of risk factors (annex 3).

Product, service and transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by the Company of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- proceeds of crime – the risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from the employer;
- anonymous payment methods such as pre-paid cards and virtual assets;
- use of casino accounts – this should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play;
- types of specific games (e.g. roulette, craps → even bets);
- peer-to-peer gaming;
- the use by customer of accounts held or cards issued in the name of third parties;
- the transfer of funds from one gaming account to another;
- types of financial services (credit/marker, currency exchange, check cashing);
- multiple casino accounts or wallets (internet operator may own and control multiple websites);
- changes to financial institution accounts to fund casino account;
- identity fraud - details of stolen financial institution accounts or stolen identities used to successfully open financial institutions accounts and used on websites;
- using cash to fund a pre-paid card poses similar risks as cash;
- games involving multiple operators (poker on platforms shared by multiple operators);
- electronic wallets (e- wallets) - not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the casino. This may be useful for dishonest customers who wish to disguise their gambling.

The list of products or services and payment methods which are considered high risk is provided in the list of risk factors (annex 3).

Distribution channels risk

The channels through which the Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction, including:

- channels that Favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;

- non-face-to-face interactions - while situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the Company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- involvement of a third party in the interactions between the customer and the Company. This is especially the case where these third parties are not themselves subject to any form of AML/CFT/CFP obligations.

The Company has a list of risks related to delivery channels which are considered high risk provided in the list of risk factors (annex 3).

Technological developments risk assessment

The Company shall also maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of ML/FT/FP. The Company shall identify and assess the ML and T risks that may arise whenever:

- a new product is developed;
- a new business practice emerges;
- a new delivery mechanism becomes available;
- a new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented. Where risks are identified, measures must be taken to mitigate these risk

Customer Acceptance Policy

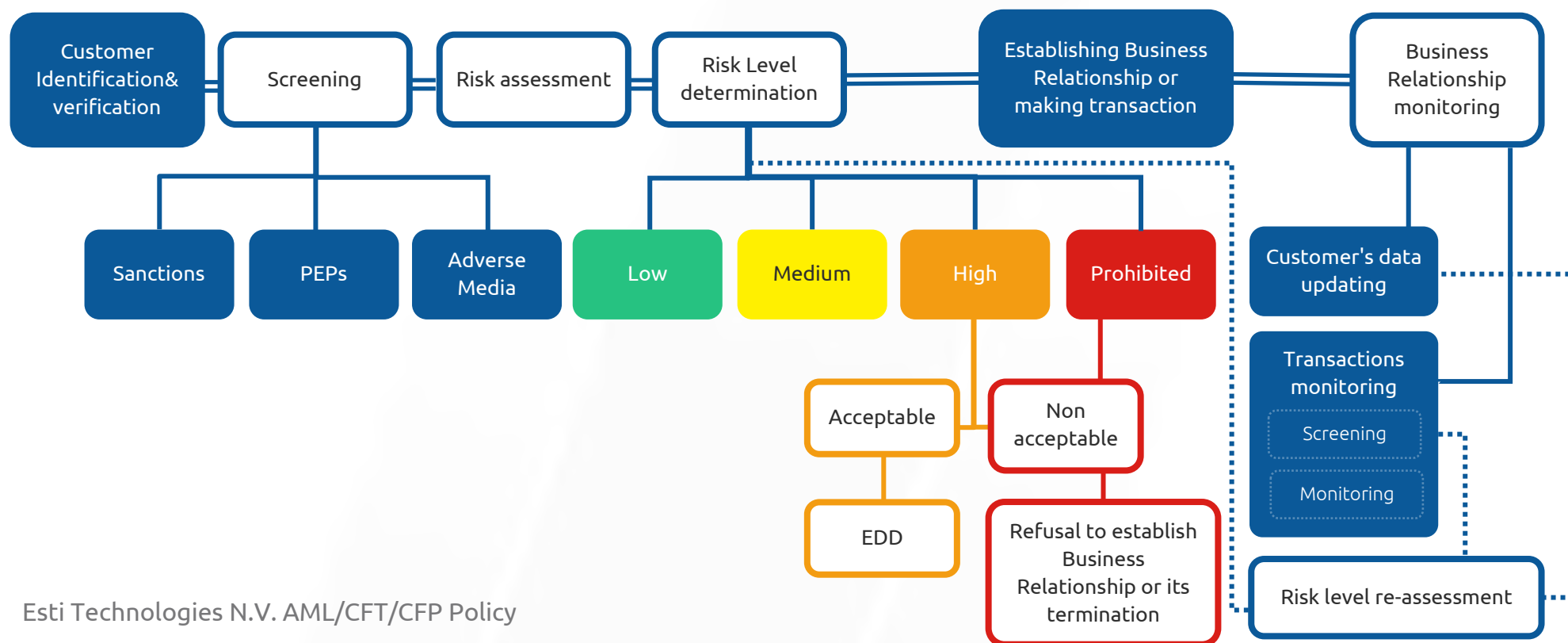
On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy.

Any unusual behavior needs to be reported to the FIU. If FIU, after proper analysis of an unusual transaction, concludes that there is a suspicion of ML and/or TF, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

Customer Due Diligence

Customer due diligence (CDD) is central to an effective AML/CFT/CFP 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 **CDD measures** to be taken are as follows:

1. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
2. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the Company is satisfied that it knows who the beneficial owner is.
3. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
4. Conducting ODD on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, its economic activity and risk profile, including, where necessary, the source of funds.

The Company has described its onboarding procedure within which the CDD measures are applied in its **Customers' Onboarding Procedure** (annex 4).

Timing of CDD Measures

The Company has the obligation to undertake CDD measures when:

- when the customer engages in financial transactions¹⁴ equal to or above NAF. 4,000;
- carrying out occasional transactions¹⁵ above the monetary equivalent of NAF. 4,000¹⁶;
- there is a suspicion of ML/FT/FP; or
- the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

¹⁴ Financial transactions are deposits and withdrawals (bonuses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

¹⁵ An occasional transaction refers to a transaction with a one-off customer, that at that point, is not expected to return. This applies typically to land-based casinos, where no opening of an account is required to play.

¹⁶ A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of NAF. 4,000.

All CDD measures must have been conducted at the time the NAF. 4,000 threshold is reached. The threshold is to be **calculated on a daily basis taking into account all deposits and withdrawals made by the customer since the establishment of the business relationship**, including any peer-to-peer transfers. In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the NAF. 4,000 threshold is reached because of a customer's deposit, the customer shall be prohibited from depositing funds into the account or withdrawing funds from the account. The Customer may still be allowed to play, using the funds already in his account. However, if the NAF. 4,000 threshold is reached because the customer wants to withdraw his money, a **complete freezing of the account** should occur. In this case it will not be possible for the customer to continue playing.

If the requested information and documentation is not received **within 30 days from the moment the NAF. 4,000 threshold was reached**, the Company has to **terminate the relationship** with the customer and **report the transaction to the FIU if the presumption of ML/FT/FP exists**. If no presumption ML/FT/FP exists, the **funds should be transferred to the same bank account or wallet it was deposited from**. If the presumption of ML/FT/FP exists the funds shall be blocked if required by the Company's internal procedures. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.

Minimum level of CDD measures

The Company is required to apply a **minimum level of CDD measures** prior to reaching the NAF. 4,000 thresholds. Thus, simultaneously with the opening of an account, the Company must identify the customer by collecting the minimum personal details, including:

1. name and surname;
2. permanent residential address; and
3. date of birth.

The Company must also conduct the PEP status and sanctions screening simultaneously with the opening of an account.

Identification and verification of the customer

Identification refers to the collection of personal details of the customer to establish the identity of the customer. Verification of identity refers to actions taken to verify that the customer exists and is who the customer claims to be. Verification consists of confirming the information collected for identification purposes using reliable, independent source documents, data or information. The personal information required and the extent of verification to be carried out will vary depending on risk¹⁷.

When identifying the customer, at a minimum the following information must be collected:

- full name;
- permanent residential address;
- date of birth;
- place of birth;
- nationality; and
- identity number.

The Company shall carry out a CRA in order to have sufficient information available to detect unusual activity in the course of the business relationship. A provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered, or additional information is received. On the basis of the CRA, the proper level of CDD can be applied.

Verification of identity is carried out by making reference to an **unexpired government-issued document containing photographic evidence of the customer's identity** (e.g. passport, identity card), including:

- driver's license;
- identification card;

¹⁷ If the player is required to open an account for playing demo games and that account can be used for paid games as well, the casino needs to collect the personal information of the player at this stage.

- travel document or passport.

Where such a document does not allow the verification of the customer's residential address, the Company obtains an another document **not older than 6 months**, to verify the residential address, including:

- bank statement;
- utility bill¹⁸;
- correspondence from a central or local government authority, department or agency;
- rental or lease agreement.

Other verification methods which may be applied by the Company include:

- contacting the customer by letter, e-mail or telephone to verify the information supplied;
- sending a verification code to the e-mail address to verify that the address is current and genuine;
- checking social media, telephone directories, companies' registries or media and news sources;
- Biometric checks to confirm that the individual providing the document is the one described therein;
- cross referencing the information in the Company's possession with geo-location information, IP address data, funding method data etc.

Verification is carried out for the Company to determine to its own satisfaction that the customer is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is **authentic, clear, legible, legitimate, of good quality and that it has not been stolen from the true owner**. If the Company obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

If the customer is **not physically present** for identification, the identification and verification shall be carried out taking into account the specific risks associated with business relationships or transactions without personal contact.

¹⁸ For phone bills, only fixed line telephone bills are accepted as proof of address.

Where the Company does not have sufficient comfort that it knows its customer, the Company shall take additional measures to do so. Some of these measures include requesting additional identification documents, asking the customer to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

Identification and verification of the Beneficial Owner

The Company shall make sure that customers are registering an account to play and transact on his/her own behalf. For this purpose, the Company **includes a specific wording in the terms and conditions** that the customer must explicitly accept, together with a **declaration in the form of a tick box that the customer is registering to play on his/her own behalf**. The Company has to ensure that its ongoing procedures allow for the detection of possible instances where the customer is actually playing on behalf of third parties.

In an instance where funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons are considered as beneficial owners and the Company has to identify them and verify their identity.

Obtaining information on the Purpose and Intended Nature of the Business Relationship

The Company should understand why a prospective customer is seeking to acquire a specific service or product from the Company. Within the context of the gambling sector, the purpose behind the opening of a gaming account is quite self-evident for which it is not required to obtain any additional information from the customers. However, this CDD measure also requires the development of a customer risk profile to have sufficient information available to allow the detection of unusual activity in the course of a business relationship.

To this end, the Company has to collect sufficient information and, where it is necessary, documentation to establish a customer's **source of wealth and the expected level of activity**. As to the extent of the information that the Company is to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment. Where the risk is not high, a **declaration from the customer with some details** (e.g. nature of employment/business, usual annual salary etc.) can be sufficient. **Social media** can also be used as a source of information. Where the risk of ML/FT is higher or the Company has doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation.

In developing a customer risk profile, the Company may also consider using statistical data to develop behavioral models against which to eventually gauge a customer's activity rather than collect the source of wealth information¹⁹. It is important to note that the use of statistical data is incompatible with high-risk situations as the transactional pattern will deviate from the average behavioral model. In such circumstances, the Company would have to collect the source of wealth information as set out above.

Politically Exposed Persons identification

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are:

- Heads of State or of government;
- senior politicians;
- senior government;
- judicial or military officials;
- senior executives of state-owned corporations;
- important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions. Examples are:

- Heads of State or of government;
- senior politicians;
- senior government;
- judicial or military officials;

¹⁹ Where the Company opts to adopt this approach, it can use data collected from a relevant central statistics department, such as average national income, average disposable income etc. These indicators should allow the Company to determine the average wagering power of customers from a given jurisdiction. The Company can also use data collected over a period of time by the Company itself, which allows to create the profile of an average customer. It is important to note that the reference is not to the statistical data on the individual customer but

to statistical data obtained from a range of customers. The Company should therefore only use this specific alternative where their customer-base is wide enough to allow the creation of an average profile. New casinos would therefore not be expected to use this method unless they are able to obtain gaming data from another casino offering the same games within the same markets and having a similar business model to the one being adopted by the new casino.

- senior executives of state-owned corporations;
- important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The Company shall take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. **Screening for PEP status** has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the Company must regularly screen for PEP status during the business relationship. For PEP status screening the Company relies on internet search and/or consults the relevant reports and databases.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Reliance on Third Parties and Outsourcing

The Company may rely on third parties when performing elements 1.-3. of the CDD measures in the chapter “Customer Due Diligence” above, provided that the criteria set out below are met. The third party should be subject to CDD and record-keeping requirements. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the Company. Where such reliance is permitted, the ultimate responsibilities for CDD measures remain with the Company.

The criteria for the third party to be met are as follows:

- The Company has to obtain the information concerning elements 1.-3. of the CDD measures immediately from the third party it is relying upon.
- The Company should have an agreement with the third party being relied upon that copies of identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. The Company, however, remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting ODD.

- The Company should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements as described in this regulation. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform CDD measures.
- When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

It must be noted that the situation is different for the outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the Company, in accordance with its procedures, and is subject to the Company's control of the effective implementation of those procedures by the outsourced entity. It is important that the Company is aware that it will remain responsible at all times for compliance with said regulations. For this reason there should be periodical assessments of how the outsourced entity is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively. However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

Any activity performed by an agent or group company is to be considered as an activity performed by the Company. As such, any customer on-boarded by the agent or group company has to undergo the same checks and controls as customers on-boarded by the Company itself. It is therefore up to the Company to ensure that its AML/CFT/CFP controls, policies, measures and procedures are applied by the agent or group company.

Simplified Due Diligence

Where the risks of ML/FT/FP are lower, the Company may conduct SDD, which should take into account the nature of the lower risk.

In low-risk scenarios the Company may limit identification to the following information:

1. full name;
2. permanent residential address;
3. date of birth;

Examples of other possible measures:

- verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- adapting verification to perceived risk. The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the customer's identity (e.g. birth certificates, bank statements etc.);
- limiting the extent of personal details to be verified. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is the discretion of the Company, as long as it has sufficient comfort that it knows who its customer is;
- reducing the frequency of customer identification updates;
- reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

SDD measures are not acceptable whenever there is suspicion of ML/FT/FP, or where specific higher-risk scenarios apply.

Enhanced Due Diligence

In circumstances where the risk of ML/FT/FP is higher, EDD measures have to be taken to mitigate the increased risk. The EDD measures should be consistent with the risks identified. In particular, the Company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual.

High risk circumstances refer, among other things to:

- residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);
- products or transactions that might favor anonymity;
- new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Examples of EDD measures include:

- obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds or source of wealth of the customer.
 - in situations presenting a higher risk of ML/FT/FP, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer;
- obtaining information on the reasons for intended or performed transactions;
- obtaining the approval of senior management to commence or continue the business relationship;
- conducting enhanced ODD;
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Politically Exposed Persons

The Company is required, in relation to foreign PEPs, (whether as a customer or beneficial owner) in addition to performing normal customer due diligence measures, to:

1. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;
2. obtain senior management²⁰ approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship with existing customers or for conducting the occasional transaction);
3. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the customer's spending pattern matches his legal source of funds. The Company requests a statement from the customer about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be

²⁰ senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be from the manager of the Compliance department

public sources. When public sources cannot, or can insufficiently verify the received information, the Company can request the customer to provide additional documents; and

4. conduct enhanced ongoing monitoring of the business relationship.

Although EDD is required for each PEP, the measures do not have to be the same for every PEP. In cases of a higher risk business relationship with such persons, the Company is required to apply the measures referred to in points 2.-4. above. Should a customer who had not been identified as a PEP at the on-boarding stage result to have become one, the Company is required to implement the measures described above within the **30-day window**. If the measures cannot be successfully applied within the specified time period, the Company shall terminate the relationship with this customer.

The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

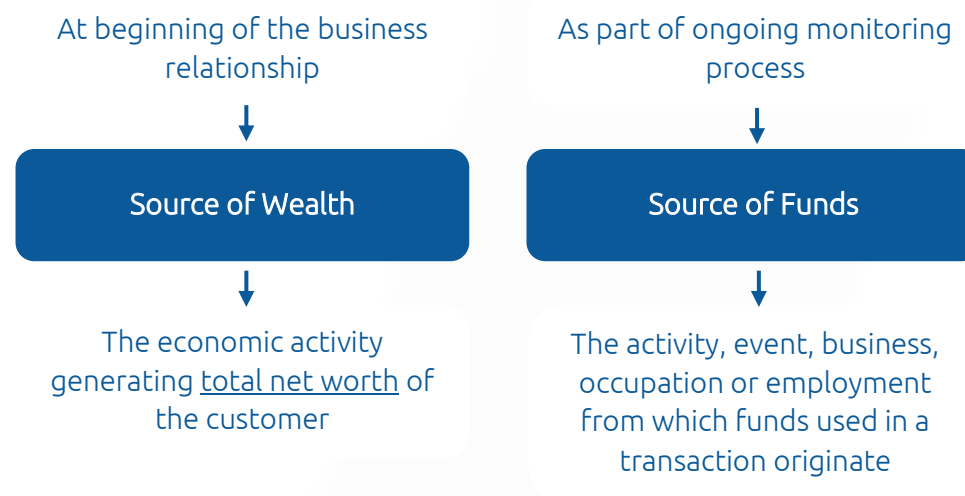
Source of Wealth and Funds

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 the 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 the 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 the expected turnover specified by the customer.

Source of Funds refers to the origin of funds being deposited, received, or transferred with the Company. SoF tells where the assets are coming from, which can be proven through bank statements, tax returns or the customer's financials, etc. Typically, SoW is requested when establishing a business relationship or performing EDD, and 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 pay slips or wage slips 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;
- a copy of a will;
- sales and purchase agreements.

Ongoing Due Diligence

The Company must conduct ODD of business relationships and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's economic activity and risk profile.

Ongoing monitoring of identity

In conducting ODD on the business relationship the Company has to:

- Ensure that documents, data and information collected under the CDD measures are kept up-to-date and relevant
 - obtain fresh documents when the expiry date of identification documents held on file is reached;
 - question the data and information already in its possession whenever any inconsistencies arise;
 - obtain evidence of identity periodically to detect any changes;
 - refresh the data on key events (i.e. change of payment instrument).

The Company should determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions

Transaction monitoring is executed to prevent the involvement of the Company with ML/FT/FP and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions the Company notices that the customer's transactions are not consistent with what it knows or expects from the customer, the Company has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. The reason for deviation may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date. The Company has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving the additional information the Company has to decide whether the transaction is an unusual transaction and needs to be reported to the FIU.

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. FIU, FATF, CFATF).

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 a 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/FT/FP risk involved, and the nature of the business relationship are fully understood by the Company. Ongoing monitoring procedures take into 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/FT/FP 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 are 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.

Refusal or Termination of the Business Relationship

In case the obligations arising from the CDD application cannot be met, the Company cannot establish the business relation or perform the transaction or is obliged to terminate the business relationship with the customer. **The Company must keep a record of all the attempts made to get the necessary information and documentation.** To this end, the Company may decide to either close the account or to keep it blocked and suspended in its entirety. In the event that the customer makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the account, the Company has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The Company is to consider whether there are any grounds giving rise to suspicion of ML/FT/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/FT/FP. The Company should consider all factors and information it has at its disposal to

decide whether there are grounds to suspect ML/FT. **If however the presumption of ML/FT exists, the Company should submit an unusual transaction report to the FIU with regard to this customer.** Where there is no reason for the retention of funds, the funds are to be remitted back to the customer. This has to be done through the same channels used to receive the funds.

Targeted Financial Sanctions

The Company takes measures to ensure compliance with the relevant regulations and legislation on sanctions in Curaçao. The Company takes into account at least the following sanction regimes:

- United Nations Security Council resolutions²¹;
- Common Foreign and Security Policy of the European Union²².

The Company shall monitor for amendments in Sanctions Decrees and Regulations on a regular basis, at least via the GCB website²³, and update their CDD- and AML/CFT/CFP policies and procedures accordingly to reflect such amendments.

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

Procedure for identifying the subject of sanctions and a transaction violating sanctions

All customers should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Company should also take that local list into account. The Company must ensure it does not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a customer, the Company should check published lists of known or suspected terrorists or other sanctioned persons or companies.

²¹ <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

²² <https://www.sanctionsmap.eu/#/main>

²³ <https://www.gamingcontrolcuracao.org/notifications>

A mechanism must exist to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from an account that should be frozen.

Actions when identifying the sanctions subject or a transaction violating sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. The Company is required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities taking into account the **process for the freezing of resources**²⁴.

In case the Company must apply a targeted financial sanction, **a report must be filed with the Curaçao FIU**.

Reporting Obligations

Recognition of Unusual Transactions

An unusual transaction is a transaction inconsistent with the customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the customer. The purpose of collecting information is to provide the Company with documentation to assess the risk that may be associated with the customer and to build a customer profile to assess how the customer is going to act within the framework of the business relationship.

The Company must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions shall be deemed unusual:

²⁴ https://cbcs.spin-cdn.com/media/legislation_guidelines/20190120_process_for_the_freezing_of_resources_for_the_implementation_of.pdf

Objective indicators

The Company shall consider the following objective indicators:

- transactions which in connection with ML/FT/FP are reported to the Police or to the Department of Justice;
- transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- transactions in the amount of **NAf. 5,000 or more**, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000. This includes but is not limited to:
 - a cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the customer;
 - accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the customer;
 - sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits;
 - a cash out in the amount of NAf. 5,000 or more.

Subjective indicators

The Company shall consider the following subjective indicators:

- transactions where there is cause to presume that they can be related to ML/FT/FP. Examples of situations that may be possibly related to ML/FT/FP include:
 - setting up dozens of betting accounts, with deposits well below the reporting threshold to withdraw the money after a short while;
 - regularly depositing or transacting similar amounts of cash;
 - funding the account with credit and debit cards, prepaid cards, checks and cryptocurrency and then asking for a pay out;
 - unexplained income inconsistent with the financial situation/customer profile;
 - customers claiming machine credits/payouts with no jackpot;
 - association with multiple accounts under multiple names;

- frequent betting transactions just under threshold;
- cash deposits/withdrawals just under threshold;
- parallel even money betting;
- betting against associates/intentional losses, where money launderers deliberately lose to one of the party who is able to receive a casino issued check or wire transfer of legitimate winnings (poker, roulette);
- multiple currency exchanges;
- currency exchange for no reasonable purpose;
- currency exchanges with low denomination bills for high denomination bills;
- currency exchanges with little or no gambling activity;
- wire transfers/currency exchanges just under thresholds;
- frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa.

Internal Reporting of Unusual Transactions

All unusual individual transactions or series of transactions must be reported internally to the Compliance Officer by filling the approved **internal report in the form** (annex 5), **without any delay** but not later than the time periods specified in this section. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements.

The Company must report unusual transaction or any intended unusual transaction through the Compliance Officer to the FIU **without delay** but not later than the time periods specified in this section.

Reports of **objective indicators** must be submitted within **48 hours of the transaction taking place**.

Reports of **subjective indicators**:

- Internal reporting to the Compliance Officer is to be submitted within **24 hours of the transaction taking place**.
- The Compliance Officer has **10 working days** to complete relevant research.
- If the presumption of ML/FT/FP exists, the compliance officer shall submit the report **within 48 hours** to the FIU.

A report shall contain, as far as possible, the following information:

- the identity of the customer;
- the nature and number of the client's identity document;
- the nature, time and place of the transaction;
- the size, destination and origin of the funds, securities, precious metals or other assets involved in the transaction;
- the circumstances on the basis of which the transaction is considered unusual.

External Reporting of Unusual Transactions

The Compliance Officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company shall report to the FIU the details of the transactions by means of the **goAML reporting portal**²⁵²⁶. The reports and the submission of the thereto related information (all supporting documents) should be done in **English**. If internally reported transactions are not reported to the FIU, the reason shall be adequately documented and signed off by the Compliance Officer and/or senior management.

The Company and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

Blocking/freezing accounts

The Company shall block/freeze the customer's account as a result of sending an unusual transaction report when:

- transactions which in connection with ML/FT/FP are reported to the Police or to the Department of Justice;
- transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

²⁵ https://portal.fiucuracao.cw/goAMLWeb_PRD/Home

²⁶ The FIU allows bulk reporting, therefore the casino account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

- transactions where there is cause to presume that they can be related to ML/FT/FP.

The Compliance Officer shall assess the risk of tipping off accompanying the blocking/freezing of the customer's account. In case there is a suspected risk of tipping off the customer caused by the blocking/freezing of the account, the Company shall not block/freeze the account. In such case, the Company shall also monitor the account in an enhanced manner and report any unusual activity to the Compliance Officer who shall re-assess the requirement to block/freeze the account for each such report. Clear documentation should support the decision to refrain from blocking/freezing the account and the enhanced monitoring procedures that will follow.

Tipping Off

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. They are not permitted to disclose information to the customer nor to third parties. The reason for this is not to jeopardize an analysis or investigation into ML/FT/FP.

Caution is advised when the Company takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the customer. In such circumstances, it would be more advisable to increase ongoing monitoring and submit additional reports to the FIU on any other suspected instances of ML/FT/FP.

If there is a suspicion that transactions relate to ML/FT/FP, the Company should take into account the risk of tipping off when performing the CDD measures. If the casino reasonably believes that performing the CDD process will tip off the player, the Company may choose not to pursue that process, and should file a report to the FIU.

Record keeping

The Company shall record the following data in such a way that it is accessible:

- the name, address and domicile or place of business of the customer and, if any, the ultimate beneficial owner and of the person in whose name the deposit or account is made, of the person who will have access to the safe deposit box or the person in whose name a payment or transaction is made, as well as their representatives;
- the nature, number, date and place of issue of the document by means of which the identity was established;
- the nature of the service; and
- the nature, origin, destination, extent and other unique characteristics of the values or items concerned in a transaction.

The Company shall maintain, the **data referred to above as well as all other relevant data relating to both domestic and international transactions** for at least **5 years after the execution of the transactions** in question, in such a way that those data are retrievable and the transactions in question can be reconstructed for a period of **5 years** to enable them to comply with information requests from the competent authorities.

The Compliance Officer shall adequately document unusual transactions. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The FIU or staff of the FIU to be designated by the FIU, may, in the case of a transaction that has been reported to the authorities, charged with the investigation and prosecution of criminal offences, issue an instruction to set the retention period at **10 years**. Acting contrary to such instruction is prohibited.

The Company shall keep **data and documents obtained through the CDD measures application**, including the risk profile of the customer, contact information and the copies or registers of official identity documents and passports, identity cards, driving licenses or similar documents, account statements and business correspondence, in an accessible manner **for at least 5 years after the termination of the business relationship**.

The data and information obtained from the CDD and transaction files shall be made available without delay to the competent authorities and the authorities that are authorized to inspect or obtain this information on the basis of the NOIS.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

Training and Screening of Employees

The Company shall screen their employees for criminal records before the conclusion of the employment contract.

The Company shall develop training programs and provide training to its employees. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Company's AML/CFT/CFP systems and procedures. Most areas of the Company should receive training, and the target audience should include most employees. However, each segment should be trained on topics and issues that are relevant to them. Training must at least address the following topics in regard to different types of employees:

For new KYC Agents (i.e. employees who will handle customers or their transactions), irrespective of their level of seniority:

- the nature and process of ML, FT and FP;
- the Company's existing internal policies, procedures concerning ML, FT and FP;
- regulations concerning ML, FT and FP;
- the reporting requirements;
 - the need to report any unusual transactions to the appropriate designated officer;
 - objective and subjective indicators for reporting unusual transactions;
- ML methods and trends in the gambling sector;
- explanation on CDD.

For audit staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and enforcement, and their impact on the Company.

For Compliance Department staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company and how the Company manages the arising risks.

This will require attending conferences or AML-specific presentations to go into greater detail.

For supervisors and managers:

- a higher-level instruction of the Company's existing internal policies, procedures concerning ML, FT and PF;
- a higher-level instruction of the regulations concerning ML, FT and PF.

For senior management and the board of directors:

- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company.

The training held is to be documented and confirmed with the employees' signatures on the **training protocol** (annex 6). This protocol should include:

- details on the content of the training programs;
- the names of the staff members who have received the training;
- the date on which the training was provided;

To demonstrate compliance with the abovementioned training guidelines, the Company shall also maintain records that include:

- the results of any testing carried out to measure staff understanding of ML, FT and FP requirements; and
- an ongoing training plan.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding ML, FT and FP techniques, methods and trends.

Independent Audit of the AML/CFT/CFP Policy

The AML/CFT/CFP Policy must be monitored and evaluated **at least annually** by an adequately resourced internal audit department or an outside independent party (hereinafter – Internal Auditor). The audit must be independent, thus performed by an Internal Auditor not involved with the organization's AML compliance staff (incl. the KYC Agents and the Compliance Department). Internal Auditor performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. These tests must include at least:

- an evaluation of the institution's AML, CFT and CFP manuals;
- customer's file review;
- compliance management;
- performance of transaction testing;
- assessment of training adequacy;
- assessment of compliance with applicable laws and regulations;
- evaluation of the system's ability to identify unusual activity;
- interviews with employees who handle transactions and with their supervisors;
- a sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- an assessment of the adequacy of the record retention system.

The Internal Auditor should also consider whether the Company's senior management and board of directors were responsive to earlier audit findings.

The scope of the testing and the testing results must be documented within the **internal audit report form** (annex 7), with any deficiencies reported to senior management and/or the board of directors, and to the designated officers with a request to take prompt corrective actions by a certain

deadline. These corrective actions could also include the enhancement of controls and procedures. 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 have been performed;
- results of the 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 the period of exercising the internal control;
- measures that are required to implement for elimination of determined deficiencies;
- general conclusions from the exercised internal control.

The senior management and/or the board of directors 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 a format which can be reproduced in writing. For this reason, the senior management and/or the board of directors is obliged to:

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

Examination by the Gaming Control Board

The Company shall provide information or documentation on their ML, FT and FP and deterrence and detection procedures to the examiners of the GCB in preparation for or during an examination and upon GCB request during the year. The Company shall make the following items readily available:

- its written and approved AML/CFT/CFP Policy on ML, FT and FP;
- records of its Business Risk assessment;

- the name of each Compliance Officer responsible for the Company's overall ML, FT and FP policies and procedures and his/her designated job description;
- records of reported unusual transactions;
- records of unusual transactions which required closer investigations;
- records of frozen accounts;
- schedule of the training provided to the Company's personnel regarding ML, FT and FP;
- the assessment report on the Company's policies and procedures on ML, FT and FP by the internal audit department or an external auditor;
- the customer's files including customer risk assessment, CDD, customer acceptance and transaction information.