

The Prevention of Money Laundering and Funding of Terrorism
Policies and Procedures Manual

May 2025

Version	Date	Approved CO	Approved MD
1.1	May 27, 2026	Yes	Yes

Preface

These policies and procedures have been approved by the Company and are considered to be binding upon such and also upon any persons engaged by the same. These policies and procedures are subject to periodic review in view of continuous developments in the industry, in an effort to maintain the policy of best practice. In fact, this AML Policies and Procedures Manual should be seen as a '*working document*', which is amended from time to time.

It is to be noted that the Company shall refer to the Laws of Curacao, guidelines issued by the Financial Intelligence Unit in Curacao, AML best practices and European directives and regulations whilst applying the principles and procedures contained herein.

The objective of this document is to establish and maintain policies, procedures and controls, which deter criminals from using our lawful facilities for money laundering and the funding of terrorism.

This document is for internal use only.

Abbreviations

CDD- Customer Due Diligence

EDD – Enhanced Customer Due Diligence

ID - Identity

FATF – Financial Action Task Force

FIU- Financial Intelligence Unit

M&As- Memorandum & Articles of Association

ML/FT- Money Laundering/Funding of Terrorism

MLRO- Money Laundering reporting Officer

PMLFTR – Prevention of Money Laundering and Funding of Terrorism Regulations

SDD – Simplified Customer Due Diligence

STR – Suspicious Transaction Report

Definitions:

For the purposes of the provisions of this manual:

“Player” means the natural or legal person, who can be acting either as principal or as agent, with whom deal with whom the Company deals, when embarking on a business relationship or occasional transaction;

“Funding of Terrorism” shall have the meaning ascribed to it under European Directives (AMLDs) and may be described generally as “the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism”;

“Money Laundering” shall have the meaning ascribed to it under Curacao Law and European Directives (AMLDs), and may be described generally as “the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds”

“PEP” (Politically Exposed Person) means a natural person who is or has been entrusted with prominent public functions and for a period of 12 months thereafter, including:

- (i) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
- (ii) Members of Parliament;
- (iii) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- (iv) Members of courts of auditors, Audit Committees or of the boards of central banks;
- (v) Ambassadors, charges d'affairs and other high ranking officers in the armed forces;
- (vi) Members of the administrative, management or boards of State-owned corporations;

and the immediate family members or persons known to be close associates of such persons;

“Reputable Jurisdiction” means any country having appropriate legislative measures for the prevention of money laundering and the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith;

“Regulations” means the applicable anti money laundering and funding of terrorism regulations currently in force in Curacao, any issued AML guidelines and any European Directive applicable to the prevention of Money Laundering and Funding of Terrorism.

“Source of funds” means the activity, event, business, occupation or employment from which the funds used in a particular transaction are generated.

“Source of wealth” means the economic activity which generates the total net worth of the customer.

The Company means Velorum Corporation N.V., a company registered in Curacao, licensed and operating in the field of remote gaming.

Scope:

This manual seeks to implement the provisions of the Regulations which require the Company (as a “subject person” in terms of the Regulations) to take appropriate measures to make employees aware of:

- Customer due diligence, record-keeping and internal reporting measures required to be applied and maintained by the Company;
- Policies and procedures, including internal control, risk assessment and management and communications, which are aimed at preventing the carrying out of operations that may be related to money laundering or the funding of terrorism; and
- The provisions of the Regulations.

Chapter 1: Policy document

ANTI-MONEY LAUNDERING POLICIES FOR THE COMPANY

1.1. Compliance statement

It is the policy of the Company to comply in all respects with any applicable AML legislation by ensuring that policies and procedures aid the compliance function.

1.2. Policy on money laundering

The Company is committed to following the requirements of the money laundering legislation and supporting authoritative guidance issued by relevant regulatory authorities. It is committed to promoting a culture of compliance throughout the organisation and practice. The Company confirms that the policy is:

- to ensure that prevention of money laundering is addressed appropriately in all player transactions.
- to ensure that commercial considerations never override the need to comply with the Regulations;
- to ensure sufficient resources are devoted to the development, documentation and training necessary to ensure compliance; and
- to ensure that, where necessary, they appoint, a suitable Money Laundering Reporting Officer to monitor compliance.

The current Compliance Officer also responsible for AML is Michael Muscat.

1.3. Policy and procedure on due diligence

It is the policy of the Company to undertake a risk assessment (using the due diligence measures) and ensure that evidence of identity is obtained and retained as appropriate to that risk assessment for all players. This evidence will be obtained on a risk-based approach.

- Due diligence is undertaken on all players at different stages of the relationship depending on the risk profile of the Player.
- Knowledge of the player's identity is always requested prior to opening an account.
- Knowledge of the player's profile is gathered during the business relationship, on an ongoing basis, enabling the Company to establish a risk-profile, and manage such with regards to each player.

- Verification is carried out upon the player account reaching XCG 4,000 /Eur 2,000.
- Further KYC is obtained at withdrawal.
- Source of Funds is carried out on a risk-based approach.
- Source of wealth is carried out on a risk-based approach.

Player gambling patterns and deposit patterns are continuously monitored by our platform technology.

1.4. Policy and procedure on reporting

It is the policy of The Company to report all suspicions identified by the Compliance Officer/MLRO or by any other practitioner appointed on behalf of The Company to the FIU and the gambling regulator.

Deposits, Withdrawals over EUR 2,500/ XCG5,000 are flagged. These could be multiple transactions on an aggregated basis.

All assistants, whenever and wherever appointed, will report suspicions to the Compliance Officer/ MLRO as soon as the suspicion arises. The report will be made using internal reporting tools. This report will not be discussed with anyone apart from the Lawyers and the Compliance Officer/ MLRO and at no stage must the player or third parties be given any details of the report, without the specific agreement of the Compliance Officer/ MLRO.

On receipt of the report, the Compliance Officer/MLRO will consider the contents, request further information where required and determine what action should be taken. His decision will be recorded on the internal reporting tool and then where necessary a report will be submitted to the FIU.

At this stage the Compliance Officer/MLRO will inform the Lawyer and/or assistant of The Company and/or player relationship manager in charge, if any, of any action that he needs to take (for example, blocking balances, ceasing to take bets.).

The Company shall never carry out a transaction that is suspected or known to be related to ML/FT. Upon customers' requests for such transaction, the employee shall inform the Compliance Officer/MLRO immediately.

When an assistant or appointee of The Company has suspicions that ML/FT is occurring, all assistants or appointees, are prohibited from disclosing to the person under investigation or to third parties, that an investigation is being carried out, may

be carried out, or that information has been or may be transmitted to FIU. Disclosure of such information would give rise to the offence of tipping off and may prejudice an investigation.

Suspicious should not be discussed with anyone other than the MLRO.

The Company, must however still retain the necessary contact with a customer and should enquire, in a tactful manner, about any transaction which is not consistent with the customer's normal pattern of activity.

1.5. Policy and procedure on record keeping

It is the intention and an inherent policy of The Company to maintain records of identification and consideration of money laundering issues for the entire relationship and for at least five years thereafter.

The customer due diligence measures will be completed for all customers and updated at appropriate times. These measures, along with supporting documentation, will be filed in the corporate file of the respective customer.

At the end of the relationship, this information will be archived in the archive file with a date logged.

1.6. Policy and procedure on third party reliance

It is the policy of The Company not to rely on third parties for due diligence purposes.

1.7. Policy and procedure on internal control

It is the policy of The Company to facilitate adequate internal control to allow for compliance with the Regulations and other appropriate legislation.

As set above, The Company's Compliance Officer/MLRO will be given authority to implement the necessary changes in these procedures to ensure compliance. All assistants or appointees will be required to accept the changes necessary and service/partnership agreement, where applicable, that confer the necessary authority on the Compliance Officer/MLRO. Moreover, all assistants and appointees will be required to make the necessary internal reports using our internal reporting tool when they have a suspicion in respect of a player.

1.8. Policy and procedure on risk assessment and management

It is the policy of The Company to undertake AML risk assessments for players and retain the same on file for a period of 5 years.

1.9. Policy and procedure on compliance management

It is the policy of The Company to undertake a regular compliance review to ensure that the requirements of the Regulations are being followed. Compliance Audits will also be carried out.

1.10. Policy and procedure on communication

It is the policy of The Company to ensure that all assistants and appointees have access to adequate training to ensure that they have the necessary knowledge of the Regulations and of these policies and procedures.

All assistants will be required to undertake an update course on anti-money laundering procedures and compliance, at least once every two (2) years. This should be provided by a reputable educational institution or institution of practitioners such as Society Education, ACAMS, and/or the FIU and/or the 'Big Four' audit firms.

1.11. Other policies and procedures

Where players do not provide sufficient documentation to render compliance herewith, the Company shall not provide services to such players.

Moreover, any document which is in a language not understood by The Company should be translated in English. The translation should be signed, dated and certified by an independent person of proven competence, confirming that it is faithful translation of the original.

Chapter 2: Customer Due Diligence Measures

The Company must apply and maintain, **in all cases**, customer due diligence measures when forming a relationship or carrying out an occasional transaction. Enhanced Customer Due Diligence **must be applied** when the risk assessment of a relationship and/or an occasional transaction is considered as 'High-Risk'.

2.1. Purpose of Customer Due Diligence Measures:

These measures will assist The Company in:

- Determining if the player poses a high or low money laundering risk;
- Determining the business profile of the player, in order for The Company to be able to identify those transactions which may be deemed to be unusual for such player;
- Assisting the FIU by providing timely and precise information on Players and their transactions.

The Company may have a system in place, which detects whether a Player is subject to any financial sanctions issued by the UN Security Council or the EU in relation to persons known to be involved in terrorism:

- (i) Sanctions websites shall be consulted as soon as the identity of the Player is established.
- (ii) Independent research should be carried out through world-check and other similar online commercial databases (for example, a Google search).

The Company should be alerted to the OECD Anti-Bribery Convention.

The Company will strive to use automated sanction checking platforms such as Sumsb and LexisNexis.

2.2. Enhanced Customer Due Diligence:

Enhanced Customer Due Diligence is to be applied and maintained in relation to all Players considered to be on a high risk-sensitive basis.

In addition to the three specific instances mentioned above, The Company must conduct EDD in relation to a business relationship or a transaction connected to a jurisdiction listed under the public documents issued by the FATF, which is contained in Appendix II. Moreover, The Company must inform the FIU of any business relationships or transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity from a non-reputable jurisdiction.

Generally, the Company will refrain from conducting business with persons from non-reputable jurisdictions and/or jurisdictions on any high-risk FATF lists.

2.2.1. The identification of the Player and the verification of his identity¹:

The Company must first identify the player and in a separate procedure verify such identity.

2.2.1.1. Natural Person:

Identification:

All of the following should be obtained:

- (a) Full name and surname;
- (b) Place and date of birth;
- (c) Permanent residential address;
- (d) Identity reference number (I.D./Passport number); and
- (e) Nationality.

i. Verification:

When the applicant for business is **present for verification purposes**, the verification of the person's identity shall be made by reference to **any one** of the following containing photographic evidence of identity:

- (a) Valid, unexpired passport (original);
- (b) Valid, unexpired government-issued ID card (original); or
- (c) Valid unexpired driving license (original).

Verification of the person's residential address shall be made by reference to **any one** of the following which must be **not more than 6 months old**:

- (a) A recent statement from a recognised bank (original);
- (b) A recent utility bill (original);
- (c) A correspondence from a local or central government entity (original);
- (d) Any government-issued document listed in (Aii) above, where a clear indication of residential address is provided

The verification of the person's identity shall be made by applying **one or more** of the following measures:

- (a) Use identity verification software and video conferencing together with document scanning software to establish authenticity and confirm identity.
- (b) Require certified confirmation of the documentation supplied by a person carrying out relevant financial business.
- (c) Ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution holding a license in a reputable jurisdiction.

2.2.2 Legal Persons

The Company shall generally have no relationships with companies in that its customers shall only be natural persons. When dealing with suppliers, mostly technology companies will be dealt with as software providers and similar. In this case, a request of the share register of the supplier, its certificate of registration, its memorandum and articles together with a confirmation of beneficial owner will be requested. The same checks as carried out above for Players will be carried out for beneficial owners of suppliers in order to ensure that the Company does not do business with sanctioned and/or questionable persons.

2.2.3. When the applicant for business is a PEP

The Company will refuse business from PEPs as a general policy.

Chapter 3: Understanding the nature and profile of the business relationship

3.1. Information on the purpose and intended nature of the business relationship

The Company must obtain all the following information in order to establish the business and the risk profile of the application for business:

- Identity, Age, Place of Residence, Nationality.
- The nature and details of the business/ occupation/ employment of the applicant for business;
- The source(s) of funds and wealth;
- The expected source and origin of the funds to be used in the business relationship;
- The anticipated level and nature of the activity that is to be undertaken through the relationship;

3.2. On going monitoring of the business relationship

Once the business profile of the customer has been established, The Company must continue monitoring the activities on an on-going basis in order to identify any unusual transactions which may involve ML/FT. On-going monitoring of a business relationship includes:

- The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including **where necessary**, the source of funds. The Company must ensure that the customer's business corresponds to the information disclosed by the customer at the beginning of the business relationship and that the business patterns of the customer are consistent with the risk profile established by the subject person.
- Ensuring that the documents, data or information held by the subject person are kept up to date. The Company must ensure that any expired documentation is replaced by the latest documents within 2 months of the expired date.

The Company should pay special attention to any large complex transactions, including patterns of transactions that have no apparent or visible economic or lawful purpose and business relationships and transactions with persons from non-reputable jurisdiction. A list of countries associated with non-reputable jurisdiction is found in Appendix II. These are generally not accepted by the Company.

3.3. Monitoring complex or large transactions

The Company must examine complex or large transactions with special attention to the following transactions:

- the background and purpose of any complex or large transactions,
- unusual patterns of transactions,
- complex or/and large transactions which have no apparent economic or visible lawful purpose and
- transactions which are particularly likely, by their nature, to be related to ML/FT.

Where it is revealed that the customer's business and risk profiles have significantly diverged from the established patterns or for no apparent economic or lawful purpose, the employee or appointee must immediately report to The Company by submitting an internal report.

3.4. Source of wealth and source of funds

The Company shall enquire about the source of wealth at the beginning of the business relationship.

In higher risk scenarios, the customer must provide detailed explanation together with documents to substantiate such explanations such as contracts.

The Company must also obtain information on the source of funds. In higher risk scenarios, the Company shall not, to the extent possible, be satisfied with a generic description when questioning the customer about the origin of the funds used in the context of a business relationship. For example, in a high risk scenario, an explanation by the customer stating that funds consist of the proceeds generated by a business would not be sufficient and more detailed information on the business concerned as well as producing copies of invoices or contracts to substantiate such explanation need to be requested. The source of funds to be utilised for an occasional transaction must also be identified by The Company.

3.5. Risk- assessment procedures

The Company must identify and assess ML/FT risks posed by our customers, products and services. The risk assessment procedure shall include the below, together with automated analyses of betting patterns, deposits and withdrawals:

3.5.1. Customer risk Assessment

The Company conducts a manual risk evaluation as part of the Customer Due Diligence (CDD) process whenever a customer's activity reaches a threshold of NAF 4,000 (approximately €2,000.00) in a single deposit or over a rolling period. This evaluation is carried out in accordance with the Financial Intelligence Unit (FIU) Guidelines, which identify four key risk factors:

- Customer Risk
- Product, Service, and Transaction Risk
- Distribution Channels Risk
- Geographical Risk

Depending on the assigned risk level, the Company applies different levels of due diligence:

- Low-Risk Customers: Standard Customer Due Diligence (CDD) procedures are followed, which include verifying basic customer information.
- Medium-Risk Customers: In addition to the standard CDD, the Company collects further details such as occupation, source of funding and wealth, place of birth, and nationality.
- High-Risk Customers: Enhanced Due Diligence (EDD) procedures are required, involving a thorough verification of all relevant documentation and a more extensive review of the customer's background.

By analyzing these factors, the Company seeks to thoroughly assess the potential risk presented by each customer. This enables the Company to make informed decisions and apply appropriate risk mitigation measures, ensuring compliance with regulatory requirements.

This risk is generally based on the person's economic activity, deposits, and/or source of wealth. The following is a list of categories of customers whose activities may pose a higher risk:

- Customers conducting their business relationship or transactions in unusual circumstances;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests;
- Cash and cash equivalent intensive business, **cash is not accepted by the company.**
- Use of digital assets
- Use of intermediaries within the relationship who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised;
- Customers that are PEPs (in General The Company will not service PEPs);
- Customers who are subject to sanctions or other economic measures.

The Customer Risk Assessment (CRA) is carried out within 30 days after the customer reaches the deposit threshold of NAF 4,000 (€2,000) within a rolling 180-day period. The outcome is a Customer Risk Profile, which is reviewed continuously throughout the course of

3.5.2. Product/service risk

Some products/ services are inherently more risky than others and are therefore more attractive to criminals. The following is a list of number of factors that The Company should take into consideration when determining the risks of products and services:

- The nature of the product/service offered by the Company, that of gambling related services, may be more attractive to criminals looking to launder money. This is to be kept in mind when analysing customers and transactions. Vigilance must be placed upon customer backgrounds

and types, together with betting behaviour in order to ensure that our platform is not used to launder the proceeds of crime.

3.5.3. Interface risk

The channels through which a subject person establishes a business relationship and through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. The use of internet for the provision of services is considered as a high risk, in view of the rapidity with which online transactions may be conducted and the level of anonymity that such transactions may offer. Customers dealing in crypto currency should be treated as high-risk.

3.5.4. Geographical risk

This risk relates to the geographical location of the business/economic activity and the source of wealth/ funds of the business relationship. The following list should be assessed in determining when a country poses a higher risk:

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as United Nations Security Council.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

3.5.5 Scoring

The Company defines the allocation of risk percentages across various categories as part of its comprehensive, risk-based approach. These allocations reflect the relative importance of each risk area in determining the overall risk associated with a customer. The risk categories and their corresponding allocations are as follows:

- Customer Risk (30%): This category evaluates the individual characteristics of the customer, including their financial background, occupation, and potential exposure to high-risk activities. A higher weight is assigned to customers whose profiles present elevated concerns regarding illicit activities or financial crime.
- Product, Transaction, and Service Risk (40%): This category focuses on the risk associated with the products, services, and transactions that the customer engages with. Higher percentages are allocated to high-risk products or services, such as those involving large or complex financial transactions, or gambling activities, which may present increased money laundering risks.
- Delivery Channel Risk (10%): This assesses the risk posed by the method through which services are delivered, including online channels or physical locations. Digital platforms or other remote services may carry higher risks due to their susceptibility to anonymous transactions or lack of face-to-face interaction.

- Geographical Risk (20%): This category evaluates the risk related to the customer's location and the jurisdictions they are connected to. Regions known for weak anti-money laundering controls or high levels of corruption may contribute to a higher risk assessment.

NON-REPUTABLE AND NON-COOPERATIVE JURISDICTIONS

The following is a list of countries recognised by the Financial Action Task Force as high risk and non-cooperative jurisdiction as per the FATF Public Statement & On-going Process Document which is amended and updated from time to time:

Afghanistan
Albania
Algeria
Angola
Argentina
Cambodia
Cuba
Democratic People's Republic of Korea
(DPRK)
Ecuador
Ethiopia
Indonesia
Iran
Iraq
Kuwait
Lao PDR
Myanmar
Namibia
Nicaragua
Pakistan
Panama
Papua New Guinea
Sudan
Syria
Tajikistan
Turkey
Uganda
Yemen
Zimbabwe

Business Risk Assessment
(BRA)

Version:	1.1
Date of version:	26/05/2025
Created by:	Michael Muscat (CO) /Cindy Drommond (MD)
Approved by:	Michael Muscat (CO) /Cindy Drommond (MD)
Confidentiality level	Restricted

Change History

Version	Date	Author	Comment
1.0	02/05/2025	Michael Muscat (CO)	Initial Release
1.1.	26/05/2025	Cindy Drommond (MD)	Amendments added

Review History

Version	Date	Reviewed By	Comment
1.0	26/05/2025	CindyDrommond (MD)	Amendments added (1.1) & approved
1.1.	27/05/2025	Michel Muscat (CO)	Approved

1. Overview and Objective

Velorum Corporation N.V. (hereinafter referred to as "the Company") has established comprehensive measures to effectively mitigate the risks associated with Money Laundering and the Financing of Terrorism (ML/FT).

The Company operates within the regulatory framework set forth by the Curacao Gambling Authority (CGA) and holds a Business-to-Consumer (B2C) license, which authorizes it to provide remote gaming services to eligible clients. Its core mission is to offer gaming entertainment across jurisdictions deemed acceptable by the Curacao Gaming Control Board (GCB), fully compliant with applicable terms, conditions, and regulatory standards.

Operating under the brand name BonkersBet, the Company utilizes a gaming platform to deliver its services, ensuring operational functionality across all critical sectors, including player registration, transaction processing, customer support, and responsible gaming practices.

In strict adherence to its obligations as a subject person under Curacao's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regulations, the Company has undertaken a comprehensive AML/CFT Business Risk Assessment (BRA) to identify, assess, and manage the risks associated with its activities and service offerings.

Aligned with its overarching risk management framework, the Company has adopted and maintains a Medium Risk Appetite, balancing its commitment to business growth with the need to proactively address and minimize exposure to ML/FT threats.

1. Responsibilities

The Compliance Officer bears primary responsibility for the supervision and monitoring of all customer transactions and the verification of the identities of registered players. Beyond these core duties, the Compliance Officer is also responsible for establishing clear and effective criteria for the early detection of potentially suspicious activities. They must design, implement, and continuously update internal protocols to address identified risks and ensure that exposure to Money Laundering and Financing of Terrorism (ML/FT) threats is minimized to the greatest extent possible.

However, the obligation to combat ML/FT is not limited to the Compliance Officer alone. Every employee of the Company who is involved in customer-facing operations, payment processing, or transaction monitoring must actively participate in the Company's overarching Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) framework. This includes strict adherence to the Company's established policies, operational procedures, and internal controls designed to detect and prevent illicit activities.

To support this collective responsibility, the Company must ensure that all relevant employees receive comprehensive and ongoing AML/CFT training programs. These training sessions are designed not only to enhance awareness of emerging ML/FT risks but also to reinforce employees' understanding of their personal and professional obligations under the regulatory

regime. Training must be updated regularly to incorporate changes in legislation, regulatory guidance, and identified risk trends.

2. Risk Assessment

Risk is defined as the possibility of an adverse event occurring, or the failure to achieve a desired outcome, which negatively impacts business operations, reputation, or financial stability. Risks become evident in a variety of situations, including:

- Failure to meet established business objectives and performance targets.
- Non-compliance with internal organizational policies, external regulations, or relevant legislation.
- Inefficient, ineffective, or inappropriate use of business resources or assets.

To proactively manage these risks, the Company must implement a comprehensive and effective risk assessment and management framework. This framework should be designed not only to prevent potential threats from arising but also to ensure that contingency plans are in place to mitigate the impact of risks if they do materialize.

The risk management process should be robust, standardized, and well-documented, providing clear guidelines for conducting assessments. This ensures that assessments produce consistent, valid, and comparable results, regardless of who conducts them or when they are carried out.

In line with industry standards, the Company adheres to risk assessments performed by the Curacao regulatory authorities, as well as relevant supranational risk assessments for the gaming sector. These assessments consistently highlight the gaming industry as a high-risk environment due to its susceptibility to various forms of financial crime, including money laundering and terrorist financing. The Company also aligns its operations with the Curacao Framework, ensuring that its risk management processes are in line with national and international best practices.

3. Criteria Risk Assessment

There are various situations in which conducting an Anti-Money Laundering and Financing of Terrorism (AML/CFT) risk assessment becomes essential for the Company. These situations typically include:

- Performing a comprehensive risk assessment that evaluates a wide range of factors, including the diverse customer types the Company serves, the range of services it provides, the communication channels used to interact with customers, and the geographical regions in which the Company operates. This ensures a holistic understanding of the associated risks.
- Integrating periodic updates to the AML/CFT risk assessment into the Company's regular management review process. This ongoing review helps to adapt to changing internal and external conditions, ensuring the Company remains vigilant to emerging risks.
- Evaluating internal projects or strategic initiatives that are expected to introduce significant changes to the Company's business model. These changes may involve new services, markets, or technological innovations, each of which could introduce new risks that require thorough assessment.

- Undertaking a reassessment of the existing risk landscape when substantial external events or changes occur that could render prior risk assessments outdated or incomplete. Such events include alterations to applicable laws, regulations, or other significant shifts in the external environment that could affect the Company's risk exposure.

In cases where there is any doubt or ambiguity regarding whether a risk assessment is needed, the Company should adopt a precautionary approach and proceed with conducting an assessment. This ensures that potential risks are proactively identified and addressed, minimizing the possibility of compliance gaps.

4. Process – Risk Assessment

The risk assessment process follows a structured series of steps as outlined below:

- **Asset Identification:** This step involves recognizing the critical assets at risk related to Anti-Money Laundering and Financing of Terrorism (AML/CFT). The primary focus is on protecting assets such as the Company's reputation and its compliance standing. Failure to safeguard these assets could lead to severe consequences, including the suspension of operational licenses, financial penalties, or potential legal action against individuals responsible for AML breaches.
- **Risk Area Identification:** This step is concerned with identifying the various risk areas across the organization. It encompasses customer types, services provided, communication channels used, geographical locations of operation, as well as both internal and external operational risks, particularly those related to employees who manage customer relationships.
- **Threat Identification:** This involves evaluating threats specific to each identified risk area, taking into account known occurrences and vulnerabilities within the Remote Gaming Industry. Understanding these threats allows the Company to anticipate and prepare for potential risks.
- **Vulnerability Assessment:** Here, the Company assesses vulnerabilities that arise from factors such as limited face-to-face interactions with customers, the use of diverse payment methods, and the potential inadequacies in AML/CFT frameworks in certain jurisdictions. These vulnerabilities are critical to understanding areas where the Company is more susceptible to risk.
- **Risk Scenario Identification:** This step identifies specific risks to compliance and business operations through collaborative discussions and interviews with relevant stakeholders. The findings are documented in a Risk Matrix, which includes feedback from the Director, the Compliance Officer, and employees engaged in customer relations and payment processing.
- **Probability Assessment:** In this step, the likelihood of identified threats materializing is estimated based on historical data, trends within similar organizations, and the presence of sufficient motive, opportunity, and capability for the threat to manifest. This assessment is vital to gauge the likelihood of a risk occurring in the future.
- **Impact Assessment:** Finally, the Company evaluates the potential consequences of Money Laundering and Financing of Terrorism incidents. This includes assessing the legal, compliance, and operational impacts on the Company, as well as the broader implications for individuals and countries potentially vulnerable to terrorist activities.

This structured process ensures that all aspects of AML/CFT risk are thoroughly assessed, with an emphasis on proactive identification, evaluation, and mitigation of risks.

5. Evaluation and Analysis of Risks

To assess risks to assets and develop appropriate mitigation strategies, the Company has conducted a comprehensive analysis covering potential threats, vulnerabilities, the likelihood of occurrences, and the possible impact of such events. A 5-point scale is employed to quantify both the probability of risk and its corresponding impact.

The likelihood scale ranges from 1 (improbable) to 5 (almost certain), while the impact scale spans from 1 (negligible) to 5 (very high). This organized method enables effective risk prioritization, aiding in the development of more targeted management strategies. The risk matrix shown below visually displays these scales and supports the prioritization of risks.

The classification of each risk is based on the score derived from multiplying the likelihood and impact ratings. With both scales ranging from 1 to 5, the final scores range from a minimum of 1 to a maximum of 25, as shown in the matrix. Risks are categorized as follows:

- High: Scores of 12 or higher
- Medium: Scores between 5 and 10
- Low: Scores from 1 to 4

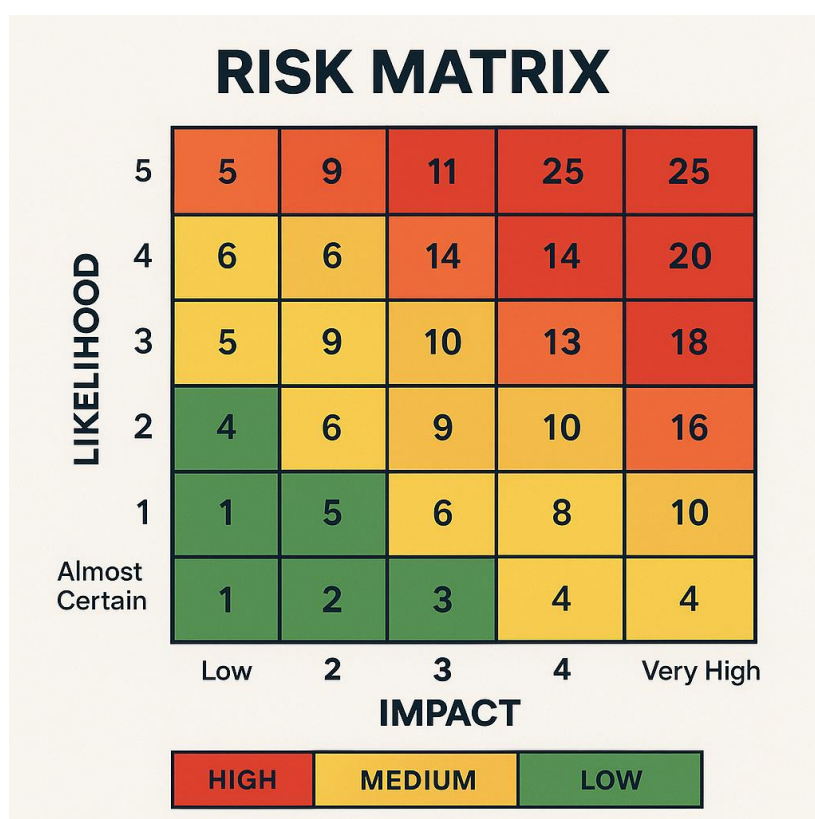


Figure 1 Risk Matrix Table Sample

The reasoning behind the assigned likelihood and impact ratings is documented to ensure that any significant changes can be assessed over time. If any material changes occur, the risk matrix will be updated, maintaining consistency in the evaluation of risks.

6. Effectiveness

The table below demonstrates the performance of the applied controls, offering a clear view of their strength in mitigating identified threats. This evaluation supports the analysis of the remaining (residual) risk level after all risk-reduction measures have been executed.

Mitigation Level	Description
4 – Robust	Controls are comprehensive, consistently applied, and proven to effectively mitigate associated risks. No immediate improvements are necessary.
3 – Adequate	Controls are generally effective and applied with reasonable consistency. Risk is managed satisfactorily, though some enhancements could improve overall performance.

2 – Limited	Controls exist but are inconsistently applied or only partially mitigate risk. Significant improvements are required to manage threats effectively.
1 – Absent	No meaningful controls are in place, or existing measures fail to mitigate the risk. Immediate corrective action is required.

The diagram below provides a structured representation of the methodology used to determine the Residual Risk outcome. This process involves evaluating the level of inherent risk, defined as the exposure to risk in the absence of any controls—and assessing the effectiveness of the existing mitigation measures. By cross-referencing these two variables in a matrix, the residual risk level is calculated. This outcome reflects the degree of risk that remains after all mitigating controls have been applied, and serves as a key indicator for decision-making in risk management strategies.

Residual Risk				
		Inherent Risk		
		Low	Medium	High
Aduacus Adequacy	Robust	Low	Low	Medium
	Adequate	Low	Medium	Medium
	Limited	Medium	Medium	High
	Absent	Medium	High	High

Figure 2 Residual Risk

7. Risk Identification, Analyses and Evaluation

The following table presents an overview of the key business risk factors related to money laundering and terrorist financing (ML/FT), including the primary threats identified and the corresponding mitigation measures established.

A comprehensive breakdown of the risk identification and analysis process—along with an evaluation of the effectiveness of the controls, internal policies, procedures, and other risk mitigation strategies currently in place at the Company shall be entered into a risk matrix.

Risk Factor	Risks Identified	Mitigation Measures Implemented	Residual Risk
Interface	- Lack of in-person interactions increases the risk of customer anonymity and identity fraud. - Potential for misuse of digital onboarding channels.	- Basic Customer Due Diligence (CDD) conducted at onboarding and further upon reaching transactional thresholds. - Enhanced monitoring of behavioural patterns and unusual activity.	Medium
Customer	- Diverse customer types including VIPs, and high-risk individuals. - Risk of fraudulent or multiple account registrations.	- Standard and Enhanced Due Diligence applied based on risk classification. - Targeted screening of VIPs using reliable databases. - Continuous transaction monitoring.	Low
Product	- Abuse of certain products or payment functionalities (e.g., prepaid cards, rapid withdrawals). - Exploitation through repetitive behaviour patterns.	- Real-time monitoring of transactions for anomalies. - Implementation of strict controls on deposits and withdrawals. - Reporting of suspicious transactions as required.	High
Geographical	- Customers accessing services from jurisdictions listed as high-risk by FATF or similar bodies. - Use of payment methods linked to high-risk territories.	- Routine Geographical Risk Analysis mapped against FATF lists. - Application of SDD, CDD, and EDD as per risk level. - Regular review of country risk indicators. Persons from high-risk jurisdictions will generally not be serviced.	Medium
Employee Risk	- Possibility of unintentionally or intentionally facilitating ML/FT due to lack of awareness or controls. - Assignment of AML responsibilities inappropriately.	- Thorough pre-employment screening of relevant staff. - Mandatory AML/CTF training and regular refreshers. - Supervision and periodic internal audits.	Medium
Outsourcing	- AML obligations are performed in-house; outsourcing such functions is restricted or non-permissible under the company policy.	- Not applicable, as AML tasks are exclusively managed internally under strict oversight.	N/A

8. AML/CFT Risk Management Process

The overall medium risk rating assigned to all identified risk factors is deemed reliable only if the Company constantly and effectively enforces its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), Fraud Prevention, Business, and Customer Risk Management Policies and Procedures. The ongoing success of this risk level classification is

also contingent upon the company's continuous monitoring and scrutiny of customer activity across all operational channels.

As part of this assessment, the company's relevant internal policies and procedures have been thoroughly reviewed and updated to reflect the current AML/CFT Risk landscape. These updates are essential to ensure that the control framework remains effective and proportionate to the level of risk identified.

The company is committed to conducting periodic reviews and timely updates of these procedures, with the objective of maintaining full alignment with applicable legal and regulatory obligations. Moreover, regular evaluations of the adequacy and efficiency of implemented risk mitigation measures will be performed to ensure that the residual risk remains within acceptable limits, as defined by the company's stated risk appetite.

This AML/CFT Risk Assessment shall be reviewed and updated at least once every 12 months. However, it must also be re-evaluated sooner if there are any significant changes in the company's operational structure, customer base, product offering, risk exposure, or applicable laws and regulations.

Until the next scheduled review date, the company must maintain heightened awareness of any developments that could impact its risk profile. Any such changes may trigger an early reassessment of this document to ensure continued relevance and regulatory compliance.

Current Risk Evaluation Summary:

Inherent Risk Level: Medium

Residual Risk Level: Medium