

Business Risk Assessment Report

Aquarius Entertainment N.V.

Curaçao

May 2026

Approval date	Board of directors' signature
21.05.2026	

Table of Contents

Table of Contents	2
Purpose	3
Sources used	3
Understanding the Company's Business	3
Methodology	4
Risk identification	4
Risk analysis and evaluation	5
Inherent risk assessment	5
Mitigation measures assessment	7
Residual risk assessment	8
Risk appetite	9
Annexes	10

Purpose

This Business Risk Assessment Report ("BRA") identifies, assesses, and documents the ML/FT/FP risks arising from the Company's operations as an online casino in Curacao, establishing the grounds and principles for the Company's ML/FT/FP risk management framework.

The purpose of the BRA is to:

- identify inherent ML/FT/FP risks associated with the Company's business operations;
- evaluate the likelihood and impact of those risks;
- assess the effectiveness of mitigating controls;
- determine the Company's residual risk exposure; and
- support compliance with applicable AML/CFT/CFP obligations.

Sources used

The BRA has been prepared using the following sources:

- internal AML/CFT/CFP policies and procedures;
- the latest national risk assessment on ML of Curaçao;
- FATF and similar international organizations' guidance and typology reports applicable to online casino operators;
- national AML/CFT/CFP regulations and regulatory guidance applicable to online casino operators, primarily;
- other industry guidance for online casino operators.

Understanding the Company's Business

The Company operates an online casino platform offering remote gambling services to customers across various jurisdictions. The fully remote and cross-border nature of the business increases exposure to financial crime risks, particularly in relation to customer onboarding and source/destination of funds verification.

Key elements of the Company's business operations which are considered in the risk assessment include:

- business relationship establishment;
 - the Company establishes business relationships remotely;
 - the Company establishes business relationships only with natural persons;
 - the Company accepts customers from various countries (incl. countries in high-risk lists);
- deposits and withdrawals;
 - the Company allows to make deposits and withdrawals for the use of the services using both fiat currencies and crypto assets;
 - the payment processing is done through third-party providers;
- casino gameplay and wagering;
 - the Company provides its services via its online platform;
 - the estimated average amount of a single transaction ranges from 1.5-1,000 USD;

- the estimated average monthly deposit amount is 10,000 USD.
- customer relationships management;
 - the Company communicates with the customers via email.

By detailing the services or products offered, how and where they are provided, the Company is able to assess risks effectively. It ensures compliance with applicable regulations, addresses potential ML/FT/FP risks and outlines how resources will be allocated to manage these risks. Additionally, it provides a basis for continuous monitoring and quick adaptation to emerging threats, helping the Company stay resilient in the face of challenges.

Methodology

When conducting the BRA, the Company follows the risk assessment process detailed in the Company's AML/CFT/CFP Policy, consisting of the following stages:

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

Risk identification

This process consists of the identification and description of events that threaten the achievement of the Company's objectives (risks). It also seeks to identify the risks arising from missed opportunities and the opportunities arising from addressing risks.

To identify risks, the Company is guided by the following objectives:

- what could go wrong (event)?
- why might something go wrong (risk factors, i.e. causes)?
- what are the possible consequences (impact)?

When identifying risks, it must be taken into account that different risk factors may lead to the same risk materializing, the same risk factor may lead to different risks materializing and a risk may have multiple adverse consequences. The Company determines if there are any requirements for managing specific risks and develop description of such risks according to such requirements, as well as decides if there's any risks which the Company intends to manage according to business decision (i.e. without an obligation arising from applicable legislation or other sources).

The Company categorizes the risks across the following key categories:

- **customer risk** - the risk for the Company to be potentially abused due to the business field or profile of the customer or the acts of customer or those acting on behalf or for the benefit of the customer for money laundering or terrorist financing purposes;
- **geographic risk** – the risk of potential financial, legal, or reputational losses that may arise from operating in a foreign country and exposing itself to unfamiliar regulations, a different legal system, and potentially unstable political environments;
- **service risk** - the potential risk that products or services offered by the customer may be misused by the criminals for money laundering or terrorist financing activities;

- **delivery channel risk** – the risk of potential misuse of the financial channel supplied through the customer for ML/FT/FP.

The Company has described the risks identified in a reasonably generalized formulation in the **Risk Register** (annex 1).

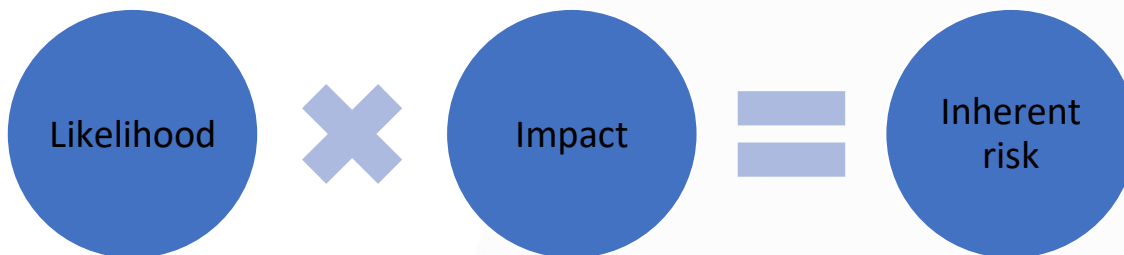
Risk analysis and evaluation

In the course of this process the Company identifies possible consequences (impact types) arising from risks to be managed, methods (incl. scales) for risks assessment and maximum acceptable value of such consequences. Each risk factor is assessed based on:

- likelihood of misuse for ML/FT/FP purposes;
- potential regulatory, legal, financial, and reputational impact;
- complexity and scale of exposure;
- availability and effectiveness of mitigating controls.

Inherent risk assessment

Inherent risk level is found via an assessment of the risk factors using the following formula:



Likelihood is the probability that a given risk event will occur, which can be expressed using numerical values (1-4), as a score to measure the probability, complexity of a business process and frequency. Likelihood is found using the following criteria against three separate dimensions:

Likelihood of a risk event			
Score	Possibility	Complexity of a business process	Frequency
4	More often than once a year	Business is very complex; changes in the business process are significant and frequent.	The risk occurred within the last year and mitigation measures have not yet been implemented.
3	Once a year	Process of above average complexity.	Risk has occurred in the last 3 years and mitigation measures have not yet been implemented.

2	Once during three years	Process of medium complexity.	The risk has not yet materialized and may occur in very specific circumstances.
1	More rarely	The process is simple, straightforward and stable, with few participants.	The risk has not yet materialized; The risk has occurred in the past, but adequate mitigation measures were applied to reduce the likelihood of the risk occurring.

The score should be assigned, if at least one Likelihood with such score exists regarding risk factor (e.g., if possibility is 4 and all others are 1, for example, then the overall Likelihood = 4).

Impact is the extent to which a risk event might affect the Company, which can be expressed using numerical values (1-4), as a score to measure the impact on four separate dimensions (financial, reputational, business interruption, legal). Impact is found using the following criteria against four separate dimensions:

Impact of a risk event				
Score	Financial impact	Reputational impact	Business interruption	Legal impact
4	Decrease in revenue or increase in costs >20%;	Reputational impact significant and long-lasting, negative news in national publications, social media coverage, as well as international mentions.	Long-term business process interruption. Significant negative impact on the Company's objectives.	License revocation; Significantly material penalty; Loss of critically important outsourcing partner.
3	Decrease in revenue or increase in costs 5%-20%;	Reputational impact Significant and short-lived, negative news in a national publication, social media coverage.	Business process interruption can be restored in a longer time than planned	Monetary Penalty
2	Decrease in revenue or increase in costs 2%-5%;	Reputational impact short term and insignificant	The business process breaks down, but quickly recovers	Regulatory precept
1	Decrease in revenue or increase in costs <2%;	No reputational impact.	Business process is not interrupted, but there are glitches	No legal impact

The score should be assigned, if at least one impact with such score exists regarding risk factor (e.g., if financial impact is 4 and all others are 1, for example, then the overall Impact = 4).

4	8	12	16
3	6	9	12
2	4	6	8
1	2	3	4

According to the assessed likelihood and impact level, the risk is assigned a corresponding **Risk Level**:

- Red - Critical
- Orange - High
- Yellow – Medium
- Green – Low

The Company evaluates each risk factor to determine the inherent risk score which is specified in the **Risk Register**.

Mitigation measures assessment

After the inherent risk has been identified, the Company performs an assessment of the **mitigating measures** and controls to evaluate the appropriateness and effectiveness of such measures. The following scale should be used for evaluation of mitigating measures.

Mitigation Measure Effectiveness	Description of the effectiveness of the mitigation measure
Effective (score - 4)	Systems and processes effectively mitigate risk, accountability is clear, well documented, and subject to regular and appropriate monitoring. There is a high level of confidence that the risk is avoided or mitigated properly.
Sufficient (score - 3)	Mitigation measures contribute to reducing risk. Process improvements are needed to achieve better efficiency. There is reasonable assurance that the risk is avoided or mitigated properly.
Insufficient (score - 2)	Mitigation measures have a limited impact on risk mitigation, and processes and systems need significant improvement and monitoring. There is insufficient assurance that the risk is avoided or mitigated properly.
Not acceptable (score - 1)	Mitigation measures do little or nothing to reduce the impact of inherent risk. Immediate management intervention and efforts are necessary to manage the risk. Significant re-design and streamlining of processes and systems required. There is a belief that the risk can't be avoided or mitigated properly.

Factor-specific mitigation measures and the evaluation results are placed into the **Risk Register**. In addition to the factor-specific measures, the Company also considers the following generally applicable ML/FT/FP risk mitigation measures applied by the Company, including:

- preparation and the regular review of an AML/CFT/CFP Policy;
- regular internal audit of the effectiveness and compliance with the AML/CFT/CFP Policy;
- defining the responsibilities of relevant persons under the AML/CFT/CFP Policy (incl. appointment of a qualified Compliance Officer);
- establishment and application of CDD/EDD/ODD procedures;
- establishment of internal unusual transaction reporting channel(s) and the obligation to report unusual transactions or the suspicion thereof (incl. external reporting);
- screening and periodic AML/CFT/CFP training of employees;
- establishing the consequences of violations of the obligations under the AML/CFT/CFP Policy.

Residual risk assessment

After inherent risks and controls have been evaluated, the Company calculates residual risk score for each risk factor and puts the results to the **Risk Register**.

Residual Risk is assessed using the following formula:



The Company should also calculate average residual risk score for each risk and risk category (if any).

According to the assessed inherent risks and controls, the score of residual risk shall be determined as follows:

Effectiveness of Migration Measures					
Inherent Risk	Score	Effective	Sufficient	Insufficient	Not acceptable
	Critical	Low	Medium	High	Critical
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

As result of the above process, the Company analyzes if there is a necessity to implement any of the following actions:

- amending and approval of the Company's Risk Appetite;

- implementation of additional mitigating measures;
- ongoing continuous monitoring (incl. enhanced monitoring);
- making changes in business process(es).

Risk appetite

As result of the above process, the Company establishes its risk appetite, which is outlined in the **Risk Appetite statement** (annex 2).

Annexes

Annex title	Document description
1. Risk Register	Documentation of the identified ML/FT/FP risks and their assessment.
2. Risk Appetite Statement	The articulation in written form of the aggregate level and types of risk that the Company is willing to accept, or to avoid, in order to achieve its business objectives.

Risk Appetite Statement

Aquarius Entertainment N.V.

Curaçao

May 2026

Version Control Table

Approval date	Changes description	Board of directors' signature
21.05.2026	First issue	

Introduction

The Company's Risk Appetite Statement articulates the Company's philosophy and approach to the management of its key ML/FT/FP risks based on the business risk assessment (BRA) carried out as well as guides decision-making and ensures appropriate governance around risk-taking within the Company.

The Company's Risk Appetite is the type and the amount of risk that the Company is willing to accept or to avoid in order to achieve its business objectives. The Risk Appetite Statements clarify those risks and associated limits that the Company must manage and, where appropriate, is prepared to accept in the pursuit of its vision and objectives.

The Senior Management is responsible for setting the Risk Appetite of the Company which it reviews and approves **at least annually**. The Senior Management of the Company is responsible for ensuring that their business is operating within their stated Risk Appetite parameters. The Company's Risk Appetite is forward-looking and it evolves to reflect external market developments and the Company's strategic focus.

Risk Appetite Statement

The Company has a **medium-to-high** risk tolerance for ML/FT/FP risk. This includes undertaking activities that may involve elevated inherent or residual risk, provided such risks are identified, assessed, and considered controllable to a large extent through appropriate governance, oversight, and risk mitigation measures. The Company does not seek to eliminate all risk but aims to manage it responsibly to support sustainable growth and informed decision-making.

At the same time, the Company maintains a zero-tolerance approach toward ML/FT/FP, sanctions violations, and other illicit use of its services. To mitigate these risks, the Company implements proportionate mitigation measure and controls within its AML/CFT/CFP Policy to identify, investigate, and report suspicious or unusual activities and to prevent misuse of its services for unlawful purposes.

The established ML/FT/FP risk management controls are proportionate to the risks faced by the Company. The Company is committed to combating financial crime and continually strives to ensure that accounts held at the Company are not misused for the purpose of ML/FT/FP. In line with this, the Company will not:

- knowingly facilitate criminal activities carried out by customers;
- accept any deliberate or systemic breaches of applicable laws and regulations;
- facilitate transactions with individuals that cannot be identified in accordance with Company's AML/CFT/CFP Policy and are unresponsive to information requests by the Company which is significant to their identification, or intentionally provide misleading information to the Company which is significant to their identification or activities;
- allow the use of the Company's services using anonymity-enhancing methods, including:
 - use of certain crypto assets, accounts/wallets and payment institutions/VASPs;
 - use of measures which allow to conceal the location of the customer's devices;
 - use of un-approved identification and communication methods;
- establish or continue business relationships with customer who are subject to risk factor(s) with prohibited risk in accordance with the Company's **List of Risk Factors**, including:
 - customers with certain characteristics (incl. behavior, area of activity, age restrictions);

- customers residing in certain countries;
- the manner in which customers use or request to use the Company's services.

This approach allows the Company to onboard and service a wider range of customers, including those presenting elevated inherent risk, where such relationships are lawful and commercially justified. Customers subject to low-high risk factors determined in the **List of Risk Factors** may be accepted by the Company. Customers subject to one or more high risk factors (as determined by the Company's customer risk assessment) must be subjected to the relevant EDD measures in accordance with the AML/CFT/CFP Policy prior to onboarding and on an ongoing basis.

Risk factor	Category	Impact considerations
Customers may attempt use the Company's services without being identified	Customer	The customer may conceal the UBO of the transactions concluded and may be subject to unacceptable risk factors .
Customers may use illicit funds when using the Company's services or direct the funds from the Company's platform to FT/FP use	Customer/services	The Company's services may be directly involved in the process of ML/FT/FP.
Persons subject to sanctions may request to use the Company's services	Customer	It may refer to the fact, that customer is involved in ML/FT/FP.
Persons subject to adverse media can use the Company's services	Customer	It may refer to the fact, that customer is involved in ML/FT/FP.

Persons outside the average age of services user may use the Company's services	Customer	Persons above the average age of the services user are subject to heightened fraud and misuse risk.
Third persons persons may attempt to use the Company's services	Customer	It may refer to the fact, that customer is involved in ML/FT/FP or there is concealment of the UBO.
Customers can display suspicious or unusual behaviour (incl. when providing KYC info, making transactions or communicating with the Company)	Customer	It may refer to the fact, that customer is involved in ML/FT/FP or there is concealment of the UBO.
PEP's can use the Company's services	Customer	PEPs can misuse their position for ML/FT/FP activities.
The Company's services may be accessed by residents in various countries, including, countries with weak AML/CFT/CFP regimes, countries subject to higher levels of crime and/or corruption	Geographic	It may cause reduced business relationship transparency and increased difficulty in verifying customer legitimacy and source of funds.

Customers may carry out high-value transactions	Services	It may create increased exposure to ML/FT/FP risks.
---	----------	---

Customers may open more the one account with the Company	Services	It may refer to the fact, that customer is involved in ML/FT/FP or there is concealment of the UBO.
--	----------	---

Customers may attempt to use the Company's services using anonymity enhancing measures	Services/delivery channel	It may refer to the fact, that customer is involved in ML/FT/FP or there is concealment of the UBO.
--	---------------------------	---

The Company offers services for crypto assets	Services/delivery channel	Crypto assets may pose higher ML/FT/FP risks than traditional payment methods.
---	---------------------------	--

The Company may adopt 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	Services/delivery channel	New products or services may pose new ML/TF risks.
---	---------------------------	--

The Company identifies the customers remotely	Delivery channel	Remote identification inherently increases the risk of impersonation and identity fraud due to the lack of direct interaction between parties.
---	------------------	--

<u>Likelihood</u>	<u>Impact</u>	<u>Inherent risk</u>
-------------------	---------------	----------------------

2	4	8
---	---	----------

3	4	12
---	---	-----------

3	4	12
---	---	-----------

3	3	9
---	---	----------

2	3	6
---	---	----------

3	4	12
---	---	-----------

3	4	12
---	---	-----------

2	4	8
---	---	----------

4	3	12
---	---	-----------

3	2	6
---	---	----------

2	2	4
---	---	----------

3	3	9
---	---	----------

4	3	12
---	---	-----------

3

3

9

4

2

8

Mitigation measures	Mitigation score	Residual risk
In the case the customer engages in transactions below the limits established in the AML Regulation (Naf 4,000) the Company applies at least the minimum level of CDD measures prescribed in the AML Regulation. Customer identification is carried out prior to exceeding this limit or prior to the first withdrawal. The Company additionally applies screening and monitoring measures to identify cases of unauthorised access (e.g. IP detection) and cases where info provided is shared with another account. The Company refuses a business relationships if the required CDD/ODD/EDD measures cannot be applied. The Company allows deposits/withdrawals only from/to accounts/wallets held by the customer. The Company does not allow to use cash and specific crypto assets when using its services (incl. anonymity-enhancing methods, unregulated/unlicensed services/tokens). Where deemed necessary, the Company may request additional information to understand the purpose of the transactions and the customer's area of activity (incl. relations to high-risk areas). The Company applies ODD measures to identify suspicious circumstances. The Company applies EDD measures in the case of identifying suspicious circumstances concerning the source or destination of the funds used when using the Company's services. The Company prohibits subjects of sanctions from using its services. The Company screens customers against watchlists during onboarding and periodically during the ongoing monitoring. The Company checks the adverse media existence during onboarding and periodically during the ongoing monitoring. The Company applies EDD measures in the case of identifying adverse media and determines whether the business relationship may be concluded or continued on a case-by-case basis.	4 3 2 3	Low Medium High Medium

The Company applies heightened scrutiny when monitoring the activity and transactions of persons above the average age of the services user. The Company prohibits persons under the age of 18 or below the legal age of gambling from using its services.

4 Low

The Company defines the characteristics when the customer risk is unacceptable for the Company and applies CDD/EDD/ODD measures to identify such circumstances as well as circumstances where the UBO may be concealed (incl. key persons, legal entities, sanctioned persons, self exclusion periods). The Company does not open anonymous or fictitious named accounts.

The Company applies screening and monitoring measures to detect suspicious/unusual activity and cases of unauthorised access (e.g. IP detection). The Company allows deposits/withdrawals from/to only accounts/wallets held by the customer.

2 High

The Company determines indicators pointing to potentially pointing to suspicious/unusual behaviour. The Company applies EDD measures in the case of identifying suspicious/unusual behaviour and determines whether the business relationship may be concluded or continued on a case-by-case basis.

The Company applies for PEPs, their family members and close associates the EDD measures prescribed in the AML Regulation.

The Company checks the customer's PEP status during onboarding and periodically during the ongoing monitoring.

3 Medium

3 Medium

The Company applies EDD measures for persons residing in high-risk countries. The Company identifies the high-risk countries which are within the Company's risk appetite (incl. EEA countries) and high-risk countries which are unacceptable based on national and international lists (incl. CGA lists, FATF black list, sanctions, sponsors of terrorism).

4 Low

The Company allows deposits/withdrawals only from/to accounts/wallets held by the customer.

The Company does not allow to use cash and specific crypto assets when using its services (incl. anonymity-enhancing methods, unregulated/unlicensed services/tokens).

Where deemed necessary, the Company may request additional information to understand the purpose of the transactions and the customer's area of activity (incl. relations to high-risk areas).

The Company has established and monitors the expected average volume of transactions to identify great deviances.

The Company applies ODD measures to identify suspicious circumstances.

The Company applies EDD measures in the case of identifying suspicious circumstances concerning the source or destination of the funds used when using the Company's services.

4 Low

The Company determines indicators pointing to potentially pointing to suspicious/unusual behaviour.

The Company applies EDD measures in the case of identifying suspicious/unusual behaviour and determines whether the business relationship may be concluded or continued on a case-by-case basis.

The Company applies screening and monitoring measures to identify cases where anonymity enhancing measures may be used (e.g. IP detection, VNS/TOR use).

The Company does not support anonymity enhancing payment methods (incl. use of certain crypto assets and payment institutions/VASPs).

4 Low

4 Low

The Company accepts new crypto assets and partnering VASPs in accordance with its Crypto Policy.

The Company allows deposits/withdrawals only from/to wallets held by the customer.

The Company does not allow to use specific crypto assets when using its services (incl. anonymity-enhancing methods, unregulated/unlicensed services/tokens).

3 Medium

Before adopting any new business practices or products, the Company assesses the related ML/FT/FP risks, reviews its AML/CFT/CFP Policy and making updates to it, where necessary.

3 Medium

The Company adopts technological measures and controls allowing to address the heightened risk presented by non-face-to-face identification. The Company requires that only the customer be present during the identification procedure. The Company additionally applies screening and monitoring measures to identify cases of unauthorised access (e.g. IP detection) and cases where info provided is shared with another account.

4 Low