

Overseas Gaming Management N.V.

AML/CFT Procedures Business Risk Assessment (BRA)

Version: 1.0
Date: 5th March 2025

Internal Use Only

Classification - Confidential

Version History:

Author	Date	Description	Version	Approval
A.Cacciattolo	5 th March 2025	Creation in line with GCB regulations	1.0	Compliance Officer

CONFIDENTIALITY STATEMENT

This is a confidential document between Overseas Gaming Management Limited (the 'Company') and the GCB (the 'Authority'). It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the aforementioned organisations without the written approval of the Company and the Authority.

Table of Contents

1	Introduction	4
2	Responsibilities	4
3	Risk Assessment	5
4	Risk Assessment Criteria	5
5	Risk Assessment Process	6
6	Risk Analysis and Evaluation	6
7	Effectiveness	7
8	Identification of Risk, Analyses and Evaluation	8
9	AML/CFT Risk Management Process	10

1 Introduction

Overseas Gaming Management N.V. (hereinafter referred to as "the Company") has implemented measures to mitigate the risks associated with Money Laundering and Financing of Terrorism (ML/FT).

The Company operates under the regulatory framework of the Curacao Gambling Authority (CGA) and holds a B2C license, enabling it to offer remote gaming services to clients. Its primary objective is to deliver gaming services across various jurisdictions which are acceptable by the GCB in line with our terms and conditions.

Operating under the brand name www.wgwgames.com, the Company will leverage its proprietary platform to facilitate these services, ensuring functionality across critical areas.

In adherence to its legal obligations as a subject person under the Curacao legislation, the Company has conducted a thorough Anti-Money Laundering and Combatting Financing of Terrorism (AML/CFT) Risk Assessment of its business operations.

The Company shall maintains a Medium Risk Appetite in alignment with its risk management strategies.

2 Responsibilities

The Compliance Officer holds the responsibility of overseeing all transactions and verifying the identities of registered players. Additionally, they are tasked with defining criteria to promptly identify any suspicious activities and devising protocols to address these issues while mitigating risks to the lowest possible level.

Nevertheless, every employee of the Company involved in customer operations and financial transaction processing must actively engage in the Company's Anti-Money Laundering and Combatting Financing of Terrorism (AML/CFT) strategy. This entails adhering to the policies, procedures, and controls established by the Company. The Company must provide regular AML/CFT training to its employees to ensure their awareness and compliance with these measures.

3 Risk Assessment

Risk refers to the occurrence of an unfavourable event or the absence of a desired event that negatively impacts business operations. Risk becomes evident under the following circumstances:

- Failure to achieve business objectives;
- Non-compliance with organizational policies, external regulations, or legislation;
- Inefficient or ineffective utilization of business assets.

The Company must establish an efficient risk assessment and management process to prevent potential threats from materializing, or to have contingencies in place to address them if they do arise.

These processes must be sufficiently clear to ensure consistent, valid, and comparable results across successive assessments, even if conducted by different individuals.

The company adheres to risk assessments conducted by Curacao, as well as supranational risk assessments for the gaming industry. These assessments have consistently identified the gaming sector as high-risk. Additionally, the company follows the Curacao Framework.

4 Risk Assessment Criteria

There are several circumstances that necessitate the undertaking of an Anti-Money Laundering and Financing of Terrorism (AML/CFT) risk assessment. Generally, the situations that would trigger such an action include:

- Conducting a thorough risk assessment that encompasses various customer types, services rendered, communication channels utilized, and geographic areas where the Company operates;
- Incorporating updates to the AML/CFT risk assessment as part of the routine management review process;
- Assessing any internal projects within the company that are anticipated to bring about significant alterations to the business model;
- Conducting a reassessment in response to major external changes affecting the organization that could potentially invalidate previous risk assessment findings, such as modifications to relevant legislation, among others.

In instances where there is uncertainty regarding the necessity of a risk assessment, the organization should err on the side of caution and proceed with conducting one.

5 Risk Assessment Process

The risk assessment process is structured into specific steps as follows:

- Asset Identification: This entails recognizing the assets at risk concerning Anti-Money Laundering and Financing of Terrorism (AML/CFT), primarily focusing on safeguarding the reputational and compliance status assets. Failure to protect these assets adequately could result in potential repercussions such as license suspension, financial penalties, or legal prosecution of the individual accountable for AML.
- Risk Area Identification: This step involves pinpointing risks associated with various aspects including customer types, services provided, communication channels, geographic locations, and internal and external operational risks linked to employees managing customer relationships.
- Threat Identification: Assessing threats within each risk area based on known occurrences within the Remote Gaming Industry.
- Vulnerability Assessment: Evaluating vulnerabilities stemming from factors such as predominantly non-face-to-face customer interactions, diverse payment methods, and inadequacies in AML/CFT systems in certain jurisdictions.
- Risk Scenario Identification: Identifying risks to compliance and business operations through discussions and interviews with relevant stakeholders, documented within a Risk Matrix. Stakeholders include the Director of Overseas Gaming Manager, the Compliance Officer, and employees involved in customer relations and payment processing.
- Probability Assessment: Estimating the likelihood of a threat materializing by considering past occurrences in similar organizations within the industry or location, along with evaluating the existence of sufficient motive, opportunity, and capability for the threat to manifest.
- Impact Assessment: Lastly, assessing the potential impact of Money Laundering and Financing of Terrorism incidents on various aspects including legal responsibilities, compliance status, and the repercussions on individuals and countries vulnerable to terrorist activities.

6 Risk Analysis and Evaluation

To evaluate risks to assets and determine suitable mitigation strategies, the Company has conducted an analysis encompassing threats, vulnerabilities, the probability of occurrence, and the potential impact of such events. Utilising a 5-point scale, the likelihood of risk occurrence and its corresponding impact have been quantified.

The likelihood scale ranges from 1 (improbable) to 5 (almost certain), while the impact scale ranges from 1 (negligible) to 5 (very high). This structured approach facilitates the

prioritization of risks, enabling more effective management strategies. The risk matrix, depicted below, visually represents these scales and aids in risk prioritization.

	LIKELIHOOD									
	IMPROBABLE	UNLIKELY	LIKELY	VERY LIKELY						CERTAIN
	L1 Infrequent – Less than once every 5 Years	L2 Once a Year or Less	L3 Quarterly or Less	L4 Monthly or Less						L5 Persistent more than monthly
					IMPACT					
					L1 Little to no affect	L2 Affects are felt but not critical	L3 Affects are felt but can be dealt with	L4 Serious impact to the source of outcome	L5 Could become catastrophic	
					Insignificant	Minor	Moderate	Major	Severe	

Risk classification is determined by the score obtained from multiplying the likelihood and impact ratings. With both scales ranging from 1 to 5, the resulting scores range from a minimum of 1 to a maximum of 25, as depicted in the matrix.

Each risk is categorized based on its score as follows:

- High: Scores 12 or higher
- Medium: Scores ranging from 5 to 10, inclusive
- Low: Scores ranging from 1 to 4, inclusive

The rationale behind assigning likelihood and impact ratings is provided to allow for future assessment of any material changes. Should such changes occur, the risk matrix will be updated accordingly, ensuring consistency in risk evaluations.

7 Effectiveness

The following table illustrates the efficacy of the implemented measures. It provides insight into the effectiveness of these controls, allowing for an assessment of the residual risk outcome.

Mitigation Level	Description
4 – Strong	Measures that are in place are fully operational and effective to control any risks.
3 - Effective	Mitigation measures work effectively and are effective, the risks are managed sufficiently but there could be improvements.
2 – Not Effective	Improvements are needed since risks are not managed sufficiently but have some effect.
1 – Not Existent	Controls are not in place and those in place are not effective.

The following diagram illustrates the process for calculating the Residual Risk outcome.

	Inherent Risk			
Effectiveness of controls		Low	Medium	High
	Strong	Low	Low	Medium
	Effective	Low	Medium	Medium
	Ineffective	Medium	Medium	High
	Non - Existent	Medium	High	High

8 Identification of Risk, Analyses and Evaluation

The table below outlines the high-level AML/FT business risk factors, threats, and mitigation measures.

The detailed results from the Risk Identification and Analysis, along with the evaluation of proposed measures, controls, policies, and procedures implemented at Overseas Gaming Management N.V., are provided in the attached Risk Matrix document labelled "Overseas Gaming Management N.V. Risk Assessment Matrix - V1.0".

Risk Factor	Risks	Mitigation measures	Residual Risk
Interface	- Engaging in interactions without face-to-face contact heightens the	- Due Diligence checks pre and post threshold met; - Ongoing	Medium

	likelihood of anonymity and the potential for customers to impersonate others.	monitoring.	
Customer	- Different types of Customers such as PEPs, VIPs etc.; - Fake or Multiple Registrations by the customers.	- Due diligence checks carried out even enhanced; - Checks on VIP, PEP players if registered; - Ongoing monitoring.	Low
Product	- Misuse of Payment Methods; - Replicating certain actions or behaviours.	- On-Going Monitoring and actively reporting; - Deposit and Withdrawal checks; - Ongoing Monitoring.	High
Geographical	- Geographical Risk of Customers from high-risk countries in line with FATF and other regulatory bodies; - Payment Methods from different / higher risk originating countries.	- Geographical Risk Analysis; - Due Diligence Checks (SDD, CDD and EDD); - Ongoing Monitoring.	Medium
Employee Risk	- Assignment of responsibilities to unsuitable employees; - Employee Accidental or Intentional Processing of ML/FT funds.	- Employee Screening; - Employee training; - Employee Monitoring.	Medium
Outsourcing	- AML tasks are done internally outsourcing is not permissible.	Not Applicable	N/A

9 AML/CFT Risk Management Process

The resulting overall medium risk level rating assigned to all risk factors is considered accurate only if the Company effectively implements and maintains its AML/CFT, Fraud, Business, and Customer Risk Policies and Procedures, and conducts ongoing monitoring of its active customers.

Relevant policies and procedures have been reviewed and updated based on this AML/CFT Risk Assessment.

Regular reviews and updates of procedures will be conducted as needed to ensure compliance with regulations. Additionally, frequent assessments of the effectiveness of measures and controls must be implemented as part of an ongoing process to keep risk levels aligned with the company's risk appetite.

This AML/CFT Risk Assessment must be reviewed annually at minimum, or more frequently if there are changes within the company related to AML/CFT or if legislation changes.

Until the specified date, the company must remain vigilant, as any changes affecting the Risk Factors may necessitate an earlier revision of this AML/CFT Risk Assessment.

As assessed, the company's overall risks are as follows:

Inherent Risk: Medium

Residual Risk: Medium