

Overseas Gaming Management N.V.

AML/CFT Procedures Customer Risk Assessment (CRA)

Version: 1.0
Date: 6th March 2025

Internal Use Only

Classification - Confidential

Version History:

Author	Date	Description	Version	Approval
A.Cacciattolo	6 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	Methodology.....	4
3	Risk Scoring	5
	3.1 Customer Risk	5
	3.2 Product, Transaction, and Service Risk	6
	3.3 Delivery Channel Risk.....	7
	3.4 Geographical Risk.....	8
4	Due Diligence Process	8
	4.1 Enhanced Due Diligence	9
5	Due Diligence Sanctions.....	10

1 Introduction

Overseas Gaming Management N.V. (hereinafter referred to as "the Company") has implemented protocols to evaluate the risk associated with each customer registering to participate in its gaming services.

The Company conducts a manual assessment of customer risk concurrently with the completion of Customer Due Diligence, triggered when a customer reaches a threshold of NAF 4,000 (equivalent to €2,000.00) in either a single deposit or over a rolling period. This assessment aligns with the guidelines outlined in FIU Guidelines, which delineate four primary risk factors:

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

By scrutinizing these factors, the Company aims to comprehensively gauge the level of risk associated with each customer, enabling informed decision-making and appropriate risk mitigation strategies in accordance with regulatory requirements.

2 Methodology

The company conducts a manual customer risk assessment based on the information gathered during the registration process. This assessment occurs once a customer reaches the NAF 4,000 (€2,000.00) deposit threshold. At this point, a risk rating is assigned to the customer, categorized as low, medium, or high risk.

Depending on the risk score assigned, different levels of due diligence procedures are initiated:

- Low-risk customers, standard Customer Due Diligence (CDD) is conducted.
- Medium-risk customers undergo CDD along with additional information gathering, including details about occupation, source of funding and wealth, place of birth, and nationality.
- High-risk customers undergo Enhanced Due Diligence (EDD), requiring comprehensive verification of all relevant documentation.

This risk assessment governs the extent and intensity of CDD and ongoing monitoring applied to customers. The evaluation considers the customer's economic activities and/or sources of wealth (SOW).

The Customer Risk Assessment (CRA) is performed within 30 days of a customer reaching the Naf 4,000 (€2,000) deposit threshold, within a rolling 180-day period. The resulting Customer Risk Profile is continuously reviewed as additional information becomes available during the business relationship. According to regulations, the initiation of this business relationship is marked by a customer opening an online account via the Company website in operation.

Furthermore, there is a possibility of reassessing the customer's risk rating at a later stage in the business relationship, potentially leading to an adjustment in their risk level. Customer risk is reviewed at least semi-annually, or more frequently in response to trigger events such as increased spending or reluctance to provide documentation for CDD. If the customer fails to provide the required documentation within 30 days, the company has the right to suspend and/or even close the account.

3 Risk Scoring

The allocation of percentages for each risk category is determined by the Company as part of its risk-based approach. This allocation is as follows:

- Customer Risk: 30%
- Product, Transaction, and Service Risk: 40%
- Delivery Channel Risk: 10%
- Geographical Risk: 20%

If a customer is identified as a Politically Exposed Person (PEP), they are automatically assigned a risk score of 100% and classified as High Risk. According to the Anti-Money Laundering (AML) Fraud Management document, the Company retains the discretion to decide whether to accept the registration of such individuals or not.

Both the business risk assessment and the customer-specific risk assessment focus on four primary risk areas. Such primary risk areas are:

3.1 Customer Risk

For the Company, a customer denotes a natural person seeking to initiate or having already established a business relationship with the organization. The degree of risk associated with each customer can vary depending on their profile. The Company exclusively engages with natural persons as customers, and the assessment of risk for such individuals primarily hinges upon their economic activities and/or sources of wealth.

The risk assessment process evaluates the consistency and reliability of the information available about the customer. The verification of client identification details is conducted using methods outlined in the Rules for the Implementation of Anti-Money Laundering (AML). These methods are also applied during the initial assessment of the client's risk profile.

Upon analysis, the Company identifies certain categories of clients or business relationships that pose higher risks, subjecting them to heightened surveillance and implementing additional measures. Transactions involving individuals from countries not fully compliant with international anti-money laundering standards are particularly scrutinized.

In instances where transactions lack reasonable economic justification or appear to lack a legitimate cause, supplementary information regarding the circumstances and purpose of the transaction is diligently collected.

Clients who currently or previously held senior state positions, along with those associated with them, are subjected to significantly heightened scrutiny.

The evaluation of risk associated with a natural person primarily relies on their economic activities and/or sources of wealth. A customer with a consistent, singular source of income is deemed to present a lower risk of Money Laundering (ML) or Financing of Terrorism (FT) compared to those with multiple income sources or irregular income streams. This is attributed to the complexities involved in establishing and verifying multiple income streams and aligning deposited and wagered amounts with disclosed sources of income during ongoing monitoring.

Heightened measures concerning clients may involve requesting additional documents and information, conducting online inquiries, seeking references from counterparties, verifying the source of income with the employer, implementing directives issued by the director of the Financial Intelligence Directorate, or employing other suitable measures.

Certain business or professional activities, from which the customer or applicable beneficial owner derives wealth or funds, pose a heightened risk of ML and FT. These include activities involving substantial amounts of cash, sectors prone to corruption or ML/FT risks (e.g., fire arms trade, defence industry, and mining industry), virtual currencies, or charitable organizations facilitating funds transfer to third countries.

Conversely, some activities present a lower-than-average risk of ML and FT, such as entities listed on regulated markets subject to enforceable disclosure requirements, entities engaged in financial business under effective supervision, or entities within the public administration.

Apart from business activities, other factors contributing to heightened ML/TF risks include individuals seeking residence rights or citizenship through capital acquisitions or individuals associated with Politically Exposed Persons (PEPs) or prominent public positions susceptible to exploitation for personal gain.

3.2 Product, Transaction, and Service Risk

Certain products, services, or transactions inherently hold elevated risks and are attractive to potential criminals. These encompass activities susceptible to exploitation by illicit actors,

such as services enabling customers to influence game outcomes, particularly through collaborative efforts. Additionally, high-risk factors encompass the utilization of specific funding methods, such as cash or anonymous payment mechanisms like prepaid cards or virtual currencies, which afford a degree of anonymity, thereby disrupting audit trails.

An especially high-risk factor entails the extraordinary use of accounts or cards under the guise of third parties. Conversely, when customers transfer funds from their bank accounts or affiliated cards registered in their name with reputable institutions in compliant jurisdictions, the risk of Money Laundering (ML) diminishes.

The risk associated with a product, service, or transaction is contingent upon various factors including transparency, complexity, and value. Products or services affording anonymity, such as nominee accounts, are considered higher risk. Complexity, particularly evident in international transactions involving multiple entities and jurisdictions, amplifies risk. Furthermore, products or services reliant on cash transactions are deemed higher risk compared to those with discernible sources of funds.

In essence, inherent risks are derived from the intrinsic nature of the product, service, or transaction, influenced by factors like transparency, complexity, and cash intensity. Certain activities pose heightened risks of Money Laundering or Financing of Terrorism. Moreover, consideration should be given to whether the product or service facilitates high-value transactions. A payment instrument or account devoid of limits or capping presents a greater risk compared to a similar instrument or account with such constraints. Nonetheless, the extent of these limits or capping measures should also be factored into assessments.

3.3 Delivery Channel Risk

The company's risk exposure in its business relationships or transactions is shaped by the channels utilized for initiation and execution. Channels that offer anonymity inherently elevate the risk of Money Laundering/Financing of Terrorism (ML/FT), unless appropriate mitigating measures are in place. Technological safeguards are deployed to address the heightened risk of identity fraud or impersonation, with additional measures implemented on a risk-adjusted basis to effectively mitigate these risks.

When relying on electronic databases, they can validate whether the provided identification details correspond to an actual individual but may not suffice to ascertain the true identity of the customer. Therefore, supplementary measures, as prescribed in the company's obligations, must be undertaken to verify the accuracy of the player's declared identity.

Interface risk escalates when third parties are involved in customer-licensee interactions, particularly if these third parties lack Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) obligations. The risk varies depending on the extent of the third party's involvement in the licensee-customer relationship. Introducers, such as affiliates directing traffic to the licensee's website, pose a lower ML/FT risk compared to licensees employing physical establishments to expand their network. The challenge with physical

establishments lies in overseeing the funds deposited by customers through them, thereby compromising the licensee's efficacy in applying AML/CFT measures.

Moreover, this risk is contingent on how the subject entity interacts with customers and the channels utilized to deliver specific products or services. While non-face-to-face interactions with customers do not inherently entail a high risk of Money Laundering/Financing of Terrorism (ML/FT), the Company has integrated technological measures into its systems to mitigate the risk of impersonation or identity fraud, thereby reducing the inherent risk in such interactions. In the absence of these systems, the risk is considered high, particularly in cases involving relations mediated through multiple intermediaries. The Company assesses the reliability and AML/CFT standards of these intermediaries and weighs the risk when a customer is referred by an introducer or another entity within the same structure.

3.4 Geographical Risk

The Company proactively maintains awareness of reports issued by FATF sanction list, UN and sanction lists, and country-specific reports to ensure up-to-date assessments of country risk. Consideration is given to customer nationality, residence, and place of birth, as these factors may signal heightened geographical risk.

Customers associated with countries characterized by weak systems for Money Laundering/Financing of Terrorism (ML/FT), inclusion on sanctions lists, a reputation for significant corruption, or sanctions related to terrorism or arms proliferation are classified as high risk. Conversely, those linked to countries posing a low or moderate risk of ML/FT are categorized differently.

The Company evaluates various factors to ascertain geographical risk, including countries and jurisdictions with AML/CFT deficiencies, those flagged by reputable sources such as FATF, MONEYVAL, and IMF for serious AML/CFT shortcomings, countries subject to sanctions by international bodies, and those known to support terrorist activities. Furthermore, countries characterized by high levels of corruption, inadequate tax transparency, and failure to implement beneficial ownership transparency measures are regarded as high risk for ML/FT.

4 Due Diligence Process

Once a deposit is received from a registered customer, thus establishing a business relationship, the Company initiates customer due diligence procedures. This includes verifying the customer's identity and ensuring no duplicate accounts exist under the same name, thereby mitigating the risk of multiple accounts per customer. This verification occurs prior to the customer's initial deposit. Customers are also given the opportunity during this phase to disclose any Politically Exposed Person (PEP) status they may hold.

Upon the customer's first deposit, their details undergo automatic screening against PEP and Financial Sanctions lists. Subsequently, a comprehensive review of the customer's risk assessment is conducted, taking into account the aforementioned factors and provided information. Monitoring is then carried out according to the determined risk level for the customer.

All customer due diligence measures, including those mentioned above and subsequent procedures, are meticulously documented and retained while the business relationship remains active. Furthermore, these records are stored for a minimum of five years following the termination of services, adhering to regulatory requirements, unless an extension is sought or mandated following the submission of a Suspicious Transaction Report (STR).

Customer Due Diligence (CDD) is performed under specific circumstances: when a customer's linked deposits reach a threshold of NAF 4,000 (€2,000), or when a customer is identified as a potential high-risk client. Additionally, full CDD is undertaken when nationality and place of birth details are required, and identity and address verification are carried out through reputable verification services that cross-reference the customer's data with reliable databases.

The verification process necessitates specific documents, including valid, unexpired identification such as a passport, national ID card, residence card, or driving license. Proof of residential address can be established through various means, including recent bank statements, utility bills, official conduct certificates, or other government-issued documents indicating the residential address. Moreover, customers are required to provide evidence of the source of their funds, which may include bank statements, card copies, or documentation from licensed E-wallet backends, demonstrating ownership of the deposit method. Similarly, customers are expected to declare their source of wealth, typically through employment declarations or bank statements evidencing their wealth.

4.1 Enhanced Due Diligence

If a customer is identified and categorized as high-risk, the following procedures must be diligently undertaken:

- **Secondary Identity Verification:** Additional measures for identity verification are imposed, including:
 - Obtaining a certified copy of the customer's identity document from a reputable professional whose credentials can be validated.
 - Cross-referencing customer details with a secondary reliable electronic database.
- **Source of Wealth Verification:** The company must ascertain the legitimacy of the customer's wealth acquisition and provide supporting evidence. Mere customer statements are insufficient. Evidence may include:

- For salary income or company profits: Recent payslips from the employer or financial statements for self-employed individuals.
 - For property sales: Copies of the sales contract.
 - For inheritances: Copies of the will, along with details of the inheritance value.
 - For company sales: Contracts, letters from accountants, or solicitors' statements.
- Source of Funds Verification: The origin of the customer's funds must be established to ensure they are not derived from illicit activities. Deposits should originate from payment methods issued by licensed EEA financial institutions.
 - Confirmation with Payment Providers: Whenever feasible, communication with the payment method provider should be initiated to verify their confidence in the mutual customer's credibility.
 - Enhanced Due Diligence for PEPs: If the customer is identified as a Politically Exposed Person (PEP), a comprehensive evaluation of their reputation is warranted to understand its implications on the associated risk level of the business relationship.

5 Due Diligence Sanctions

Customers are provided with a thirty (30) day timeframe to fulfill Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) requests to the satisfaction of the company. Depending on the risk profile of a customer, certain restrictions may be placed on their account during this period. These restrictions could include limitations on specific deposit or withdrawal methods, or on the use of deposited funds for playing purposes.

Upon the expiration of the initial thirty (30) day period for completing CDD or EDD, if a customer has not fulfilled the requested requirements, it will be deemed that the customer has failed Due Diligence, the Company has every right to close the account. Should a customer be identified as a potential high risk for Money Laundering or Financing of Terrorism (ML/FT), the company will consider initiating a Suspicious Transaction Report (STR) in accordance with the Internal Suspicious Transaction Report Procedure. Subsequent business transactions with such a customer will be suspended unless authorized by the Financial Intelligence Unit (FIU), to whom the Suspicious Report will be reported by the Compliance.

In scenarios where a customer has not completed the CDD/EDD requirements within the stipulated 30-day period but has not been flagged as a potential high risk for ML/FT, their account will be closed. Any remaining deposits will be refunded back to the original deposit method used by the customer, wherever feasible.

