Business Risk Assessment for the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing

1. Introduction

1.1 Overview

The purpose of this Business Risk Assessment (BRA) document is to provide a comprehensive framework for identifying, evaluating, and managing the risks associated with the operations of our online casino. The Business Risk Assessment is a critical component of our online casino's risk management framework. It ensures regulatory compliance, protects our operations, and maintains our reputation and financial stability through the systematic identification, evaluation, and mitigation of risks.

1.2 Management

Intelligent Innovations N.V., a limited liability company incorporated under the laws of Curaçao, with the company number 142065, having registered office at Heelsumstraat 51 Ecommerce Park, Curaçao (hereinafter – the Company) appointed a Compliance Officer as part of the art. 5g of the NOIS.

Compliance Officer, the key individual responsible for the prevention of money laundering and the financing of terrorism, has overall responsibility for ongoing regulatory compliance and anti-money laundering procedures.

1.3 Objectives

The key objectives of the BRA are:

- **Identify Risks:** To systematically identify potential risks that could impact the casino's operations, including but not limited to money laundering, terrorist financing, and other illicit activities.
- **Evaluate Risks:** To assess the likelihood and potential impact of identified risks on the casino's operations and reputation.
- **Mitigate Risks:** To develop and implement effective strategies and controls to mitigate identified risks, ensuring they are within acceptable levels.
- **Compliance:** To ensure full compliance with all relevant regulations and guidelines issued by the Curaçao GCB, maintaining the integrity and credibility of the casino.
- **Continuous Improvement:** To establish a continuous review process for the BRA to adapt to new threats, regulatory changes, and operational modifications.

1.4 Scope

The scope of the BRA encompasses all aspects of the online casino's operations, including:

- **Customer Base:** Evaluating the risk profiles of different customer segments.
- **Products and Services:** Assessing risks related to the various products and services offered by the casino.
- **Delivery Channels:** Identifying risks associated with different channels through which services are delivered to customers.

- **Geographical Risks:** Considering risks related to the geographical locations of customers and operations.

1.5 Importance of the BRA

Conducting a BRA is crucial for several reasons:

- **Risk Awareness:** Increased awareness among employees and management about potential risks and the importance of risk management in protecting the business.
- **Operational Integrity:** Protects the casino from potential operational disruptions caused by risk events.
- **Reputation Management:** Safeguards the casino's reputation by demonstrating a proactive approach to risk management.
- **Regulatory Compliance:** Ensures that the casino meets all regulatory requirements, avoiding legal penalties and preserving its operating license.

1.6 Review and Update

The BRA is a dynamic document that must be reviewed and updated regularly to remain effective. This includes:

- **Annual Review:** Conducting a comprehensive review of the BRA at least once a year.
- **Trigger-Based Review:** Updating the BRA in response to significant changes in the regulatory environment, introduction of new produ cts or services, or other relevant factors.
- **Continuous Monitoring:** Ongoing monitoring of risks and the effectiveness of mitigation measures to ensure continuous improvement.

1.7 Legal Framework

The legal framework for creating a BRA includes the following key documents and acts:

- National Ordinance Reporting Unusual Transactions (NORUT) of November 7, 2017;
- National Ordinance Identification when Rendering Services (NOIS) of October 2, 2017;
- National Ordinance Penalization of Money Laundering (NOPML);
- National Risk Assessment (on) Money Laundering Curaçao 2020;
- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018;
- EU-Directive 2018/1673 Of the European Parliament And Of The Council Of 23 October 2018;
- The FATF Recommendations.
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025;

2. Risk Assessment Methodology

The Risk Assessment Methodology section details the structured approach used to identify, evaluate, and mitigate risks within the online casino's operations. This methodology ensures a comprehensive and systematic assessment of all potential risks, aligning with regulatory requirements and industry's best practices.

The company adheres to the NOIS and NORUT, the GCB Regulations, the EU Fifth Directive, FATF Recommendations, and all other relevant laws and regulations listed above and in our AML Policy. In preparing the BRA, the company considered the guidance provided in the GCB Regulation for combating ML/FT and the proliferation of weapons of mass destruction. Additionally, the AML/CFT National Risk Assessment and sections related to the remote gaming sector are referenced. Other information sources, primarily obtained through desktop research, are also consulted.

2.1 Risk-Based Approach

Our company employs a risk-based approach to risk assessment, focusing on identifying and prioritizing risks based on their likelihood and potential impact. This approach allows us to allocate resources efficiently and implement the most effective risk mitigation strategies. The key elements of our risk-based approach include:

- **Proportionality:** Ensuring that the intensity and scope of risk management efforts are proportionate to the level of risk identified.
- **Focus on High-Risk Areas:** Prioritizing efforts on areas with the highest risk to ensure that resources are directed where they are most needed.
- **Dynamic Adaptation:** Continuously adapting our risk management practices to respond to changes in the risk landscape and emerging threats.
- **Integration with Business Processes:** Embedding risk management into our daily business operations to ensure it is an integral part of our decision-making process.

2.2 Risk Evaluation Criteria

The company employs a methodology where **risk rating (RR)** is calculated by multiplying **likelihood (L)** and **impact (I)**.

likelihood ("L") X impact ("I") = risk rating ("RR").

Risk likelihood refers to the probability of a specific ML/TF/PF risk occurring during regular operations. This can also be seen as the vulnerability of each identified area and the likelihood of it being targeted by criminals. Consequently, some risks are more probable than others.

Risk impact measures potential damage to the company and industry if the identified ML/TF/PF risks materialize without any specific control measures in place.

Inherent risk is determined by multiplying the likelihood of a threat (rated from 1 for low probability to 5 for high probability) by the potential impact (rated from 1 for negligible impact to 5 for severe impact) should the threat occur.

Residual risk refers to the level of risk that remains after the company has applied its risk mitigation measures and controls. It reflects the effectiveness of existing procedures in reducing the identified inherent risks. Residual risk is categorized as Low, Medium, or High, depending on how much the initial (inherent) risk is reduced by implemented safeguards. This evaluation helps determine whether additional controls are necessary or if the current measures are sufficient.

Risk scores are categorized into three levels:

- Low risk: 1 to 4
- Medium risk: 5 to 11
- High risk: 12 to 25

Risk Assessment Matrix			**Impact**				
Low Risk – 1-4 Medium Risk – 5-11			Negligible	Minor	Moderate	Major	Extreme
High Risk – 12-25			**1**	**2**	**3**	**4**	**5**
Likelihood	Very Unlikely	**1**	1	2	3	4	5
	Rarely Occur	**2**	2	4	6	8	10
	Possible	**3**	3	6	9	12	15
	Likely Occur	**4**	4	8	12	16	20
	Occurs Frequently	**5**	5	10	15	20	25

2.3 Categories of Risk Factors

The identified risks are categorized into several key areas to ensure a structured approach to risk management:

- **Customer Risks:** potential risks posed by customers who may engage in illicit activities such as money laundering, fraud, or terrorist financing.
- **Product and Service Risks:** potential vulnerabilities associated with the various gambling products and services offered by the online casino.
- **Delivery Channel Risks:** potential vulnerabilities associated with the various methods through which the online casino's services are provided to customers, including risks associated with different payment methods used by customers.
- **Geographical Risks:** potential threats and vulnerabilities associated with the locations where the online casino operates and where its customers are based.
- **Employee Risks:** potential threats and vulnerabilities posed by the casino's staff, which can impact operational integrity and compliance.

3. Risk factors

Risk Factor	Likelihood	Impact	Risk Score	Inherent Risk	Mitigation Measures and Controls	Residual Risk
Customer Risks						
Using gambling products and services by criminals to store and move the proceeds of crime.	3	4	12	H	The company's AML policy includes Adverse Media and Sanctions Lists checks within CDD and ongoing monitoring to assess user backgrounds and prevent criminals from accessing products and services.	M
Laundering of proceeds from criminal activity by sanctioned individuals or entities	1	5	5	M	The company's AML policy includes Sanctions Lists checks within CDD and ongoing monitoring. Any new or existing customer found on sanction lists is assigned a High-risk status, leading to the rejection of their registration or the closure of their account.	M
PEPs using casinos to clean criminal funds	2	4	8	M	The company's AML policy includes PEP checks within CDD and ongoing monitoring. Any new or existing customer identified as a PEP or a relative of a PEP is assigned a High-risk status, resulting in the rejection of their registration or the closure of their account.	M
Customers who login or reside in high-risk jurisdictions pose significant risks due to the higher prevalence of financial crimes and weaker regulatory environments in these areas.	2	4	8	M	The company's AML policy prohibits registration and usage of accounts from high-risk jurisdictions. Access to the website from these jurisdictions is restricted by IP addresses, and CDD is applied at the registration stage to refuse registration for residents of high-risk jurisdictions.	L

Organized crime gangs transfer illicit funds through third-party bank accounts (known as 'money mules') to obscure the audit trail of transactions.	4	4	16	H	The company's AML policy includes adverse media and sanction lists checks within CDD and ongoing monitoring to assess user backgrounds and prevent criminals from accessing services. Additionally, all payment methods used for deposits and withdrawals are verified. Any doubts about the adequacy or veracity of user-provided documents or information result in High-Risk status and EDD. The use of payment methods that do not belong to the account owner is prohibited.	M
Customers may deposit funds and leave their accounts dormant for an extended period, then withdraw the funds later with minimal activity, attempting to distance themselves from their crimes over time.	3	3	9	M	The company has terms and conditions regarding dormant accounts that customers must agree to upon registration. If an account is unused for 12 months, a monthly administrative fee is charged. For continued inactivity, the company may notify the customer via email about potential account termination and request the withdrawal of remaining funds.	M
Customers may open multiple accounts using different names and identities, making it difficult to verify the real account holder (beneficial owner) and/or the source of the funds.	3	3	9	M	The company's AML policy mandates documentary verification at the registration stage for all users. Any doubts about the adequacy or veracity of the provided documents result in a High-Risk status assignment and EDD. The verification process includes a liveness check selfie to reduce the risk of using third-party documents to register multiple accounts. Additionally, the company conducts multiple account checks by analyzing IP addresses and device fingerprints to identify and prevent the creation of multiple accounts by the same individual.	L
Individuals using multiple payment methods to fund their accounts without a clear rationale may be attempting to structure deposits and move illicit funds undetected. The use of various payment methods allows customers to shift funds easily between different platforms or bank accounts, potentially using both refundable and non-refundable options.	4	4	16	H	We enforce a closed-loop policy where winnings are paid back to the original deposit source whenever possible. Withdrawal requests that appear to circumvent these controls are investigated by our Risk & Fraud teams. If needed, we require proof of bank account ownership before processing payments. Additionally, our ongoing monitoring system flags attempts to use multiple payment types for further investigation.	M

A significant and sudden increase in betting activity, beyond what is considered normal for a specific customer, may indicate that the account is being used for money laundering, either by the customer or on behalf of someone else.	3	4	12	H	Customers are monitored around the clock, and certain red flags are triggered when a customer’s betting behavior dramatically increases. The AML team reviews such accounts where necessary, and further CDD or EDD is conducted as appropriate.	M
A customer who changes personal details such as their residential address, email, or phone number poses a higher money laundering or terrorist financing risk, especially if the updated information is not promptly shared with the operator. This can compromise ongoing monitoring, including sanctions screening or EDD checks.	2	3	6	M	We adopt a risk-based approach requiring customers to periodically confirm their information based on their risk rating. Customers are restricted in what information they can change independently and are required to contact customer support and provide evidence, such as proof of address, for significant changes.	L
High-value deposits may represent proceeds from criminal activities that customers intend to launder or spend through the casino's platform	3	3	9	M	EDD is required for customers who reach certain financial thresholds or whose behaviors escalate their risk rating. SOF and, in some cases, SOW are required to justify large deposits.	M
There is a risk that customers could transfer proceeds of crime between accounts held with the same operator, either to obscure the money trail or to facilitate payments for goods or services related to criminal activity.	1	4	4	L	Our platform does not allow customers to transfer funds between themselves. Only deposits and withdrawals are permitted to and from a customer’s own account, ensuring no direct customer-to-customer transactions can occur.	L
Customers may attempt to evade CDD requirements by making numerous low-level transactions to avoid detection and minimize suspicion, a practice known as smurfing.	3	4	12	H	Each player's behavior is continuously monitored for money laundering indicators. Suspicious transactional and gambling patterns are scored and combined with other red flags for money laundering or terrorist financing. Users exhibiting suspicious transactions are flagged as High-Risk. We utilize a set of financial and behavioral thresholds that trigger additional KYC, CDD, or EDD checks when necessary.	M

The accessibility of multiple online casinos allows customers to spread their gambling activity across different operators, potentially falling below each operator's internal reporting thresholds, which may lead to the evasion of scrutiny despite significant overall gambling activity.	2	3	6	M	During onboarding CDD or any subsequent checks, if a customer provides documentation (e.g., bank statements) indicating high gambling activity across multiple casinos, we closely review this information and apply necessary measures or restrictions to manage the risk.	L
Product and Service Risks						
Peer-to-peer gaming allows customers to transfer money to one another, creating the potential for money laundering.	3	5	15	H	The company does not offer peer-to-peer gaming, ensuring that all gameplay is conducted directly between players and the platform. This eliminates the risk of users transferring funds to each other, reducing opportunities for money laundering.	L
Customers could deposit illicit funds into their account and then withdraw them without wagering, engaging in minimal play or low-risk betting activity.	4	4	16	H	To prevent withdrawals without gameplay, wagering requirements and monitoring betting activity for minimal play or low-risk patterns are imposed. EDD is applied to accounts showing suspicious deposit and withdrawal behavior, ensuring funds are used for legitimate gaming.	M
The risk of multiple accounts includes the potential for users to engage in fraudulent activities, such as bonus abuse, or money laundering. By opening multiple accounts, individuals can obscure their identity, evade limits, and manipulate transactions to bypass anti-fraud and AML controls. This increases the difficulty of monitoring player behavior and identifying suspicious activity.	3	4	12	H	The company prevents the creation of multiple accounts by implementing KYC procedures, requiring verification, and using an in-built system to detect duplicate accounts which lead to account closure in case any are found. Additionally, IP tracking and monitoring for suspicious patterns and behavior associated with multiple account creation is used.	M
The use of accounts or cards registered in the names of third parties may facilitate fraudulent activities, including identity theft and financial fraud, as it obscures the true identity of the user	3	4	12	H	To minimize such risks, the company implements verification procedures for payment methods. This includes conducting thorough checks to confirm that payment methods are registered in the customer's name and verifying the identity of the cardholders.	M

and complicates the tracking of illicit transactions.						
Unregulated betting events pose risks such as increased vulnerability to fraud, manipulation, and money laundering. Without oversight, there is a higher chance of illicit activities, including the fixing of outcomes and lack of player protection.	2	3	6	M	The company uses a trusted bookmaker and regularly reviews markets, odds and services offered to all customers to minimize risks.	L
Delivery Channel Risks						
Peer-to-Peer Transactions between players enable funds to be exchanged directly, potentially bypassing the casino's AML monitoring systems.	3	4	12	H	The casino prevents such transactions by making this process impossible by not providing such services.	L
Unverified E-Wallets allow users to fund accounts without direct verification, making it difficult to trace the source of the funds or the customer’s identity.	3	3	9	M	The casino applies verification measures for e-wallet users based on a risk-based approach, ensuring that accounts are connected to verified identities.	M
Cash deposits are difficult to trace and can be used to launder money.	4	4	16	H	The company does not accept cash deposits as part of its risk mitigation strategy. Deposits must be made through regulated and traceable payment methods that comply with AML/CFT regulations.	L
Gift cards, especially those purchased with cash, can be used anonymously for deposits. They are difficult to trace back to the purchaser, enabling criminals to convert illicit funds into casino credits.	2	3	6	M	The casino restricts the use of gift cards for deposits to minimize the risk of anonymous transactions. By limiting or prohibiting the use of gift cards, we ensure that all deposits are made through traceable and verified payment methods, reducing the likelihood of money laundering and other fraudulent activities.	L
Third-party deposits, where funds are transferred from an account or payment method not directly linked to the customer, increase the risk of anonymity. These transactions can	3	4	12	H	The Company does not allow third-party deposits, including those made by friends, relatives, or partners. Deposits must originate from an account, payment system, or credit card registered in the customer’s name. Only personal payment details linked to the verified account	M

obscure the true source of funds and the identity of the customer, making it easier for individuals to engage in money laundering or fraudulent activities.					holder are permitted for deposits, ensuring compliance with security and regulatory requirements.	
Non-face-to-face interactions, such as online account registration and transactions, pose an elevated risk of identity fraud, impersonation, and the use of false credentials.	4	4	16	H	The Company mitigates the risks associated with non-face-to-face interactions by implementing identity verification, geolocation tracking, and biometric verification (Facial Recognition). These controls ensure that customers' identities are accurately verified and monitored, reducing the risk of fraud or impersonation during remote interactions.	M
Geographical Risks						
Customers from jurisdictions known for weak AML/CFT regulations or high levels of corruption may attempt to use the casino for money laundering or other illicit activities. These jurisdictions might lack robust regulatory oversight, making it easier for criminal elements to operate.	3	5	15	H	Implementing geographical restrictions on account registrations and transactions, conducting EDD on customers from high-risk jurisdictions, including thorough KYC checks and monitoring for suspicious transactions considering information produced by the FATF and non-governmental well-known bodies.	M
International politically exposed persons (PEPs) may utilize casinos to launder illicit or criminal funds. Due to their prominent public positions and access to substantial financial resources, PEPs may engage in transactions that obscure the origins of their funds, increasing the potential for money laundering.	3	5	15	H	The casino implements enhanced due diligence measures and may refuse registration for customers identified as politically exposed persons (PEPs).	M
There is a risk that a customer may attempt to transfer funds to a destination outside of their country of residence to obscure the origin and/or destination of the funds. This risk is	3	5	15	H	The casino conducts thorough due diligence on transactions, including verifying the source of the funds and assessing the risk associated with the sending and receiving countries.	M

heightened when payments originate from high-risk jurisdictions.						
Countries that are subject to international sanctions related to terrorism or the proliferation of weapons of mass destruction pose significant risks. Engaging with individuals or entities from these jurisdictions can lead to potential legal repercussions and regulatory violations.	2	4	8	M	We adhere to international sanctions by conducting thorough screening of customer registrations and transactions against updated sanctions lists. Any connections to sanctioned countries result in immediate account restrictions and reporting to relevant authorities to ensure compliance.	M
The geographical location of players may pose risks related to regulatory compliance and increased vulnerability to fraudulent activities. Players in jurisdictions with weak AML/CFT regulations or high levels of corruption may attempt to exploit the casino for money laundering or other illicit activities.	3	4	12	H	Use of IP or geolocation masking technologies, including VPNs and proxy servers, is discouraged. Accounts may be closed, and any associated bets, bonuses, or winnings may be voided if these methods are detected.	M
Employee Risks						
Operators may not adhere to legislation and guidance regarding the prevention of money laundering and terrorist financing.	4	5	20	H	The company maintains a comprehensive AML policy dedicated to upholding the highest standards in preventing money laundering and terrorist financing.	M
The operator sets high limits to bypass the requirements for customer due diligence (CDD) and enhanced due diligence (EDD).	4	4	16	H	The company employs a multifactor risk score calculation system that evaluates each user's risk score based on various factors, rather than solely on monetary thresholds. This approach effectively identifies high-risk users and facilitates the performance of enhanced due diligence.	L
Gambling operations may be conducted by organized criminals to facilitate money laundering.	3	4	12	H	The company mandates that all employees, including key management, undergo thorough screening prior to employment to ensure they are suitable for their roles and do not have a criminal background.	M
Operators may depend on payment providers to carry out KYC checks, which can result in	2	3	6	M	The AML policy outlines a comprehensive system of KYC procedures that the company independently implements. This system ensures that all	L

inadequate verification processes and increased exposure to money laundering risks.					customer verification processes are conducted internally and do not rely on checks performed by payment providers, thereby enhancing the effectiveness of the KYC measures and reducing potential vulnerabilities.	
Operators may stake and win directly or indirectly on their own products, creating potential conflicts of interest and compromising the integrity of the gaming environment.	2	3	6	M	The company has a policy that prohibits employees from using the services, thereby eliminating the risk of insider influence and maintaining a fair playing field for all customers.	L
Operators may implement a generic ‘one size fits all’ approach to their Risk Assessment, which fails to account for the specific money laundering (ML) and terrorist financing (TF) risks relevant to their particular operations.	4	4	16	H	The casino employs a tailored risk-based approach for all aspects of ML, TF, and PF prevention, ensuring that the Risk Assessment accurately reflects the unique risks associated with its business model.	M
There may be a failure to adequately align the Risk Assessment with the Commission’s standards and to stay current with evolving regulations in alternative jurisdictions. This oversight can result in ineffective policies, procedures, and controls if the overarching Risk Assessment is lacking.	4	4	16	H	Documentation utilized in the creation and ongoing maintenance of this Risk Assessment is provided at the beginning of this document, ensuring that the casino remains compliant with applicable legislation and can effectively adapt to fluctuating standards.	M
License holders may demonstrate insufficient knowledge, raising concerns about their competence and integrity in managing operations.	3	4	12	H	Senior members of the AML team have completed relevant AML courses and obtained certifications to enhance their expertise and ensure they possess the necessary knowledge to fulfill their roles effectively.	M
There may be a failure to provide staff, including Money Laundering Reporting Officers and Nominated Officers, with regular and high-quality training on AML practices.	2	4	8	M	All employees undergo comprehensive training during their induction and receive annual refreshers. Additionally, any significant updates related to money laundering, terrorist financing, or proliferation financing are communicated and trained on an ad hoc basis to ensure staff remain well-informed.	L

The organization may lack sufficient 'Know Your Employee' (KYE) data, leading to inadequate understanding of employee backgrounds and integrity.	3	4	12	H	Before hiring employees, the company conducts relevant integrity checks aligned with their roles, responsibilities, and access levels. The organization does not employ individuals deemed unfit or improper, with senior staff undergoing more rigorous scrutiny than junior staff to ensure higher standards of integrity.	M
A static and ineffective approach to customer risk profiling and enhanced due diligence may fail to identify evolving or current risks, compromising the effectiveness of AML measures.	3	4	12	H	Customers undergo continuous risk assessment throughout the entire business relationship. Risk profiling considers various factors, and risk ratings are updated dynamically based on ongoing monitoring of transactions and behaviors, allowing for timely identification and response to emerging risks.	M

Responsible department for oversight:

Compliance function