
BETS ENTERTAINMENT N.V.

BUSINESS RISK ASSESSMENT FOR THE PREVENTION OF
MONEY LAUNDERING, TERRORIST FINANCING AND
PROLIFERATION FINANCING

April 2025

Date	Version	Approved by: Glenn C. Rellum, o.b.o Downtown E-Commerce Company B.V.
April 9, 2025	1.0	

1. INTRODUCTION

1.1. OVERVIEW

Bets Entertainment N.V. (hereinafter “Bets Entertainment” or the “Company”) is incorporated under the laws of Curaçao with company number 155648 and has its registered office at Zuikertuintjeweg Z/N (Zuikertuin Tower), Willemstad, Curaçao. The Company operates under license number OGL/2024/1178/0479 issued by the Curaçao Gaming Authority on July 29, 2024.

The purpose of this Business Risk Assessment (hereinafter “BRA”) is to establish a comprehensive framework for identifying, evaluating, and managing the risks associated with the operations of Bets Entertainment. As a critical component of the Company’s risk management framework, the BRA ensures regulatory compliance, safeguards operations, and upholds the Company’s reputation and financial stability through the systematic identification, evaluation, and mitigation of risks.

The Compliance Officer is the key individual responsible for preventing Money Laundering and the Financing of Terrorism and holds overall responsibility for ongoing regulatory compliance and Anti-Money Laundering (AML) procedures.

1.2. OBJECTIVES

The key objectives of the BRA are to systematically identify potential risks that could affect the casino’s operations, including money laundering, terrorist financing, and other illicit activities; evaluate the likelihood and potential impact of these identified risks on the casino’s operations and reputation; develop and implement effective strategies and controls to mitigate these risks, ensuring they remain within acceptable levels; ensure full compliance with all relevant regulations and guidelines issued by the Curaçao Gaming Authority (hereinafter “CGA”) to maintain the integrity and credibility of the casino; and establish a continuous review process for the BRA to adapt to new threats, regulatory changes, and operational modifications.

1.3. SCOPE

The scope of the BRA includes all aspects of the online casino’s operations, such as evaluating the risk profiles of different customer segments, assessing risks related to the various products and services offered, identifying risks associated with the delivery channels used to provide services to customers, and considering geographical risks linked to the locations of customers and operations.

1.4. SIGNIFICANCE OF THE BRA

Conducting a BRA is essential for several reasons: it enhances risk awareness among employees and management, emphasizing the significance of risk management in safeguarding the business; it protects the casino from potential operational disruptions caused by risk events; it helps maintain the casino’s reputation by showcasing a proactive approach to risk management; and it ensures compliance with regulatory requirements, thereby avoiding legal penalties and preserving the operating license.

1.5. REVIEW AND UPDATE

The BRA is a dynamic document that requires regular review and updates to maintain its effectiveness. This process includes conducting a comprehensive review of the BRA at least once a year, updating the document in response to significant changes in the regulatory environment, the introduction of new products or services, or other relevant factors, and continuously monitoring risks and the effectiveness of mitigation measures to ensure ongoing improvement.

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 CGA Regulations, the EU AML Directives, FATF Recommendations, and all other relevant laws and regulations listed in our AML Policy. In preparing the BRA, the company considered the guidance provided in the CGA 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.

2.1. RISK-BASED APPROACH

The 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)**.

$$\text{likelihood ("L")} \times \text{impact ("I")} = \text{risk rating ("RR")}$$

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.

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			Negligible	Minor	Moderate	Major	Extreme
Medium Risk – 5-11							
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.

3. RISK FACTORS

Risk factor	Likelihood	Impact	Risk Score	Inherent Risk Rating	Control framework
Customer Risks					
Criminals may use gambling products and services to store and move proceeds from illegal activities	3	4	12	H	Customer Due Diligence (CDD) measures are integral to the AML policy, employing risk-based assessments to identify and monitor customers potentially using gambling services for illegal activities, with transaction monitoring systems in place to flag suspicious behaviours.
Sanctioned individuals or entities may launder proceeds from criminal activities through casinos	1	5	5	M	Sanctions screening occurs at the onboarding stage, ensuring customers are checked against relevant sanctions lists, with ongoing monitoring to detect any changes in their status.
Politically exposed persons (PEPs) may utilize casinos to launder illicit funds	2	4	8	M	Enhanced Due Diligence (EDD) measures are applied to PEPs, requiring verification of source of funds and management approval for onboarding, alongside regular transaction monitoring and biannual reviews of PEP profiles.
Customers logging in from high-risk jurisdictions pose significant risks due to higher financial crime prevalence and weaker regulatory environments	2	4	8	M	Registration and account access from identified high-risk jurisdictions are subject to geo-blocking, with enhanced due diligence required for customers logging in from these areas, including proof of residence and monitoring for VPN usage.
Organized crime gangs may transfer illicit funds through third-party accounts (money mules) to obscure transaction trails	4	4	16	H	Third-party transactions are closely monitored, with systems in place to flag mismatched names on accounts and payment methods. Any suspicious patterns trigger investigations and potential blocking of third-party payments.
Customers might deposit funds and leave accounts dormant for extended periods, later withdrawing funds to distance themselves from criminal activities	3	2	6	M	Dormant accounts are flagged for inactivity after 6–12 months, with KYC re-verification required before any withdrawals, alongside regular checks for unusual login attempts or changes in ownership.
Multiple accounts opened under different names may hinder the verification of the actual account holder and the source of funds	3	3	9	M	Mechanisms for detecting multiple accounts involve KYC checks, device fingerprinting, and AI tools to identify pattern similarities, with strict verification processes to confirm the beneficial ownership of accounts.
Individuals using various payment methods without clear rationale may be structuring deposits to move illicit funds undetected	4	2	8	M	Bets Entertainment allows multiple payment methods for customer convenience, but monitors for inconsistent payment behaviour and flags any frequent changes or mismatches in payment sources for further investigation.

A sudden increase in betting activity beyond a customer's normal pattern may indicate potential money laundering.	2	2	4	L	Significant increases in betting activity are identified through monitoring systems that flag large spikes or deviations from normal betting patterns, with responses including transaction holds and reviews of source of funds.
Customers changing personal details without promptly notifying the operator pose higher risks for money laundering or terrorist financing, complicating ongoing monitoring.	2	3	6	M	Changes in personal details trigger automatic alerts for manual review, requiring verified documentation for updates, especially for high-risk changes that may indicate attempts to evade detection.
High-value deposits may indicate attempts to launder proceeds from criminal activities through the casino.	2	3	6	M	High-value deposits are subject to additional scrutiny, with thresholds set for enhanced due diligence, including verification of source of funds and background checks against sanctions and PEP lists.
Customers could transfer proceeds of crime between accounts with the same operator to obscure the money trail or facilitate payments for illicit goods or services.	1	4	4	L	Transfers between accounts held by the same operator are monitored for unusual patterns, with identity verification required for both parties involved in the transfer to ensure transparency.
To evade CDD requirements, customers may engage in numerous low-value transactions, a practice known as smurfing.	3	4	12	H	Controls for detecting smurfing include automated monitoring for frequent low-value transactions near reporting thresholds, with cumulative limits set to mitigate risks of structuring.
The availability of multiple online casinos allows customers to spread gambling activity across different operators, potentially avoiding internal reporting thresholds and scrutiny despite significant overall activity.	2	3	6	M	Cross-platform gambling activity is monitored through shared data networks to identify rapid account creation and similar usage patterns across multiple casinos, with alerts for suspicious behaviours.
Individuals with a history of gambling addiction may attempt to register or access accounts, posing risks to themselves and the casino's compliance obligations.	3	2	6	M	Measures to prevent access by individuals with a history of gambling addiction include checks against self-exclusion lists and monitoring for indicators of problematic gambling behaviour, prompting interventions when necessary.
Individuals engaging in frequent account manipulation may indicate attempts to evade detection or compliance measures.	3	2	6	M	Monitoring systems are implemented to track account manipulation patterns, flagging suspicious changes for further investigation and manual review.
High-risk affiliates or marketing partners may attract high-risk customers, increasing exposure to money laundering or fraud.	4	3	12	H	Due diligence processes for high-risk affiliates and marketing partners involve KYC checks, risk assessments based on their business models, and ongoing monitoring of player quality to prevent attracting high-risk customers.
Product and Service Risks					
Peer-to-peer gaming enables customers to transfer funds to each other, increasing the risk of money laundering.	3	5	15	H	Peer-to-peer gaming activities are monitored for unusual betting patterns or collusion, with limits imposed on stakes and transfers between players to mitigate risks of money laundering.
Customers may deposit illicit funds and withdraw them without wagering, often engaging in minimal play or low-risk betting.	4	4	16	H	Detection measures for customers depositing illicit funds without wagering engage monitoring systems to flag accounts with large deposits and minimal play, leading to manual review processes.
Multiple accounts can facilitate fraudulent activities like bonus abuse and money laundering, allowing users to obscure their	3	4	12	H	Multiple account detection systems employ KYC checks, device fingerprinting, and AI-driven behaviour analysis to identify and block fraudulent activities, with strict enforcement of identity verification.

identities, evade limits, and manipulate transactions, making it difficult to monitor behaviour and identify suspicious activity.					
Accounts or cards registered in third-party names can lead to fraudulent activities, such as identity theft and financial fraud, by obscuring the true identity of users and complicating the tracking of illicit transactions.	3	4	12	H	The use of third-party accounts is restricted, with verification of ownership required for all payment methods. Transactions involving accounts not matching the customer's name are flagged for compliance review.
Unregulated betting events heighten risks of fraud, manipulation, and money laundering, with increased chances of illicit activities and inadequate player protection.	2	3	6	M	Bets Entertainment avoids unregulated events, implementing a risk scoring system and oversight mechanisms to ensure compliance with regulatory standards.
The use of cryptocurrencies for transactions may facilitate anonymous, untraceable financial activities	3	4	12	H	The company limits or prohibits the use of cryptocurrencies that lack clear regulatory oversight, requiring strict verification processes for any transactions that are permitted. Cryptocurrency transactions are monitored using blockchain analytics, with stringent KYC requirements and ongoing surveillance of high-risk wallets to mitigate potential abuse.
Time-limited promotions encouraging high stakes may lead to impulsive gambling behaviour, increasing the risk of addiction or financial crime.	2	3	6	M	Bets Entertainment reviews promotional campaigns for responsible gambling standards, setting deposit limits and monitoring for impulsive betting behaviour, with interventions in place for at-risk players.
High-risk game types and features may be exploited for money laundering due to their potential for quick wins and losses.	2	3	6	M	Bets Entertainment evaluates game types and features regularly, implementing monitoring for suspicious activity in high-risk games and adjusting limits or restrictions as needed.
Delivery Channel Risks					
Peer-to-peer transactions allow players to exchange funds directly, potentially evading the casino's AML monitoring.	3	4	12	H	Tracking of peer-to-peer transactions involves monitoring frequency and size of exchanges, with KYC verification required to ensure compliance and reduce risks.
Unverified e-wallets enable account funding without direct identity verification, complicating the tracing of fund sources.	3	3	9	M	Bets Entertainment blocks unverified e-wallets, requiring comprehensive identity verification before acceptance for funding accounts, alongside monitoring for high-risk transaction patterns.
Cash deposits are challenging to trace and can facilitate money laundering.	4	4	16	H	Cash deposits are not accepted, with all deposits required to be made through regulated, traceable payment methods that comply with AML/CFT regulations.
Gift cards purchased with cash can be deposited anonymously, making it hard to link them back to the buyer and enabling the conversion of illicit funds into casino credits.	2	3	6	M	Gift card deposits are treated as high-risk, requiring KYC verification before acceptance, and monitored for patterns that may indicate misuse or fraud.
Third-party deposits obscure the true source of funds and customer identity, increasing the risk of money laundering and fraud.	4	3	12	H	Third-party deposits are restricted, requiring verification of ownership for all payment methods. Transactions involving non-matching accounts are flagged for compliance review.

Non-face-to-face interactions, such as online registrations and transactions, heighten the risk of identity fraud and use of false credentials.	5	4	20	H	KYC checks during online registrations involve biometric verification and cross-referencing data with fraud databases to prevent identity theft and ensure accurate identification.
Marketing campaigns through social media and influencers may attract high-risk customers or promote unhealthy gambling behaviours.	3	4	12	H	Marketing campaigns are evaluated for compliance with responsible gambling standards, ensuring that promotions do not target vulnerable populations while being monitored for spikes in high-risk sign-ups.
Inadequately secured online platforms may expose customer data or allow unauthorized access, leading to potential identity fraud or financial crime.	4	3	12	H	Bets Entertainment implements robust cybersecurity measures, including encryption, regular security audits, and access controls, to protect customer data and prevent unauthorized access.
Geographical Risks					
Customers from jurisdictions with weak AML/CFT regulations or high corruption may attempt to launder money through the casino due to insufficient oversight.	3	5	15	H	Customers from jurisdictions with weak AML/CFT regulations undergo stringent identification checks against FATF lists, with additional EDD measures implemented to mitigate associated risks.
International PEPs may use casinos for high-value transactions to obscure the origins of illicit funds linked to their public positions.	3	5	15	H	Transactions involving international PEPs are subject to enhanced scrutiny, requiring thorough verification of source of funds and ongoing monitoring of high-value transactions, with alerts triggered for any unusual activity that deviates from expected patterns.
Customers might transfer funds to foreign destinations to conceal their origins, particularly from high-risk jurisdictions.	3	5	15	H	Fund transfers to foreign destinations are monitored closely, with identity verification required for all outbound transactions, alongside regular reviews of transaction patterns to detect any potential money laundering activities.
Engaging with individuals or entities from countries under international sanctions related to terrorism or weapons proliferation poses significant legal and regulatory risks.	2	4	8	M	Bets Entertainment implements strict sanctions screening processes, ensuring that all customers and transactions are checked against relevant sanctions lists, with immediate blocking of any engagements with sanctioned individuals or entities and mandatory reporting to regulatory authorities.
Players in jurisdictions with weak AML/CFT regulations may exploit the casino for money laundering and other illicit activities, raising compliance concerns.	3	4	12	H	Customers from jurisdictions with weak AML/CFT regulations undergo stringent identification checks against FATF lists, with enhanced due diligence measures applied to monitor account activity closely. Continuous risk assessments are conducted to adapt compliance measures as needed to mitigate potential risks associated with these jurisdictions.