

BUSINESS RISK ASSESSMENT FOR BOOST GAMING B.V.

Version updates

Prepared by	Date	Version
Compliance Officer/ MLRO	12.05.2025	1.0 – Created

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 1 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

1. General.

Title	BUSINESS RISK ASSESSMENT
Type	Policy
Version	1.0
Created on	1 st of May 2025
Created by	MLRO
Next Review	Annually or upon significant business changes

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 2 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

Contents

1. General.	2
2. Scope.	2
3. Overview.	2
4. Purpose and risk appetite statement	3
5. Identifying and assessing the Risks.	3
6. Risk Categories.	4
7. Matrix and Risk Score for Probability, Impact, and Residual Risk.	5
8. Customer and Transaction Risk	6
8.1 Remote Operator Risk.	6
8.2 Multiple platforms and accounts.	6
8.3 Customer profile and gambling habits.	6
8.3.1 Politically Exposed Persons.	6
8.3.2 Third parties/nominees.	7
8.3.3 High Spenders.	7
8.3.4 Sanctioned/designated persons.	7
8.3.5 Suspicious transactional behaviour.	8
8.4 Controls for Customer and Transaction Risk.	9
8.5 Customer and Transaction - Overall Inherent and Residual Risk.	16
9. Product Risk.	18

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 2 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

9.1 Controls for Product Risk.	18
9.2 Product - Overall Inherent and Residual Risk.	22
10. Payment Risk	22
10.1 Remote Operator Risk.	22
10.2 Payment Methods.	23
10.2.1 Bank Account Methods.	23
10.2.2 Mobile Payment Method.	23
10.2.3 E-wallets Payment method.	23
10.2.4 Anonymous Payment Method.	24
10.3 Controls for Payment Risk.	23
10.4 Payment Method – Overall Inherent and Residual Risk.	25
11. Geographical Risk.	26
11.1 High Risk Jurisdictions.	26
11.2 Controls for Geographical Risk.	27
11.3 Geographical - Overall Inherent and Residual Risk.	28
12. Employee Risk.	29
12.1 Controls for Employee Risk.	29
12.2 Overall Employee Inherent and Residual Risk.	32
13. Conclusion.	33

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 3 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

2. Scope.

This policy supports the implementation of a risk-based approach (RBA) and assesses the ML and TF risks of the business operated by Boost Gaming B.V.

3. Overview.

Due to legal and license requirements, Boost Gaming B.V. must implement measures as described in the Curacao laws. Being a Curacao online gaming operator, (Boost Gaming B.V. is also subject to the following regulations:

- Curacao Gaming Board Regulations for AML/CFT
- National Ordinance on Identification when rendering services (N.G 2017, no 92)
- NORUT – National Ordinance on the Reporting of Unusual Transactions (N.G 2017, no 99)
- Sanctions National Ordinance (N.G 2014, no 55)
- Kingdom Sanction Act (N.G 2016, no 54)
- National Decree entering into force of Kingdom Sanction Law (N.G 2017, no 2)
- The Code of Criminal Law (Penal Code) N.G 2011, no 48)
- Financial Action Task Force (FATF) and Caribbean Financial Action Task Force (CFATF)
- National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63) (NOOGH).
- National Ordinance for Games of Chance (LOK)

The legal provisions require operators to have a policy and procedure in relation to risk assessment and management. The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:

- identify the money laundering and terrorist financing risks that are relevant to the operator.
- design and implement policies and procedures to manage and mitigate these assessed risks.
- monitor and improve the effective operation of these controls, and
- record what has been done, and why.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 2 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

4. Purpose and risk appetite statement

The purpose of the risk assessment is to set out three objectives

1. To provide comprehensive information about threats, vulnerabilities, and risks on the Curacao gambling market.
2. To comply with the regulatory framework for AML and CFT with the aim to report suspicious transactions to competent authorities while avoiding dealing with criminal proceeds in an illegitimate manner

To provide support in the work of the Authority through risk-based oversight.

Boost Gaming B.V. places great importance on compliance and has little or no tolerance or appetite for any non-compliance with the regulatory framework to which it is subject. Boost Gaming B.V. strives to avoid its risk appetite and tolerance resulting from non-compliance. Boost Gaming B.V. aims to avoid risk resulting from a lack of ethical or professional standards or compliance culture, fraud, or bribery. The residual risk generally matches the Company's risk tolerance, subject to ongoing business risk assessments. The Company is committed to continuing to ensure that the residual risk benefits from continuous efforts to maintain effective controls. The Company is determined to maintain a compliant risk culture in which the propensity to take risk is low/medium and the propensity to exercise control is high.

5. Identifying and assessing the Risks.

Boost Gaming B.V., as a Curacao operator, assesses its risks in the context of how it is most likely affected by money laundering or terrorist financing. To define the risks, it is necessary to identify risk variables. An overall view of the risk variables will show the risk of money laundering and terrorist financing.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 3 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

6. Risk Categories.

Boost Gaming B.V.'s Compliance Officer/MLRO conducts an AML & CTF risk assessment (Risk Assessment), which is reviewed on an annual basis, and on an ad-hoc basis, by the Directors.

The Risk Assessment will seek to identify the potential risks to Boost Gaming B.V. in the following areas:

- Customer and Transaction risk.
- Product Risk
- Geographical risk.
- Payment risk.
- Employee risk.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 4 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

7. Matrix and Risk Score for Probability, Impact, and Residual Risk.

The probability of a risk occurring and the impact these risk events will have on the business were brought together in a table below. By using this Table, it is possible for each risk factor considered to be given a level of importance that is based on the probability and impact assigned to each individual risk factor.

	Very Likely	Low-Medium	Medium	Med-High	High	High
	Likely	Low	Low-Medium	Medium	Med-High	High
Probability	Moderate	Low	Low-Medium	Medium	Med-High	Med-High
	Unlikely	Low	Low-Medium	Low-Medium	Medium	Med-High
	Rate	Low	Low	Low-Medium	Medium	Medium
	Risk Eliminated	No Risk	No Risk	No Risk	No Risk	No Risk
		Insignificant	Minor	Moderate	Major	Severe
		Impact				

All customers of (XXXXX) are categorised according to their AML/CFT risk. Customers posing the highest risks receive the highest attention.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 5 of 37
------------	-----------------------------	----------------	---	-----------------	-------------------------	---------------------

8. Customer and Transaction Risk

8.1 Remote Operator Risk.

All user's data is recorded, such as name, social security number, address, age, nationality, copy of the passport, bank account, etc. but every step that the user takes is recorded, down to the time at which a button is clicked. A seamless record of their gaming behaviour can be retrieved at any time and analysed at length, if necessary. In addition, online gaming behaviour is entirely transparent.

8.2 Multiple platforms and accounts.

Boost Gaming B.V. does not allow customers to hold more than one account as per our terms and conditions, therefore this risk factor is not applicable to Boost Gaming B.V. .

8.3 Customer profile and gambling habits.

The company only provides gaming accounts to individuals.

Categories of customers whose activities may indicate a higher risk include:

8.3.1 Politically Exposed Persons.

A PEP is a person who is or has at any time been entrusted with prominent public functions by a state, a community institution (for example, the European Parliament), or an international body (for example, the United Nations), including the following persons:

- heads of state, heads of government, ministers, and deputy or assistant ministers
- members of parliament
- members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.
- members of courts of auditors or of the boards of central banks
- ambassadors, charge d'affairs and high-ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises.
- Director General, Vice President, and member of the board or a person with similar functions in an international organisation.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 6 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

The following persons are also regarded as PEPs by virtue of their relationship or association with the persons listed above:

- family members of the persons listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the persons listed above, including persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the PEP with whom they are associated.

Both domestic and foreign PEPs must be identified.

Due to legal obligations politically, exposed persons must be identified and classified in a high-risk category as they present a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

8.3.2 Third parties/nominees.

Criminals may use third parties (nominees), or anonymous or identified agents to avoid CDD undertaken at a threshold. They may also be used to *gamble, e.g.*, to break up large illicit amounts (“smurfing”). Third parties may be used to gamble on behalf of others with minimal play, which may include early or high cashouts.

8.3.3 High Spenders.

Customers may become high spenders because of their cumulative spend over a period of time. Similarly, causal customers, who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit to the website, could equally be high spenders. High amounts can be an indicator of M

8.3.4 Sanctioned/designated persons.

International sanctions, also known as restrictive measures, are primarily issued by the United Nations Security Council and by the European Union. There are different types of sanctions, the most common of which are diplomatic sanctions, economic sanctions (which include financial sanctions), and military sanctions. Boost Gaming B.V. will refer to the US Treasury Office of Foreign Assets, and Office of Foreign Assets Control lists in line with Curacao regulations.

International sanctions may have different purposes, e.g., to combat terrorism and terrorist groups such as Al Qaida, to impose measures against the Taliban, and to control the proliferation of weapons of mass destruction.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 7 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

8.3.5 Suspicious transactional behaviour.

- High deposit, not in line with the customer's known profile.
- Third party usage.
- Suspicion received.
- Non/low wagering.
- Responsible gaming risks
- Not cooperate in the carrying out of CDD
- Attempts to register more than one account with the same licensee.
- Considerable amounts of deposits during a single session by means of multiple prepaid cards.
- Depositing well more than what is required to sustain his usual betting patterns.
- Making small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings.
- Making frequent deposits and withdrawal requests without any reasonable explanation
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions they normally carry out.
- Enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Carry out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Seeking to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Displaying suspicious behaviour in playing games that are considered as high risk.
- Becoming uncooperative when requested to provide required details and/or documentation on a transaction.
- Subjects, or persons linked to subjects of STR are adversely known on open sources.
- Unusual or suspicious identification documents or lack of documents
- High turnover, but the account holds a low balance (E.g., conduit account activity)
- Remitting money to persons/entities (including NGOs) with suspected links to terrorism
- Withdrawal of money from locations that are in, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places.
- Transaction narrative is suspicious or does not make any commercial sense within the context of the transaction itself.
- Overall transactional activity is indicative of terrorist-related activities such as (but not limited to): purchasing camping/survival stores, first-person shooting games, or combat training-type activities, before traveling to known, or adjacent to, conflict/terrorism zones

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 8 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	-------------------------

8.4 Controls for Customer and Transaction Risk.

No	Risk Factor	Risk	Consequences	Risk Probability	Risk Impact	Inherent Risk (P & I)	Mitigation & Controls	Residual Risk
1	Registration (Simplified Due Diligence)	Customers who are not identified in line with the Curacao regulations provide an inherent risk as we do not know with whom it is transacting.	1, Increased chance of ML/FT. 2, Failure to comply with Curacao gambling regulations. 3, Identifying high-risk customers. 4, Underage gamblers. 5, Anonymous and fictitious accounts.	Low	Medium-High	Medium-High	Boost Gaming B.V. upon establishing a business relationship will collect the person's full name, residential address, and date of birth. The company will consider collecting the place of birth, Nationality, and Identity number from customers who are residents from high-risk countries.	The residual risk is medium as customers in accordance with the Curacao's AML requirements will provide all the necessary information upon establishing the business relationship and going forward will be asked to complete CDD upon reaching the 4,000 NAF threshold
2	False or stolen identity	Customers use false or stolen identities to bypass controls to facilitate the laundering of criminal funds.	1, Increased chance of ML/FT. 2, Potential Risk of Fraud. 3. Poorly trained/untrained staff members. 4, ineffective monitoring procedures	Low-Medium	High	Medium-High	Any due diligence documents received are scrutinised through a third-party tool or via the Risk team to ensure the documents are genuine. In the event the customer wishes to amend their details they must contact our customer service team to change these details and provide the relevant documentation to verify the change. All members of the risk team are trained to identify fake documents. When the documents are determined as fake or have been tampered	The residual risk is low-medium as the company utilises technological systems to identify tampered and fake documents.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 9 of 37
------------	-----------------------------	--------------------	---	---------------------	-------------------------	-------------------------

							with, an internal suspicious transaction report is completed and raised to the Compliance Persons MLRO.	
3	High Risk Customers	Failure to categorise customers who are deemed high-risk increases the risk of ML/FT, organised crime groups, and money mules targeting the gambling site. Accounts being opened using false information	1, Increased risk of ML/TF. 2, Heightens the risk of organised crime groups and money mule's targeting our site. 3, Failure to obtain customer due diligence/enhanced due diligence. 4, Failure to comply with our licence conditions.	Medium	High	Medium-High	An assessment on account is conducted at various AML risk factors to determine the risk rating. The assessment undertaken will consider the below risks: • Customer and transaction Risk • Product Risk • Payment Risk • Geographical Risk All customers undertake a customer risk assessment upon reaching these thresholds: • Total Deposits of 4,000 NAF/2K USD (Currency equivalent) in 24 hours. • Single deposits of 10K USD (Currency equivalent) deposits or withdrawals. • Deposits 5K USD (Currency equivalent) in 24 hours. • 100K USD (Currency equivalent) Deposits lifetime. Customer's residents from higher risk of geographic areas will be required to undertake enhanced due diligence upon reaching total deposits of 4,000 NAF/2K USD (Currency equivalent) in 24 hours.	A low-medium risk remains as all customers are risk assessed upon reaching 4,000 NAF and other transaction monitoring thresholds. Customers resident of higher risk of geographic areas will be required to undertake enhanced due diligence upon reaching 4,000 NAF.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 10 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

							Customers upon reaching total deposits or withdrawals of 4,000 NAF will be restricted from making further deposits and pending withdrawals will be held until documentation received. As part of the review the account will be checked for the below indicators for suspicious activity, • Third party usage • Non/low wagering. • Not cooperate in the carrying out of CDD • Attempts to register more than one account with the same licensee. • Considerable amounts of deposits during a single session by means of multiple prepaid cards. • Depositing well in excess of what is required to sustain his usual betting patterns. • Making small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings. • Making frequent deposits and withdrawal requests without any reasonable explanation • Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions	
--	--	--	--	--	--	--	---	--

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 11 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

							that are significantly larger in volume when compared to the transactions, he normally carries out. • Enquiries about the possibility of moving funds between accounts belonging to the same gaming group. • Carry out transactions which seem to be disproportionate to his wealth, known income or financial situation. • Seeking to transfer funds to the account of another customer or to a bank account held in the name of a third party. • Displaying suspicious behaviour in playing games that are considered as high risk. • Becoming uncooperative when requested to provide required details and/or documentation on a transaction. • Subjects, or persons linked to subjects of STR are adversely known on open sources. • Unusual or suspicious identification documents or lack of documents • High turnover, but the account holds a low balance (E.g., conduit account activity) Players rated as high risk are requested to provide CDD if required and EDD documentation unless the customer is de-risked. The business	
--	--	--	--	--	--	--	--	--

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 12 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

							relationship is terminated after 30 days if satisfactory EDD documents are not received.	
							Customers allocated a risk rating of medium will be assessed, and when unusual activity is identified the risk rating will be amended to high.	
							An internal STR is submitted to the MLRO when the customer is suspected of unusual activity.	
4	Politically Exposed Persons (PEPs)	There is a higher risk associated with individuals who have a high political profile or have held public office (past or present), as their positions may make them vulnerable to corruption and bribery, therefore, increasing the risk of accounts being funded by the proceeds of crime by such individuals	1. Identifying PEPs. 2. Failure of enhanced due diligence. ., Breakdown in process and procedures.	Low	High	Medium-High	All customers are screened at registration against the PEP database, through a 3rd party tool to verify if they are on this list. Should a player be identified as a potential PEP, the designated team completes an investigation. If confirmed, the customer account is closed, or if the company continues to establish a relationship the following process will be undertaken: • Approval from senior management • EDD documentation requested • Timing of ongoing monitoring. As part of the investigation, if suspicious activity is detected, the member of staff will consider raising an internal STR to the Compliance Person/MLRO. All customers are rescreened against the sanction database as part of ongoing monitoring. On a risk basis, a customer may be checked against the PEP database depending on the activity on their account.	A low risk remains as all customers are screened at registration and the account is either closed or enhanced due diligence is requested if a decision to establish a business relationship. As part of ongoing monitoring, all customers are re-screened as part of on-going monitoring

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 13 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

BUSINESS RISK ASSESSMENT

5	Prohibited relationships and transactions (sanctions)	There is a risk that an individual subject to sanctions may attempt to open an account and transact with an online operator. It is a criminal offence to transact with individuals who are subject to certain types of sanctions such as asset freezes	1. Ineffective monitoring processes and procedures. 2. Insufficient staff training. 3. Criminal offence to transact with an individual who is subject to sanctions.	Low	High	High	All customers are screened against the sanction list, through a 3rd party tool to verify if they are on any sanctions database. When a customer is identified as potentially on the sanction list, the Compliance Person/MLRO completes an investigation. If confirmed, the customer account is closed, and a suspicious activity report is raised to the FIU. All customers are rescreened against the sanction database as part of ongoing monitoring. On a risk basis, a customer may be checked against the sanction list database depending on the activity on their account.	A low risk remains as all customers are screened and the account is closed if the person is found on this list. As part of ongoing monitoring, all customers are re-screened as part of on-going monitoring.
6	Source of funds/wealth is unknown for higher-spending customers	If higher-spending customers are allowed to play without source of funds/wealth being established on a risk-sensitive basis, an increased risk of ML/TF activity is posed.	1. Ineffective monitoring processes and procedures 2. Insufficient staff training. 3. Failure to conduct enhanced due diligence. 4. Identifying ML/FT.	Medium	Medium-High	Medium-High	All customers undertake a customer risk assessment upon reaching these thresholds: - Total Deposits of 4,000 NAF/2K USD (Currency equivalent) in 24 hours. Customers upon reaching total deposits of 4,000 NAF (Currency equivalent) will be required to provide estimated annual income and occupation, should they not provide this information within 30 days from the initial request the business relationship has been terminated. - Single deposits of 10K USD (Currency equivalent) deposits or withdrawals.	A low-medium risk remains as all customers are risk-assessed upon reaching 4,000 NAF and other transaction monitoring thresholds. Customers resident of higher risk of geographic areas will be required to undertake enhanced due diligence upon reaching 4,000 NAF.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 14 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

							- Deposits 5K USD (Currency equivalent) in 24 hours. 100K USD (Currency equivalent) Deposits lifetime. When the person's activity is not in line with the normal customer/ behavioural profile, enhanced due diligence will be requested. Customers rated as high risk as part of the customer risk assessment or residents from higher risk of geographic areas. will be required to undertake enhanced due diligence.	
7	Drastic Changes in Betting Behaviour	A drastic change in betting behaviour (i.e., unusually high activity when compared to what may reasonably be deemed normal expected activity from the customer in question) may indicate that the account is now being used, by the customer or by someone on whose behalf the customer is acting, for money laundering purposes.	1. identifying ML/FT. 2. Insufficient staff training. 3. Insufficient procedures and processes.	Low	Medium	Medium	All customers undertake a customer risk assessment upon relevant thresholds and the account is reviewed for drastic changes in behaviour/activity to ensure in line with the normal profile of the player. Upon a customer requesting a withdrawal, the risk and payment team will conduct a review of the person's gameplay, and transaction activity for unusual activity.	A medium risk remains as the company as additional internal controls are required to monitor customers activity is in line with the normal profile of the person.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 15 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

8	Multiple Accounts same operator	There is a risk that a customer 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.	1. Ineffective monitoring processes and procedures. 2. Poorly staff training. 3. Identifying high-risk customers. 4. Anonymous and fictitious accounts.	Low-Medium	Medium-High	Medium	Upon a customer reaching transaction monitoring thresholds, behaviour reports, or upon requesting a withdrawal a review is conducted to check if the customer holds more than one account. When a customer is located as having more than one account, a decision will be taken to close one of these accounts, and the player informed. An internal STR is submitted to the MLRO when the customer is suspected of unusual activity.	A medium risk remains as customers can create multiple accounts without detection, heightening the risk of the person circumventing the CDD thresholds and layering funds from the proceeds of crime through multiple accounts.
9	Customer-to-customer fund transfers	There is a risk that customers could pass the proceeds of crime from one account to another account held with the same operator (belonging to a different individual) in order to create distance and confuse the money trail or transfer funds as a way of paying for goods or services related to criminal activity.	1. Increase the chance of ML/FT. 2, Potential Risk of Fraud. 3. Ineffective monitoring procedures.	No Risk	No Risk	No Risk	Umiumii does not allow our customers to transfer funds to other customers therefore this risk is removed.	As Umiumii does not allow customers to transfer funds to other customers there is no risk to the business.

8.5 Customer and Transaction - Overall Inherent and Residual Risk.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 16 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

BUSINESS RISK ASSESSMENT

	Overall						Overall				
	Inherent Risk						Control Risk				
Customer and Transaction Risk	Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk		Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk
Registration (Simplified Due Diligence)						Registration (Simplified Due Diligence)					
False or Stolen identity						False or Stolen identity					
High Risk Customers						High Risk Customers					
PEP's						PEP's					
Prohibited relationships and transactions (Sanctions						Prohibited relationships and transactions (Sanctions					
Source of funds/Wealth						Source of funds/Wealth					
Drastic Changes in Betting Behaviour						Drastic Changes in Betting Behaviour					
Multiple Accounts same operator						Multiple Accounts same operator					
Customer to customer fund transfers						Customer to customer fund transfers					

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 17 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

The assessment of the overall residual risk allocated to the customer and transaction risk is **Medium** this control has been assigned as additional controls are required to identify changes in betting behaviour/activity.

9. Product Risk.

Group Limited offers the following product categories:

- Table games
- Slots
- Sportsbook

By the use of sportsbook and casino products or games, Boost Gaming B.V. cannot determine a heightened ML or TF risk. Here the analysis of the gaming behaviour could only provide information on suspicious facts.

Particular gaming behaviours that can be used by money launders e.g.

- to convert placed money from illicit sources (often by use of anonymous payment methods and/or the help of “financial agents”) or
- to disguise the illicit source of funds (“layering”) can be:

So-called “*balance betting*.” The term balance betting is mainly used in the 2-way betting area. Balance betting is a risk-free betting system where the customer has two opportunities to choose from and wagers on both (e.g., Roulette – stakes on red and black, odd, and even). This gaming behaviour can be used to convert the money before requesting a withdrawal. A behaviour like balance betting makes no economic sense and shows that a player has no view to gain. A customer with solely this gaming behaviour poses a heightened risk.

9.1 Controls for Product Risk.

No	Risk Factor	Comment	Consequences	Risk Probability	Risk Impact	Inherent Risk (P & I)	Mitigation & Controls	Residual Risk
----	-------------	---------	--------------	------------------	-------------	-----------------------	-----------------------	---------------

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 18 of 37
------------	-----------------------------	----------------	---	-----------------	-------------------------	----------------------

BUSINESS RISK ASSESSMENT

1	Slots/Jackpot Games	There is a risk that a customer may deposit criminal funds into his account and then withdraw them without wagering in any product, following minimal play, low-risk wagering activity, by covering all outcomes or by using the cash-out facility	1, Increase the chance of ML/FT. 2, Poorly trained/untrained staff members. 3, Ineffective monitoring procedures.	Low	Low-Medium	Low-Medium	All wins over a certain threshold are reviewed by the risk team and if necessary, the game provider contacted to verify the game pay-out was legitimate. The risk team requests reports from the game provider when unusual activity is detected. Should unusual activity be detected, the member of staff will consider raising an internal suspicious transaction report to the MLRO.	The residual risk is low as reports are requested when the customer wins over a certain threshold and reports are received from the provider when unusual activity is detected
2	Poker product: Peer-to-peer gambling	Poker is classed as a higher-risk product for ML/TF purposes due to the potential for collusion and soft play as there is a risk for money to be deliberately passed between players on the same network which could be the proceeds of crime, or funds could be passed to pay for goods or services related to criminal activity	1, Increase the chance of ML/FT. 2, Potential Risk of Fraud. 3, Poorly trained/untrained staff members. 4, Ineffective monitoring procedures.	No Risk	No Risk	No Risk	The company does not offer this product to customers	No Risk as this product is not offered to customers.
3	Sports betting	Sports betting is classed as a medium-risk product due to the potential of match-fixing and inside training as there is a risk this type of activity is linked to criminal activity	1, Increase the chance of ML/FT. 2, Potential Risk of Match Fixing.	Medium	High	Medium-High	The game provider blocks events in certain countries when money laundering is prevalent. The game provider monitors the following activity:	The residual risk is medium due to the type of product and not all bets are scrutinised, and unusual activity is only

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 19 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	---------------------------------

			3, Poorly trained/untrained staff members. 4, Ineffective monitoring procedures.				- Unusually high numbers of bets placed on a relatively minor match or betting option. - Unusually high bets or unusual odds such as on specific odds or bet options rarely played. - An unusual change in odds. - An unusual geographic distribution of the players who place bets on the match concerned, such as many bets from a specific location. - Placing large bets which are not in line with the customer's known income. The provider notifies the Boost Gaming B.V. whenever betting on sure outcomes is identified and. action is taken upon withdrawal. When the Risk Team identifies unusual activity on an account, the game provider is contacted	identified through specific reports.
--	--	--	--	--	--	--	---	--------------------------------------

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 20 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	---------------------------------

							to review the customer's betting pattern. Customers who are suspected of match-fixing/inside trading or money laundering are reported to the Compliance Person/MLRO in an internal suspicious activity completed.	
4	Table games	Table games are classified as medium-risk products due to the potential of players being able to place safe bets by engaging in opposite betting strategies, in addition, these games are targeted as collusion, card counting, and chip dumping can occur	1, Increase the chance of ML/FT. 2, Poorly trained/untrained staff members. 3, Ineffective monitoring procedures	Medium	Medium-High	Medium	All wins over a certain threshold are reviewed by the risk team and if necessary, the game provider contacted to verify the game pay-out was legitimate. The game provider issues a report whenever this suspicious activity is detected or when Boost Gaming B.V. requests verification of a customer's gameplay. When the Risk Team identifies unusual activity on an account, the game provider is contacted to review the customer's betting pattern. Customers who are suspected of money laundering are reported to the MLRO in an internal suspicious activity.	The residual risk is medium due to the type of product, effective controls are in place to identify unusual activity.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 21 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

9.2 Product - Overall Inherent and Residual Risk.

Gambling Activity	Overall Inherent Risk						Overall Control Risk				
	Low Risk	Medium-Low Risk	Medium Risk	Medium-High Risk	High Risk		Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk
Slots/Table Games						Slots/Table Games					
Poker product: Peer-to-peer gambling	No Risk					Poker product: Peer-to-peer gambling	No Risk				
Sports Betting						Sports Betting					
Table Games						Table Games					

The assessment of the overall residual risk allocated to the product is **Low-Medium**, although as the company the demographic of customers, play mainly table games, as we offer sports betting and table games this poses a high risk of ML/FT because of the nature of these products, effective controls are in place to identify unusual activity.

10. Payment Risk

10.1 Remote Operator Risk.

Boost Gaming B.V. utilises the reports and system alerts to flag up high-risk players. Using these risk tools enables us as a business to continually monitor changes in customer transactional behaviours to identify new methodologies of money laundering or fraudulent activity. Through this, we can put the appropriate measures/rules in place to counteract these new behaviours and minimise exposure to our business.

Boost Gaming B.V. does not allow inter account transfers between their customers. Customers are only allowed to use their betting account for gambling purposes. The use of gaming accounts for deposits and withdrawals without gambling violates the company's general terms and conditions. Deposits using cash are not possible.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 22 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

(Boost Gaming B.V. reserves the right to limit certain kinds of payment methods to customers. Customers with increased AML risk cannot or can only make restricted use of risk-intensive payment methods.

In general, money launders try to avoid identified and verified payment methods. Anonymous payment methods are very attractive as they represent a way to channel proceeds from criminal activity into the legal economy.

10.2 Payment Methods.

In general, money launders try to avoid identified and verified payment methods. Anonymous payment methods are very attractive as they represent a way to channel proceeds from criminal activity into the legal economy.

Boost Gaming B.V accepts the following payment methods:

- Swapped
- Crypto

10.3 Controls for Payment Risk.

N o	Risk Factor	Comment	Consequences	Risk Probability	Risk Impact	Inherent Risk (P & I)	Mitigation & Controls	Residual Risk
1	E-wallet payment methods	E-Wallet payment methods are potentially higher-risk payment methods as a potential means to mask the true origins of the funds deposited with the operator. The	1, Failure in identifying ML/FT. 2, Insufficient staff training.	Medium	Medium	Medium	Customers depositing via an e-wallet pose an increased ML/TF risk to the business as the source of funds are difficult to trace.	A medium risk remains as customers can deposit with these types of payment methods which are deemed to

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 23 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

		use of E-Wallet payment methods enables an individual to move funds easily to other betting sites, and bank accounts or spend via associated debit/credit cards. A customer depositing via an E-Wallet may pose an increased ML/TF risk to operators as the source of funds is difficult to trace and this payment method type offers a relative level of anonymity to the customer	3, Ineffective transactional monitoring procedures. 4, Failure to identify high-risk players.				Any (XXXXX) customers who use an alternative withdrawal method to their previous deposit will be flagged, and a check will be carried out by the team checking the player's account and transaction activity. A screenshot of an e-wallet or letter from the e-wallet provider showing customer account details will be requested on occasions when knowledge of the e-wallet account holder is not available from the e-wallet provider's back office. Proof of payment method ownership is required according to a risk-based assessment of a player's account or in high-risk situations.	pose a higher risk from an AML standpoint
2	Cash-based/Crypto payment methods	Customers using cash-based payment methods pose a higher ML/ TF risk to operators as the source of funds is in the main unknown and difficult to trace. This type of payment method is often also non-refundable, meaning that withdrawals must be processed via an alternative source. Also included in this risk (for operators who have both an online and retail betting presence) is the use of LBOs to fund an online account using cash. There is a risk that customers may abuse	1, Failure in identifying ML/FT. 2, Insufficient staff training. 3, Ineffective transactional monitoring procedures.	Low-Medium	Medium-High	Medium-High	Due to anonymous payments and pre-paid cards posing a high risk of ML/T, customers who deposit with these types of methods will be reviewed for suspicious activity on a case-to-case basis. When a member of staff notices irregular activity as part of a review of an account. the player will be required to supply due diligence. In addition, the staff	A medium risk remains as customers as the source of funds can be difficult to trace and effective controls are required to mitigate the risk of ML/FT with these types of methods.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 24 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

		these characteristics in order to carry out ML/TF activity through their betting accounts	4, Failure to identify high risk players.				member when applicable may contact the payment provider and confirm the origin of where these vouchers were purchased. Upon the customer requesting their first withdrawal and having only funded their account with an anonymous payment method. The customer will be required to provide proof of bank account will be requested from the customer before the withdrawal can be processed. The member of staff may also consider raising an internal suspicious activity report to the MLRO to review the account in further detail and decide the appropriate action to be taken on the account.	
--	--	---	---	--	--	--	---	--

10.4 Payment Method – Overall Inherent and Residual Risk.

Payment Methods	Overall Inherent Risk						Overall Control Risk				
	Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk		Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk
E-wallet payment methods											

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 25 of 37
------------	-----------------------------	----------------	---	-----------------	-------------------------	----------------------

Cash-based/Crypto payment methods						Cash-based/Crypto payment methods					
-----------------------------------	--	--	--	--	--	-----------------------------------	--	--	--	--	--

The assessment of the overall residual risk allocated to payment method is **Medium**, this control has been assigned this risk score due as customers on our site can fund their gaming account using anonymous payment methods, therefore as a company, we cannot verify the origin of these funds increasing the risk of ML/TF from this payment method.

Additional effective controls are required to identify unusual activity with higher-risk payment methods.

11. Geographical Risk.

11.1 High Risk Jurisdictions.

Boost Gaming B.V utilises several sources to define high-risk jurisdictions. The list is shown within the Terms and Conditions available on the Boost Gaming B.V website, and includes countries subject to international sanctions, other high-risk countries determined using the methodology mentioned here, as well as countries where gambling is illegal.

The main source for high-risk jurisdictions is the BASEL AML Index, however this is supplemented with the following lists:

- FATF/CFATF Jurisdictions under Increased Monitoring)
- FATF/CFATF High-Risk Jurisdictions subject to a Call for Action

Customers whose nationality is from a high-risk country are scrutinised to ensure funds are coming from a legit source and high-risk countries

Customers whose country of birth and Nationality is from a high-risk country as defined by the above data sources will be considered as potentially high risk due to, they may have received money from this country.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 26 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	---------------------------------

11.2 Controls for Geographical Risk.

No	Risk Factor	Comment	Consequences	Risk Probability	Risk Impact	Inherent Risk (P & I)	Mitigation & Controls	Residual Risk
1	Activity from outside a customer's registered country	A customer logging into his account from outside of his registered country poses a potential risk to an operator as the customer may not be who he claims to be, and the information used to verify the account as well as the source of funds may be incorrect as a result. This can pose an increased level of risk where logins are made from high-risk countries.	1. Increase the chance of ML/FT. 2. Potential Risk of Fraud. 3. Poorly trained/untrained staff members. 4. Ineffective monitoring procedures.	Low	Medium	Medium	Should unusual activity be detected, the member of staff may, if appropriate, request enhanced due diligence and on occasion, close the account. If suspicious activity is detected, the account may be closed, depending on the activity on the account. The member of staff may consider raising an internal suspicious transaction report to the AML Team.	The residual risk is medium as the customer's IP Addresses are only reviewed when they appear on internal reports or upon withdrawal stage
2	High-risk jurisdictions	There is a risk that customers highlighted by sources such as FATF as having strategic AML/CFT deficiencies look to abuse the sector for ML/TF activity. There is also a risk when accepting customers from countries that have high levels of corruption as this increases the risk of ML taking place.	1, Failure to Identify customers who are registering from countries deemed as high risk. 2, Increase the chance of ML/FT.	Medium	Medium-High	Medium-High	Customers upon reaching total deposits of 4,000 NAF (Currency equivalent), players that are residents from high-risk countries are risk rated as high, and enhanced due diligence is requested. The customer will have 30 days to provide source of documents from the initial request, should these documents not be provided	A medium risk remains as customers are not requested to provide EDD documentation until reaching 4,000 NAF (Currency equivalent)

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 27 of 37
------------	-----------------------------	--------------------	---	---------------------	-------------------------	--------------------------

							the business relationship terminated. An internal STR is submitted to the MLRO when the customer is suspected of unusual activity.	
--	--	--	--	--	--	--	---	--

11.3 Geographical - Overall Inherent and Residual Risk.

	Overall Inherent Risk						Overall Control					
Geographical	Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk		Risk	Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk
Activity outside the country						Activity outside the country						
High-Risk Jurisdictions						High-Risk Jurisdictions						

The assessment of the overall residual risk allocated to geographical risk is **Medium**, this control has been assigned this risk score as we accept customers are residents from high-risk jurisdictions.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 28 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

12. Employee Risk.

12.1 Controls for Employee Risk.

No	Risk Factor	Comment	Consequences	Risk Probability	Risk Impact	Inherent Risk (P & I)	Mitigation & Controls	Residual Risk
1	Employee screening and Training	Employees potentially pose a significant ML/TF threat by means of collusion through play, product, or record manipulation. Without appropriate identification processes in place, operators may become vulnerable.	1, Potential Risk of Fraud. 2, Failure in complying with regulations. 3, Increase the chance of ML/TF. 4, Incomplete staff screening and training. 5, Poorly trained/untrained staff.	Low	Medium-High	Medium	(XXXXX) follows high ethical standards in the recruitment of all its staff. This includes taking prospective employee's professional backgrounds into account, performing background checks, obtaining a certificate of good conduct from the local police authority, and verifying references provided, as per HR processes. Additional vetting may be conducted depending on the person's position in the company. There is mandatory training for all new colleagues and refresher training is conducted for other relevant colleagues across the business as required. The material/content is reviewed annually to ensure that it is up to date in relation to any legislation or procedural changes. We provide employees with an approved programme of training in relation to the	The residual risk is low as all new employees are vetted and depending on their position will complete relevant training before them being actively involved with any day-to-day operations.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 29 of 37
------------	-----------------------------	--------------------	---	---------------------	-------------------------	--------------------------

							topics and themes considered by the AML policy and procedures. Topics cover both money laundering and terrorist financing.	
2	Staff knowledge	Employees may pose a significant risk where they have either not received adequate training to enable them to identify potential ML/ TF issues, or where they are unable to highlight such issues through the established channels. Without sufficient training and standards in place, there is a risk that staff may become involved in assisting in the commission of an ML offence.	1, Failure in complying with regulations. 2, Poorly trained/untrained staff. 3, ineffective training manuals	Low	High	Medium-High	All operating procedures are documented in the process, clearly defining, and providing steps to resolve relevant processes. We continually review and revise our policies and procedures considering relevant legislation, regulation, and industry guidance/learning, including guidance provided by applicable regulatory bodies, to meet our licensing objectives. When a new process is identified, the Head of department or manager will implement an SOP for any procedure. If appropriate, these changes are sent to the compliance team for approval. When new methodologies of money laundering/financing of terrorism identified are detected, processes and procedures are put in place to combat these behaviours. The business risk assessment and AML/CTF procedure are reviewed on the following basis: • In response to any changes in relevant regulation and/ or legislation	A low-medium risk remains as all staff receive AML training and refresher training. The AML training is updated when there is relevant legislation or regulatory changes in Curacao.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 30 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

							• In response to general guidance notes or best practice guidance issued by any relevant regulator. • In response to any regulatory action taken against any operator by any relevant regulator • In response to findings of a relevant internal or external audit; or upon request of the management of (XXXXX).	
3	Unusual activity	There is a risk that employees do not escalate instances of unusual activity where there is an indication that a customer and/or employee may be involved in potential ML/TF activity. This is applicable to the Customer, Payment, Product, Employee, and Geographical risk areas.	1, Identifying money laundering 2, Ineffective training,	Low	High	Medium-High	All staff members conduct AML Training as part of the onboarding process and refresher training on how to identify unusual activity and when to raise an internal suspicious transaction report. A training record is kept detailing the: • The content of the training • Name of staff who have received the training The date on which the training was delivered • The results of any testing carried out. All members of staff complete refresher AML training every 6 months When unusual activity is detected the member of staff will submit an internal STR to the MLRO.	The residual risk remains low as all staff members are trained to identify unusual activity and process of raising an internal suspicious transaction report

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 31 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

12.2 Overall Employee Inherent and Residual Risk.

Employee	Overall Inherent Risk						Overall Control Risk				
	Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk		Low Risk	Low-Medium Risk	Medium Risk	Medium-High Risk	High Risk
Employee Screening & Training						Employee Screening & Training					
Staff Knowledge						Staff Knowledge					
Unusual Activity						Unusual Activity					

The assessment of the overall residual risk allocated to employees is **Low**, this control has been assigned this risk score as all new employees are vetted and must complete relevant training before being actively involved with any day-to-day operations.

All staff members are trained to identify unusual activity and complete AML Training every six months

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 32 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

13. Conclusion.

	Overall Control Risk				
	Low Risk	Low-Medium Risk	Medium Risk	Medium-High	High Risk
Customer & Transaction Risk					
Product Risk					
Payment Risk					
Geographical Risk					
Employee Risk					

This document describes the purpose, scope, and methodology used for the business risk assessment of (XXXXX) and provides an overview of its conclusions.

Through this assessment, it was concluded that presently the Company faces an overall risk of medium, after considering the inherent ML/TF risk and the controls in place which is in line with the Company's overall risk appetite.

The Business Risk Assessment is updated whenever there are material changes in the Company's risk environment and control framework, but not less often than once a year, to ensure that any changes in internal or external risk factors are accounted for and the variance in risk exposure is recorded.

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 33 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	--------------------------

Doc BRA	Issued By: Boost Gaming N.V	Issue No: 1	Issue Date: 1 st of May 2025	Rev. No. 1.0	Rev Date: 12.05.2025	Page No. 34 of 37
------------	-----------------------------	--------------------	---	---------------------	-----------------------------	---------------------------------