Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Keep On Entertainment N.V.

Business Risk Assessment

CONFIDENTIALITY STATEMENT

This is a confidential document for Keep On Entertainment N.V.. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Keep On Entertainment N.V.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Document Version Control

Version	Date	Security class	Author	Purpose
1.0	25.09.2024	Confidential	Keep On Entertainment N.V.	Creation of this document

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Table of Contents

1. INTRODUCTION 3

1.1 THE COMPANY 3
1.2 RISK CHARACTERISTICS 3
1.3 EU SUPRANATIONAL RISK ASSESSMENT & NATIONAL RISK ASSESSMENT 4
1.4 METHODOLOGY 6

2. IDENTIFICATION AND SCORING OF INHERENT RISK 7

2.1 INHERENT RISK – GAMES 10
2.2 INHERENT RISK – PAYMENT METHODS 13
2.3 INHERENT RISK – JURISDICTIONS AND PLAYERS 17
2.4 INHERENT RISK – DELIVERY CHANNELS 21
2.5 TOTAL INHERENT RISK 22

3. DETERMINATION OF RISK APPETITE 23

4. ANALYSIS OF AML/CFT CONTROLS 24

4.1 CONTROLS – GAMES 24
4.2 CONTROLS – PAYMENT METHODS 27
4.3 CONTROLS – CUSTOMER DUE DILIGENCE 34
4.4 CONTROLS – DELIVERY CHANNELS 37
4.5 CONTROLS – RISK ASSESSMENT 38
4.6 CONTROLS – TRANSACTION MONITORING AND REPORTING 39
4.7 CONTROLS – INTERNAL AUDIT 40
4.8 CONTROLS – RECORD KEEPING 41
4.9 CONTROLS – TRAINING AND HR 42
4.10 CONTROLS – MLRO AND COMPLIANCE 43
4.11 CONTROLS – GOVERNANCE 45
4.12 CONTROLS – OUTSOURCING 46
4.13 OVERALL CONTROLS 48

5. DETERMINATION OF RESIDUAL RISK 49

5.1 RESIDUAL RISK – GAMES 50
5.2 RESIDUAL RISK – PAYMENT METHODS 50
5.3 RESIDUAL RISK – JURISDICTIONS AND PLAYERS 51
5.4 RESIDUAL RISK – DELIVERY CHANNELS 51
5.5 TOTAL RESIDUAL RISK 52

6. REMEDIATION PLAN 53

7. CONCLUSION 54

APPENDIX I – BUSINESS RISK ASSESSMENT EXCEL SHEET (SCORING AND WEIGHING) 54

BOARD OF DIRECTORS SIGNATURE PAGE 55

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

1. Introduction

1.1 The Company

Keep On Entertainment N.V. (hereinafter referred to as "Keep On Entertainment" or as "the Company") is registered in Curaçao with registration number 168271 and registered address at Kaya W.F.G. (Jombi) Mensing 24 Unit A, Willemstad, Curaçao. Keep On Entertainment N.V. is a B2C remote gaming company, operating through the website https://www.keeponwin.com.

1.2 Risk characteristics

The Company's business activity is that of a remote gaming provider offering gaming services – casino, sportsbook and virtual games services. This activity constitutes a "relevant activity" in terms of Curaçao's GCAregulations.

According to the National Risk Assessment (hereinafter referred to as "NRA") of Curaçao, the overall Money Laundering and Financing of Terrorism (hereinafter "ML/FT") risk for online gambling was rated as **High,** driven by the following components:

- Curaçao is among the top 3 countries where the most servers of online gambling sites are located;
- the fact that online gambling is a cross-border activity without any real borders makes this sector even more attractive to money launderers, because of the opportunities offered to misuse the legislative, administrative, judicial differences between countries to continue criminal activities regardless of actions taken by governments;
- the vulnerability of this sector in Curaçao is exacerbated by the practice of the previous sub-licensing without any regulatory oversight. Transparency was lacking and the sector was de-risked many years ago. The inherent vulnerability as well as the final vulnerability are assessed as HIGH;

"Online gambling is inherently vulnerable to ML due to the high number of customers, high volume of transactions, the nonface-to-face nature of the business, the high percentage of non-resident customers and the use of prepaid cards that are not linked to a bank account. This is further evidenced by the high number of UTRs received. Certain remote gaming activities are more vulnerable than others. For instance, P2P and sports betting are more exposed than bingo or lotteries as they involve a transfer of value or predictable, low losses."

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

The available statistical data and evidence led the Curaçao authorities to take a conservative view of the country's FT threats hence resulting in a risk rating of High. The national threat is two-fold – stemming from the risk of terrorism itself and the risk of terrorism financing.

In the sectoral ML/FT vulnerability assessment, the NRA has identified online gambling as having an inherent risk rating as High. The overall level of controls in the sector was indicated as being Low, resulting in a residual risk rating of High.

1.3 EU Supranational Risk Assessment & National Risk Assessment

The European Commission published its revised Supranational Risk Assessment Report (hereinafter referred to as "SNRA") as required by the 4th Anti-money Laundering Directive. The Commission assessed the vulnerability of financial products and services to risks of money laundering and terrorist financing. This risk analysis is conceived as a key tool to identify, analyse and address money laundering and terrorist financing risks in the EU. It aims at providing a comprehensive mapping of risks on all relevant areas, as well as recommendations to Member States, European Supervisory Authorities and obliged entities to mitigate these risks. This risk analysis supports Member States and obliged entities when carrying out their respective risk assessments.

The SNRA has shown that *"For **online gambling** there is a high-risk exposure due to very large numbers of transaction- flows and the lack of face-to-face interaction. Although casinos present inherently high-risk exposure, their inclusion in the anti-money laundering/countering the financing of terrorism framework since 2005 has had a mitigating effect."*

The Fifth Money Laundering Directive (5AMLD) came into force on the 10th of January 2020. Building on the regulatory regime applied under its predecessor, the Fourth Money Laundering Directive (4AMLD). 5AMLD reinforces the European Union's AML/CFT regime to address a number of emergent and ongoing issues. The impact of 5AMLD is far-reaching. Key changes from the 5AMLD – which are relevant to our business – have been listed below:

- makes a significant new legislative step in the treatment of virtual currencies,
- sets a lower limit of EUR 150 for prepaid card transactions,
- companies that do business with customers from high-risk third countries are, under 5AMLD, required to perform enhanced due diligence measures,
- 5AMLD requires EU member states to compile and publicly release a functional PEP list made up of prominent politically exposed public functions.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

The 4th and 5th Anti Money Laundering Directive require that obliged entities take into account the findings of any applicable national risk assessments together with the EU Supranational Risk Assessment (SNRA) when determining the inherent risk of a business. Therefore, the results of the Curaçao National Risk Assessment (NRA) and the SNRA were considered and factored into the assessment. The SNRA has specifically identified that online gambling operators are exposed to a high risk of ML/FT due to the huge volumes of transactions passing through the operator on a daily basis, the ability of players to use anonymous means of payment and the non-face-to-face element discussed above.

The 6th AMLD is not out yet, although there was the notion that there was. The Directive (EU)2018/1673 was an enhancement of the 5th AMLD - Combatting ML by Criminal Law – the 6th AMLD is in the pipeline, probably will be a regulation not a directive. There is the new AMLA brewing.

Under the current rules, only individuals can be punished for the act of money laundering; however, 6AMLD will extend criminal liability to allow for the punishment of legal persons, such as companies or partnerships. The new rules mean that a legal person will be considered culpable for the crime of money laundering if it is established that they failed to prevent a "directing mind" from within the company from carrying out the illegal activity. Practically, the new rules will place AML/CFT responsibility on management employees along with employees acting separately.

The extension of criminal liability in this context is intended to hold larger companies to account in the global effort to combat money laundering. The move will allow financial authorities to better target organizations that do not implement AML/CFT effectively. Punishments for legal persons may range from a temporary ban on operations or judicial supervision to permanent closure.

The Company developed an understanding of the adjusted scope that 6AMLD brought to it, including new predicate offenses that must be monitored and the new risk environment in which they will be operating. In addition to managing their AML resources and training compliance staff, the Company reviewed their technology deployment in order to ensure that they have the capability to meet their new transaction monitoring and screening obligations.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

1.4 Methodology

Establishing a clear understanding of the money laundering and terrorist financing (ML/FT) risk that the Company is exposed to is an essential component for it to develop and implement an effective anti-money laundering / counter-terrorist financing (AML/CFT) framework. The company-wide risk assessment that has been carried out provides a detailed analysis of the AML/CFT risk associated with the Company's products, the payment methods it accepts and its customer base. Other qualitative and quantitative factors such as the NOIS and NORUT, Sanctions National Ordinance and Kingdom Sanction Act for the online gambling sector with all relevant regulations and the conclusions of the EU Supranational Risk Assessment have also been considered.

It is important to point out that the Company has made significant improvements to bring its processes and procedures in line with its obligations. Although there is always room for improvement, the Company has implemented several changes and tools, which shows a great commitment.

In the process of carrying out the business risk assessment, the below mentioned critical steps were undertaken. These steps were carried out in the course of different project phases, as described in parts 2 to 6 of this document.

STEP 1: Identification and analysis of the inherent risk exposure of Keep On Entertainment N.V. across a wide range of categories such as its customers, games, geographical areas, delivery methods and payment methods.

STEP 2: The determination of the level of risk that the Company considers acceptable.

STEP 3: Identification, analysis and testing of the AML/CFT controls currently in place to mitigate the inherent risk within the business undertaken by Keep On Entertainment N.V.

STEP 4: Determination and quantification of the residual risk.

STEP 5: A remediation plan outlining the steps that will be taken to reduce the level of risk and retain it within the risk appetite established by the Company's directors, also to strengthen controls that the Company has in place already.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Appendix I. is showing the weighing and scoring for all of the tables (related to inherent risks, residual risks and controls) below, which are included in this BRA. Certain questions have been asked related to each field in order to identify any risks/gaps and also questions were asked regarding how effective the controls are within the Company for the said field. Different answers will give different scores, which will provide a final score for every field (*for example: Risk Factors – Table Games = 0*).

Also, the probability, the impact and the importance of each field is visible in the Appendix which derive from Table 1, Table 2 and Table 3.

Explanation for the description of score (satisfactory, needs improvement and deficient)

Satisfactory: this score has been used when a field is fulfilling expectations or needs; it is acceptable from a regulatory point of view, though not outstanding or perfect.

Needs improvement: this score was given when the company already made efforts in order to implement improvements on a specific field, however it might be not up to industry standard or fulfil our regulatory obligation 100%.

Deficient: lacking in some necessary quality or element. This can mean we are not compliant, or we are in a potential breach from a regulatory point of view.

2. Identification and scoring of inherent risk

With the participation of company employees and senior management we aimed at obtaining a broader and deeper understanding of the inherent risks to which the Company is exposed. A detailed analysis of the Company's jurisdictional risk was carried out, the risk emanating from the payment methods used and the level of inherent risk posed by the different games offered by the Company, with a detailed examination being undertaken on all categories of games.

Participants in this process included the Senior Management of the Company.

Each risk factor was assessed separately, and its risk score calculated on the basis of the likelihood of the occurrence of the risk event and the impact that such risk event might have on the Company's operations. The probability of a risk factor occurring is a combination of threat and vulnerability, whilst impact can be defined as the loss and damage, both financially and reputationally, that would be suffered if such risk were to materialize.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Likelihood	Description
Rare	A very remote chance of happening i.e. the risk will only occur in exceptional circumstances
Unlikely	There is a small chance of the risk happening
Moderate	Neither likely nor unlikely to happen, but there is a reasonable chance of the risk occurring
Likely	The risk is likely to happen
Very likely	A very high chance of happening (almost expected) i.e. the risk is most likely to occur

Table 1: *Likelihood – Description*

Impact	Definition	Comments
Trivial	A ML/FT breach will have a trivial impact or no impact at all if the risk were to occur	• No regulatory enforcement actions • No adverse national media coverage • Isolated possible customer complaints
Minor	A ML/FT breach will have a minor impact if it were to occur i.e. impact will be almost insignificant	• No regulatory enforcement other than a possible warning or reprimand • Isolated adverse national media coverage • Increasing possibility of customer complaints
Moderate	A ML/FT breach will have a moderate impact if it were to occur i.e. impact will be potentially significant and noticeable, but can be handled with the resources that are currently available	• Formal private regulatory warnings or minor financial penalties • Short term adverse national media coverage • Contained increase in customer erosion
Major	A ML/FT breach will have a major impact if it were to occur i.e. business reputation and income will	• Significant suspension of business or license approvals and/or pecuniary regulatory measures

Initial

DS

	be seriously impacted and will present challenges for the business	• Sustained adverse national media coverage • Significant increase in customer erosion
Extreme	A ML/FT breach will have an extreme impact if it were to occur i.e. business reputation and income effectively being threatened	• Criminal or civil actions against the Company or its Directors • Sustained adverse national / international media coverage possibly coupled with regulatory intervention • Suspension of business license approvals and/or significant regulatory fines • Possible withdrawal of license to operate

Table 2: *Impact – Definition*

The heatmap shown in Table 3 below outlines the level of importance assigned to each factor in relation to probability and impact:

Probability					
Very Likely	Low-Medium	Medium	Med-High	High	High
Likely	Low	Low-Medium	Medium	Med-High	High
Moderate	Low	Low-Medium	Medium	Med-High	Med-High
Unlikely	Low	Low-Medium	Low-Medium	Medium	Med-High
Rare	Low	Low	Low-Medium	Medium	Medium
	Trivial	**Minor**	**Moderate**	**Major**	**Extreme**
			Impact		

Table 3: *Importance level – Risk Heatmap*

The attributable level of importance was then given a score range as categorised in Table 4 below. Therefore, in those cases where a risk factor was assessed as having a high or likely probability of increasing ML/FT risk and a resultant major impact on the Company would ensure if the risk materialized, through the use of the matrix in Table 1, the level of importance of that risk factor would be Medium-High. A score would then be assigned to this

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

importance level according to the ranges shown in Table 2, resulting in a score range of between 63 and 83 points for a Medium-High level of importance.

Importance Level	Score Range
High	84 – 100
Medium – High	63 – 83
Medium	42 – 62
Low – Medium	21 – 41
Low	0 – 20

Table 4: *Risk score for Level of importance*

The full list of scores and weighting applied are presented in Appendix I. A breakdown of the level of risk identified per category is provided in the paragraphs hereunder.

2.1 Inherent risk – Games

One of the main risk categories that is considered in the risk assessment is the risk derived from the products offered by the Company. These being:

- Casino games (including Table games, Live casino games and Slots);
- Sports betting; and
- Virtual games.

When identifying and assessing this category of risk, all the games provided by the Company were taken into consideration. The following tables provide the risk scoring range for games, as well as the risk factors identified and the inherent risk rating per game type:

Score Range Games	Risk Rating
0 – 80	Low
81 – 160	Low – Medium
161 – 240	Medium
241 – 320	Medium – High
321 – 400	High

Table 5: *Games – Inherent risk score range*

Casino games		
Risk factors	**Answer**	**Score**
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	All games are RNG-based; possibility of collusion is so remote that it has been excluded. However, in live casino games it is possible with the involvement of casino employees or game providers	81
Is placing safe bets possible?	No	0
Is there an element of skill?	No	0
Casino games – Risk rating	**Low-Medium**	**81**

Table 6: *Casino games – Inherent risk rating*

Sports betting		
Risk factors	**Answer**	**Score**
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	No	0
Is placing safe bets possible?	Sometimes	81
Is there an element of skill?	Sometimes	81
Sports betting – Risk rating	**Medium**	**162**

Table 7: *Sports betting – Inherent risk rating*

Virtual games		
Risk factors	**Answer**	**Score**
Is there a possibility of chip dumping?	No	0
Is it possible for players to collude?	No	0
Is placing safe bets possible?	No	0
Is there an element of skill?	Sometimes	81
Virtual games – Risk rating	**Low-Medium**	**81**

Table 8: *Sports betting – Inherent risk rating*

The following tables provide the overall risk range for the scoring of games and the overall inherent risk rating in relation to all the games:

Overall Score Range Games	Risk Rating
0 – 240	Low
241 – 480	Low – Medium
481 – 720	Medium
721 – 960	Medium – High
961 – 1200	High

Table 9: *Overall inherent risk score range for Games*

Games	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Casino games		81			
Sports betting			162		
Virtual games		81			
TOTAL	**SCORE: 324 = RISK: Low – Medium**				

Table 10: *Overall inherent risk rating for Games*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

2.2 Inherent risk – Payment methods

Another risk category that was considered in the risk assessment is the risk derived from the payment methods used by Keep On Entertainment N.V. Each payment method offered by the Company has been assessed and examined in detail to determine the degree to which the specific characteristics of the payment method render users vulnerable to ML/FT threats.

The payment methods accepted by the Company are the following and their respective risk assessment is provided in the tables below:

- Vouchers (PaysafeCard)
- E-Wallets (Skrill, Neteller, Pay4Fun, Stickpay)
- Credit and debit cards (Visa, Mastercard, Revolut)
- Bank transfers (Unlimint, eMerchantpay and direct bank transfers)
- Crypto (through CoinPayments.net)

Score Range Payment Methods	Risk Rating
0 – 100	Low
101 – 200	Low – Medium
201 – 300	Medium
301 – 400	Medium – High
401 – 500	High

Table 11: *Payment methods – Inherent risk score range*

Vouchers		
Risk factors	**Answer**	**Score**
Is there a possibility of anonymity?	Yes	100
Is it possible to fund it anonymously?	Yes	100
Can it be reloaded?	No	0
Can a closed-loop policy be applied?	No	100
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes, but the AML obligations are less rigorous	81
Risk	**Medium – High**	**381**

Table 12: *Vouchers – Inherent risk rating*

Initial

DS

E-Wallets		
Risk factors	**Answer**	**Score**
Is there a possibility of anonymity?	Yes	100
Is it possible to fund it anonymously?	No	0
Can it be reloaded?	Yes	100
Can a closed-loop policy be applied?	Yes	0
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes, but the AML obligations are less rigorous	81
Risk	**Medium**	**281**

Table 13: *E-Wallets – Inherent risk rating*

Credit and debit cards		
Risk factors	**Answer**	**Score**
Is there a possibility of anonymity?	No	0
Is it possible to fund it anonymously?	No	0
Can it be reloaded?	Yes	100
Can a closed-loop policy be applied?	Yes	0
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes, in some cases	81
Risk	**Low – Medium**	**181**

Table 14: *Credit and debit cards – Inherent risk rating*

Bank transfers		
Risk factors	**Answer**	**Score**
Is there a possibility of anonymity?	Yes	100
Is it possible to fund it anonymously?	No	0
Can it be reloaded?	N/A	0
Can a closed-loop policy be applied?	Yes	0
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes	0
Risk	**Low**	**100**

Table 15: *Bank transfers – Inherent risk rating*

Crypto payments		
Risk factors	**Answer**	**Score**
Is there a possibility of anonymity?	Yes	100
Is it possible to fund it anonymously?	Yes	100
Can it be reloaded?	No	0
Can a closed-loop policy be applied?	No	100
Are they issued by a licensed financial institution in a reputable jurisdiction?	Yes, but the AML obligations are less rigorous	81
Risk	**Medium – High**	**381**

Table 16: *Crypto payments – Inherent risk rating*

The following tables provide the overall risk scoring range for payment methods and the overall inherent risk rating in relation to all the payment methods:

Overall Score Range Games	Risk Rating
0 – 500	Low
501 – 1000	Low – Medium
1001 – 1500	Medium
1501 – 2000	Medium – High
2001 – 2500	High

Table 17: *Overall inherent risk scoring range for Payment methods*

Payment methods	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Vouchers				381	
E-Wallets			281		
Credit and debit cards		181			
Bank transfers	100				
Crypto payments				381	
TOTAL	SCORE: 1,324 = RISK: Medium				

Table 18: *Overall inherent risk rating for Payment methods*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

2.3 Inherent risk – Jurisdictions and players

The company's customer base needs to be reviewed in detail (**when the Company become operational**) to determine which customer risk factors may increase the ML/FT risk of the Company. Subsequently, the following categories need to be used to stratify the customer base and identify aspects of customer risk:

PEP status, High value depositing players (VIP players), Customers with adverse news hit / sanctions hit, Customers who deposited or withdrew without gambling activity, High risk customers associated with high-risk industry, High-risk players and High-risk payment methods used.

The assessment should include a review of the geographic locations that the Company will target, as this factor is a core component of any inherent risk assessment. The Company has, in fact, evaluated the specific risks associated with doing business in, opening and servicing, offering products and services to and/or facilitating transactions involving certain geographic locations.

Each player type will be assigned a risk score to determine the ML/FT risk each category of players poses to the Company. The risk scoring range for player jurisdictions and different player types, as well as the risk factors identified and the risk ratings per jurisdiction and player types, is provided in the tables below:

Score Range Jurisdiction	Risk Rating
0 – 30	Low
31 – 60	Low – Medium
61 – 90	Medium
91 – 120	Medium – High
121 – 145	High

Table 19: *Player Jurisdiction – Inherent risk score range*

Player Jurisdictions		
Risk factors	**Answer**	**Score**
What % of players are resident in medium risk jurisdictions?	None – N/A – Inactive Operational Status at the moment	0
What % of players are resident in high-risk jurisdictions?	None – N/A – Inactive Operational Status at the moment	0
Player Jurisdiction Risk	**Low**	**0**

Table 20: *Player Jurisdiction – Inherent risk rating*

Initial

DS

Score Range PEPs	Risk Rating
0 – 36	Low
37 – 72	Low – Medium
73 – 108	Medium
109 – 144	Medium – High
145 – 183	High

Table 21: *PEPs – Inherent risk score range*

Politically Exposed Persons (PEPs)		
Risk factors	**Answer**	**Score**
What % of players are PEPs?	None (the Company does not accept PEPs as players)	0
What % of players are resident in high-risk jurisdictions?	None (the Company does not accept PEPs as players)	0
PEP Risk	**Low**	**0**

Table 22: *PEPs – Inherent risk rating*

Score Range High Depositors	Risk Rating
0 – 52	Low
53 – 105	Low – Medium
106 – 157	Medium
158 – 210	Medium – High
211 – 262	High

Table 23: *High depositors – Inherent risk score range*

High Depositors		
Risk factors	**Answer**	**Score**
What % of players have deposited (at least once) more than Euro 2,000 in one day?	N/A - Inactive Operational Status	0
What % of players have deposited (at least once) more than Euro 10,000 in one month?	N/A - Inactive Operational Status	0
What % of players have deposited (at least once) more than Euro 30,000 in a lifetime?	N/A - Inactive Operational Status	0
High Depositors Risk	**Low**	**0**

Table 24: *High depositors – Inherent risk rating*

Initial

DS

Score Range High Risk Players	Risk Rating
0 – 100	Low
101 – 200	Low – Medium
201 – 300	Medium
301 – 400	Medium – High
401 – 500	High

Table 25: *High risk players – Inherent risk score range*

High Risk Players based on Payment Methods		
Risk factors	**Answer**	**Score**
What % of players are considered to be high risk?	N/A - Inactive Operational Status	0
What % of total deposits are done through cards including prepaid cards?	N/A - Inactive Operational Status	0
What % of total deposits are done through e-wallets?	N/A - Inactive Operational Status	0
What % of total deposits are done through paysafe cards and vouchers?	N/A - Inactive Operational Status	0
What % of total deposits are done through crypto payments?	N/A - Inactive Operational Status	0
High Risk Players Risk	**Low**	**0**

Table 26: *High risk players – Inherent risk rating*

Initial

DS

The following tables provide the overall risk scoring range for players and the overall inherent risk rating in relation to all player types:

Overall Score Range Jurisdictions & Players	Risk Rating
0 – 218	Low
219 – 436	Low – Medium
437 – 654	Medium
655 – 872	Medium – High
873 – 1090	High

Table 27: *Overall inherent risk score range for Jurisdictions & Players*

Jurisdiction & Players	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Player jurisdictions	**0**				
PEPs	**0**				
High depositors	**0**				
High risk Players based on Payment methods	**0**				
TOTAL	**SCORE: 0 = RISK: LOW**				

Table 28: *Overall inherent risk rating for Jurisdictions & Players*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

2.4 Inherent risk – Delivery channels

Keep On Entertainment N.V. also assessed whether – and to what extent – the method of servicing the player could increase the inherent ML/FT risk.

As outlined in Curaçao's NRA and in the EU Supranational Risk Assessment: online gambling is exposed to a greater level of risk due to the huge volumes of transactions and the non-face-to-face nature of the business relationship.

The tables below contain the ranges of risk scores as well as the risk factor identified, and the inherent risk rating attributed in relation to the delivery channel.

Score Range Delivery Channel	Risk Rating
0 – 12	Low
13 – 25	Low – Medium
26 – 37	Medium
38 – 50	Medium – High
51 – 62	High

Table 29: *Delivery channel – Inherent risk score range*

Delivery Channel		
Risk factors	**Answer**	**Score**
Are players serviced on a non-face to face basis?	Yes (100% of our customer base)	62
Delivery Channel Risk	**High**	**62**

Table 30: *Delivery channel – Inherent risk rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

2.5 Total inherent risk

The total inherent risk of the games, payment methods, jurisdictions & players, delivery channel and EU SNRA & Curaçao NRA have been aggregated to give a final inherent risk score, which is provided in the table below.

Overall Range Inherent Risk	Risk Rating
0 – 970	Low
971 – 1940	Low – Medium
1941 – 2910	Medium
2911 – 3880	Medium – High
3881 – 4852	High

Table 31: *Overall inherent risk range*

Category of risk	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Games		324			
Payment methods			1,324		
Jurisdiction & Players	0				
Delivery channel					62
TOTAL	**SCORE: 1,710 = RISK: Low – Medium**				

Table 32: *Overall inherent risk rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

3. Determination of risk appetite

Risk appetite can be defined as the level and type of risk that an entity is willing to take in order to meet strategic objectives.

The Board of Directors and Senior Management of the Company have established a strong AML/CFT culture within the organization and are consistently increasing their efforts on different fronts to ensure that AML/CFT remains a priority for the organization. The Company's ML/FT risk appetite is grounded in the over-arching principle that any transactions that may remotely or indirectly be linked or somehow connected to money laundering or funding of terrorism will not be tolerated, and that business with individuals or entities that might be engaged in such activities will not be entertained. Every effort is being made to minimize the possibility of products of the Company unwillingly being used by launderers or terrorist financiers.

The Directors of the Company have taken a commitment that Keep On Entertainment N.V.'s overall risk appetite remains at least at a low-medium level by ensuring that adequate policies and procedures are implemented and applied in practice. Moreover, the Board together with the Senior Management has taken a number of decisions aimed at limiting risk, that are being listed below:

- Not allowing players to open more than one account per brand;
- Not accepting players (including temporary visitors) located in or residents of certain high-risk jurisdictions;
- Not offering high risk peer-to-peer gaming facilities;
- Obtaining information and, where necessary, documentation in relation to the source of funds / source of wealth of their customers;
- Only considering the acceptance of high-risk players once it is assured that appropriate controls have been applied to mitigate the risk;
- Not accepting any players posing a very high level of money laundering or terrorist financing risk;
- Dealing with reputable affiliates only;
- Dealing with reputable suppliers/3rd party providers only; and
- Carrying out effective transaction monitoring to ensure that any unusual activity is detected and investigated immediately.

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4. Analysis of AML/CFT controls

Following the identification and assessment of inherent risk, an evaluation was undertaken of the level and effectiveness of the AML/CFT controls that the Company has in place. The strength and effectiveness of the controls were assessed by an external Gaming Consultant company. It was examined whether existing controls are sufficiently robust to mitigate the Company's inherent risk and whether these are aligned with its risk appetite.

In view of the heightened risk identified within the sector in the EU Supranational Risk Assessment and the risk assessment carried out by the Curaçao National Risk Assessment, the expectations in respect of the controls implemented by online gambling companies to mitigate the non-face-to-face nature of the business are invariably expected to be higher. The assessment of the Company's controls has therefore taken this higher benchmark into account.

A breakdown of the strength of the controls per category is provided in the paragraphs hereunder.

4.1 Controls – Games

When assessing the controls in place in relation to games, all the games provided by the Company were assessed individually. The tables below provide the scoring range for controls in place for games, the control factors which impact specifically upon the games offered and the control rating per game type. Based on this assessment, the strength of the controls for each product category has been rated as shown below.

Although it resulted that the Company has controls in place that are effective in relation to games, there are certain areas which are either deficient or require improvements, as outlined in the below tables. The Company will be ensuring that these areas are improved.

Score Range Games	Control Rating
41 – 50	Satisfactory
31 – 40	Effective
21 – 30	Needs improvement
11 – 20	Poor
0 – 10	Deficient

Table 33: *Games control score range*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Casino games		
Control factors	**Answer**	**Score**
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Needs improvement	15
Has the monitoring done by the game provider been tested by Keep On Entertainment N.V.?	Deficient	0
Casino games control	**Effective**	**35**

Table 34: *Casino games – Control rating*

Sports betting		
Control factors	**Answer**	**Score**
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Satisfactory	20
Has the monitoring done by the game provider been tested by Keep On Entertainment N.V.?	Deficient	0
Sports betting control	**Satisfactory**	**40**

Table 35: *Sports betting – Control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Virtual games		
Control factors	**Answer**	**Score**
Are checks carried out by the game provider to identify irregular play, opposite betting- and suspicious activity?	Satisfactory	20
Does the game provider provide instant reporting on suspicious play?	Satisfactory	20
Has the monitoring done by the game provider been tested by Keep On Entertainment N.V.?	Deficient	0
Virtual games control	**Satisfactory**	**40**

Table 36: *Virtual games – Control rating*

The following tables provide the overall control scoring range for games and the overall control rating in relation to all games:

Overall Score Range Games	Control Rating
120 – 150	Satisfactory
90 – 119	Effective
60 – 89	Needs improvement
30 – 59	Poor
0 – 29	Deficient

Table 37: *Overall control score range for Games*

Games	Satisfactory	Effective	Needs improvement	Poor	Deficient
Casino games		35			
Sports betting	40				
Virtual games	40				
TOTAL	**SCORE: 115 = CONTROL: Effective**				

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Table 38: *Overall control rating for Games*

4.2 Controls – Payment methods

Each payment method offered by Keep On Entertainment N.V. has been assessed in terms of controls with the help of the Senior Management. The following tables provide a control scoring range that varies for each of the payment methods due to the different control factors which impact specifically upon the payment methods offered and the control rating per payment type. Based on this assessment, the strength of the controls for each payment method has been rated as shown below.

The Company has identified that the controls in relation to payment methods require some improvement. There are certain areas which are deficient, such as the inability to have a closed looped policy on every payment method, the inability to identify players using multiple payment methods, the application of EDD measures and the technological tools in place to monitor and detect suspicious activity for AML purposes, as outlined in the tables below.

In view of the risks posed by e-wallets, the Company considered introducing an internal policy that only allows one e-wallet per provider. This means that a player only allowed to use one e-wallet (for each e-wallet provider that is accepted by the Company) e.g., the player not be able to register two Skrill accounts but allowed to register one Skrill and one Neteller account with the Company.

Score Range Vouchers	Control Rating
101 – 125	Satisfactory
76 – 100	Effective
51 – 75	Needs improvement
26 – 50	Poor
0 – 25	Deficient

Table 39: *Vouchers control score range*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Vouchers		
Control factors	**Answer**	**Score**
In cases where a closed loop policy is not possible, is the risk mitigated?	Satisfactory	20
Is there a limit on the number of vouchers accepted per player?	Needs improvement	10
Is there a limit on the value uploaded per voucher?	Satisfactory	15
Is EDD carried out on players using vouchers?	Needs improvement	5
Are players using multiple vouchers (or making many payments through vouchers) identified and monitored?	Needs improvement	5
How strong is the Anti-fraud and payments team?	Needs improvement	15
How effective are the technological tools in place to monitor and detect suspicious activity for AML purposes?	Needs improvement	15
Vouchers control	**Effective**	**85**

Table 40: *Vouchers control rating*

Score Range E-wallets	Control Rating
101 – 125	Satisfactory
76 – 100	Effective
51 – 75	Needs improvement
26 – 50	Poor
0 – 25	Deficient

Table 41: *E-wallets control score range*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

E-wallets		
Control factors	**Answer**	**Score**
In cases where a closed loop policy is not possible, is the risk mitigated?	Satisfactory	20
Is there a limit on the number of E-Wallets accepted per player?	Satisfactory	20
Is there a limit on the value uploaded per wallet?	Needs improvement	5
Is EDD carried out on players using E-Wallets?	Needs improvement	5
Are players using multiple e-wallets actively identified and monitored?	Satisfactory	10
How strong is the Anti-fraud and payments team?	Needs improvement	15
How effective are the technological tools in place to monitor and detect suspicious activity for AML purposes?	Needs improvement	15
E-wallets control	**Effective**	**90**

Table 42: *E-wallets control rating*

Score Range Credit and debit cards	Control Rating
85 – 105	Satisfactory
64 – 84	Effective
43 – 63	Needs improvement
22 – 42	Poor
0 – 21	Deficient

Table 43: *Credit and debit cards control score range*

Credit and debit cards		
Control factors	**Answer**	**Score**
Is there a limit on the number of cards accepted per player?	Deficient	0
Are players using multiple cards identified and monitored?	Needs improvement	5
How strong is the Anti-fraud and payments team?	Needs improvement	15
How effective are the technological tools in place to monitor and detect suspicious activity for AML purposes?	Needs improvement	15
Are only 3D Secure cards accepted?	Yes	25
Credit and debit cards control	**Needs improvement**	**60**

Table 44: *Credit and debit cards control rating*

Score Range Bank transfers	Control Rating
54 – 65	Satisfactory
40 – 53	Effective
27 – 39	Needs improvement
14 – 26	Poor
0 – 13	Deficient

Table 45: *Bank transfers control score range*

Bank transfers		
Control factors	**Answer**	**Score**
In cases where a closed loop policy is not possible, is the risk mitigated?	Satisfactory	20
In cases where the Company does not receive the bank details of the player, is this risk being mitigated?	Satisfactory	20
In cases where the financial institution being used by the player is licensed in a high risk or non-reputable jurisdiction, is a measure applied to mitigate this risk?	Satisfactory	25
Bank transfers control	**Satisfactory**	**65**

Table 46: *Bank transfers control rating*

Initial

DS

Score Range Crypto payments	Control Rating
57 – 70	Satisfactory
43 – 53	Effective
29 – 42	Needs improvement
15 – 28	Poor
0 – 14	Deficient

Table 47: *Crypto payments control score range*

Crypto payments		
Control factors	**Answer**	**Score**
Is there a limit on the number/value of deposits accepted through Crypto wallets per player?	Needs improvement	10
How strong is the Anti-fraud and payments team?	Needs improvement	15
How effective are the technological tools in place to monitor and detect suspicious activity for AML purposes?	Needs improvement	15
Crypto payments control	**Needs improvement**	**40**

Table 48: *Crypto payments control rating*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

The following tables provide the overall control scoring range for payment methods and the overall control rating in relation to all payment methods:

Overall Score Range Payment methods	Control Rating
389 – 485	Satisfactory
292 – 388	Effective
195 – 291	Needs improvement
98 – 194	Poor
0 – 97	Deficient

Table 49: *Overall Payment methods control score range*

Payment methods	Satisfactory	Effective	Needs improvement	Poor	Deficient
Vouchers		85			
E-wallets		90			
Credit and debit cards			60		
Bank transfers	65				
Crypto payments			40		
TOTAL	**SCORE: 340 = CONTROL: Effective**				

Table 50: *Overall Payment methods control score range*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.3 Controls – Customer Due Diligence

The strength of the customer due diligence (CDD) carried out by the Company has also been assessed. Table 51 and 52 provide the control scoring range for CDD, the control factors which impact specifically on CDD, and the control rating for CDD. Based on this assessment, it was determined that controls in this area are:

Identification: the customer identification is being done when our customers registering a gaming account with us. We are asking for personal data set, such as first name, last name, date of birth, residential address, phone number, email address.

Verification: the customer verification is being done when our customers reached the mandatory KYC threshold Naf 4,000 – or equivalent in other currencies across brands. Customers can upload their KYC documents through an external, 3rd party provider (**SumSub, in conjunction with BetConstruct platform**) who is supporting the verification of the players. If a document is out of date, the Company is receiving alerts to request up to date documentation from our players.

Information on source of funds/source of wealth: the Company has adopted a procedure whereby information in relation to the occupation, source of funds and source of wealth is obtained directly from the player when the risk is high. This information is then backed up with supporting documents to confirm either the source of funds, source of wealth or both on a later stage or when the AML risk is high.

Enhanced Due Diligence: EDD is currently being conducted on players who ought to be subjected to EDD, such as high-risk players, PEPs and where we have concerns about the funds used to deposit with us.

Multiple accounts: The Company is able to identify duplicate accounts.

PEP and Sanction screening: The Company adopted an external provider (**SumSub**) to carry out PEP and Sanctions screening. Sanctions screening happens on the first deposit attempt of the player, just as PEP check.

Ongoing Monitoring: To ensure that the documentation held on players are kept up-to-date and we have information and documentation related to source of funds and affordability. Also, the Company is monitoring customer transactions at different financial thresholds and upon withdrawal stages.

Initial MC

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Score Range Customer Due Diligence	Control Rating
245 – 306	Satisfactory
184 – 244	Effective
123 – 183	Needs improvement
62 – 122	Poor
0 – 61	Deficient

Table 51: *CDD control score range*

Customer Due Diligence Control		
Control factors	**Answer**	**Score**
Does the Company have adequate written policies and procedures for CDD/KYC principles?	Yes	3
Have these been reviewed and updated?	Yes	3
Have the policies and procedures been communicated to employees and management concerned?	Yes	6
Does the Company have an updated and documented Customer Acceptance Policy?	Yes	6
Is there a system for testing compliance with the CDD policies and procedures, and the AML/CFT legislation?	Satisfactory	24
Has the appropriate level of due diligence, including source of wealth and funds (where necessary), been applied on all players?	Needs improvement	25
Does the company collect information on the financial situation and occupation of all players who reach high risk?	Satisfactory	30
Have documents to support the source of wealth and source of	Needs improvement	25

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

funds of high depositors been collected (where necessary)?		
Have appropriate EDD measures been applied on all PEPs?	No	0
Have appropriate EDD measures been applied on all high-risk players?	Yes	30
Is due diligence applied on affiliates?	No	0
Are affiliate player accounts monitored for suspicious activity?	Yes	6
Have all customers been screened for PEPs and Sanctions?	Yes	30
Does the Company have a system in place to ensure that documents and information on players are kept up to date?	Yes	30
Are systems in place to assess changes in PEP and sanction status of the customers?	Yes	30
CDD control	**Satisfactory**	**248**
TOTAL	**SCORE: 248 = CONTROL: Satisfactory**	

Table 52: *CDD control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.4 Controls – Delivery channels

The following tables provide the control scoring range in relation to the delivery channel, the control factors which impact specifically upon the delivery channel used, the control rating for the channel used. Based on this assessment, it was identified that the delivery channel is satisfactory in its controls since the Company has implemented a face verification tool (3rd party provider) in order to mitigate the non-face-to face risk of the Company.

Score Range Delivery channel	Control Rating
49 – 60	Satisfactory
37 – 48	Effective
25 – 36	Needs improvement
13 – 24	Poor
0 – 12	Deficient

Table 53: *Delivery channel control score range*

Delivery channel		
Control factors	**Answer**	**Score**
Are technological measures in place to mitigate the non-face to face risk?	Yes	30
Where a technological measure is not in place, is EDD being applied?	Yes	30
Delivery channel control	**Satisfactory**	**60**

Table 54: *Delivery channel control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.5 Controls – Risk assessment

The tables hereunder illustrate the control scoring range adopted in relation to the risk assessment carried out by the Company, the control factors which impact specifically upon the risk assessment conducted, the control rating for the assessment carried out, as well as the Curaçao FIU audit results. Based on this assessment, the strength of the controls for risk assessment has been rated as Effective. Keep On Entertainment N.V. need to introduce a new in-house tool, which will risk rate customers. The risk rating is determined based on a number of fields and scores assigned to particular factors. When a player's risk rating changes, an alert should be generated which will necessitate a review of the player account.

Score Range Risk Assessment	Control Rating
164 – 205	Satisfactory
123 – 163	Effective
83 – 122	Needs improvement
42 – 82	Poor
0 – 41	Deficient

Table 55: *Risk Assessment control score range*

Risk Assessment		
Control factors	**Answer**	**Score**
Does the Company have an ML/FT risk classification system in place that differentiates between lower and higher risk customers?	Satisfactory	30
How adequate is the risk assessment criteria that is being used?	Satisfactory	30
Have all the Company's players been adequately risk assessed?	Yes	30
Is an automated risk assessment tool used?	No	0
Are there processes to review client's risk profile?	Yes	30
How effective are the triggers in place to alert the Company that a player may have suddenly become higher risk?	Deficient	0
Are the Board and senior management kept abreast of changing ML/FT risk? If so, how is this communicated?	Yes	25
Risk assessment control	**Effective**	**145**

Table 56: *Risk Assessment control rating*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.6 Controls – Transaction monitoring and reporting

The tables hereunder provide the control scoring range applicable in relation to transaction monitoring and reporting carried out by Keep On Entertainment N.V., the control factors which impact specifically upon the monitoring and reporting conducted, the control rating in place for the monitoring and reporting carried out. Based on this assessment, the strength of the controls for transaction monitoring and reporting has been rated as Needs improvement.

Score Range Transaction monitoring	Control Rating
129 – 162	Satisfactory
97 – 128	Effective
65 – 96	Needs improvement
33 – 64	Poor
0 – 32	Deficient

Table 57: *Transaction monitoring and reporting control score range*

Transaction monitoring and reporting		
Control factors	**Answer**	**Score**
Does the Company have an adequate policy on transaction monitoring and reporting for AML purposes?	Yes	5
Does the company have an effective system to detect unusual transactions for AML purposes?	Needs improvement	25
Does the company have enough employees to monitor transactions effectively for AML purposes?	N/A	0
Is the company's reporting procedure adequate?	No	0
Are all employees aware of suspicious behaviour and what should be done when knowledge or suspicion of ML/FT is present?	Needs improvement	25
Has the company informed staff of the procedures for internal reporting of unusual/suspicious activity/transactions ('internal reports') to the MLRO?	Yes	11
How many internal unusual transaction reports were raised from January 2024 until present?	None	0
How many of these UTRs have resulted in a disclosure to the FIU?	None	0
What is the average time it takes the MLRO to review such reports and make a prima facie determination?	Cannot determine…	0
Transaction monitoring and reporting control	**Needs improvement**	**66**

Table 58: *Transaction monitoring and reporting control rating*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.7 Controls – Internal audit

The following tables provide the scoring range in relation to the internal audit function of Keep On Entertainment N.V., the control factors which impact specifically upon the internal audit function, the control rating for this function. Based on this assessment, the strength of the controls for internal audit has been rated as Needs improvement. The Company at a later stage (1 year after it become fully operational) can either develop an internal audit function or ask an external company who can review and test the AML/CFT program together.

Score Range Internal Audit	Control Rating
40 – 48	Satisfactory
30 – 39	Effective
20 – 29	Needs improvement
10 – 19	Poor
0 – 9	Deficient

Table 59: *Internal audit control score range*

Internal Audit		
Control factors	**Answer**	**Score**
Does the Company have an Internal or external Audit Department/function?	No	0
Has the AML/CFT program been reviewed and tested?	Yes	24
Internal Audit control	**Needs improvement**	**24**

Table 60: *Internal audit control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.8 Controls – Record keeping

The following tables provide the scoring range in relation to record keeping, the control factors which impact specifically upon record keeping and the control rating. Based on this assessment, the strength of the controls for record keeping has been rated as Effective. Need to be noted, that the Company should later on hire a Data Protection Officer (DPO), who will be responsible to test the record keeping procedures.

Score Range Record keeping	Control Rating
46 – 56	Satisfactory
35 – 45	Effective
23 – 34	Needs improvement
12 – 22	Poor
0 – 11	Deficient

Table 61: *Record keeping control score range*

Record Keeping		
Control factors	**Answer**	**Score**
Has this record keeping procedure been tested?	Yes	5
Do records provide a clear audit trail?	Needs improvement	19
How long would it take to retrieve the information for a particular customer going back 5 years?	24 hours	17
Has there ever been a request for information from the authorities (e.g. Curaçao FIU) for customer data where information could not be provided?	N/A	0
Has the casino asked for an extension from the authorities in order to be able to meet these requests for information?	N/A	0
Record Keeping control	**Effective**	**41**

Table 62: *Record keeping control rating*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.9 Controls – Training and HR

The following tables provide the scoring range applied in relation to training of employees of Keep On Entertainment N.V. in relation to AML/CFT and to the vetting of employees, the control factors which impact specifically these areas, the control rating, as well as any audit results. Based on this assessment, the strength of the controls for training and HR has been rated as Deficient.

Training: The nominated Compliance Officer/MLRO should provide an AML/CFT training to the employees of Keep On Entertainment N.V., also providing specific training in relation to their AML/CFT obligations. This training should include the Board of directors and Senior management of the Company.
Vetting of Employees: The Company is requesting documentation prior to recruiting a new employee and carry out screening to identify whether the employee has a criminal record.

Score Range Training and HR	Control Rating
63 – 78	Satisfactory
48 – 62	Effective
32 – 47	Needs improvement
17 – 31	Poor
0 – 16	Deficient

Table 63: *Training and HR control score range*

Training and HR		
Control factors	**Answer**	**Score**
Is the company's staff trained to understand how AML/CFT applies to their specific model and the roles they undertake?	Deficient	0
What is the frequency of AML/CFT training provided?	Yearly	4
Does the Company provide internal AML/CFT training to employees?	No	0
Has the Board and senior management participated in AML/CFT training?	No	0
Are staff tested for knowledge retention following AML/CFT training?	No	0
Does the company screen prospective employees (e.g. criminal records)?	Yes	5
Is staff screened for criminal record during employment?	No	0
Training and HR control	**Deficient**	**9**

Table 64: *Training and HR control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.10 Controls – MLRO and compliance

The control scoring range in relation to the function of the MLRO and the Compliance Department is provided in the tables below, together with the control factors which impact specifically these areas, the control rating. Based on this assessment, the strength of the controls for the MLRO and Compliance function has been rated as shown below.

The strength of the control was rated as Needs improvement, and it should be noted that the Company should set up a compliance/legal department after it becomes operational.

Score Range MLRO and compliance	Control Rating
134 – 166	Satisfactory
101 – 133	Effective
67 – 100	Needs improvement
34 – 66	Poor
0 – 33	Deficient

Table 65: *MLRO and compliance control score range*

MLRO and compliance		
Control factors	**Answer**	**Score**
Has the Company appointed an MLRO?	Yes	5
How effective is the MLRO in carrying out his duties?	Satisfactory	30
Does the MLRO carry out other duties besides AML/CFT?	Yes	0
What proportion of time is devoted to AML/CFT issues?	Between 50-69%	25
Is the MLRO able to act independently?	Yes	3
Is the MLRO able to communicate easily and effectively with the Board?	Yes	5
Does the MLRO receive support from senior management?	Yes	5
Does the MLRO have access to all records, data and documentation?	Yes	5
Is there a compliance unit?	No	0
How many employees make up this unit?	None	0
How much of the Fraud unit's time is dedicated to AML/CFT?	Less than 50	0
How many employees make up this unit?	Less than 3	6

Initial

DS

Do the employees have some experience working in AML/CFT compliance?	Needs improvement	6
MLRO and compliance control	**Needs improvement**	**90**

Table 66: *MLRO and compliance control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.11 Controls – Governance

The scoring range in relation to the Governance function, the control factors which impact specifically this area, and the control rating are included in the tables below. Based on this assessment, the strength of the controls for the Governance function has been rated as Satisfactory.

It should be highlighted that the Company have an adequate AML/CFT procedures manual in place and the Board receive or discuss compliance issues as needed.

Score Range Governance	Control Rating
90 – 111	Satisfactory
68 – 89	Effective
45 – 67	Needs improvement
23 – 44	Poor
0 – 22	Deficient

Table 67: *Governance control score range*

Governance		
Control factors	**Answer**	**Score**
Does the Company have written AML/CFT procedures?	Satisfactory	5
Has the Board designated any of its members responsible for AML/CFT issues?	Needs improvement	6
Does the Board/ Senior management ensure that the AML/CFT program, including risk management, is effectively implemented by all relevant departments?	Needs improvement	25
Does the Board receive reports or updates on AML/CFT issues and programs?	Needs improvement	25
Are AML/CFT related matters discussed at least once quarterly?	Needs improvement	2
Is the MLRO of sufficient seniority to influence the board?	Yes	30
Governance control	**Satisfactory**	**93**

Table 68: *Governance control rating*

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.12 Controls – Outsourcing

All outsourcing relationships hold risks. Being aware of the potential risks involved and having ability to monitor, evaluate and manage these risks is crucial for the Company.

The scoring range in relation to the Outsourcing function, the control factors which impact specifically this area, and the control rating are included in the tables below. Based on this assessment, the strength of the controls for the Outsourcing function has been rated as Satisfactory.

It should be highlighted that the Company have an adequate AML/CFT procedures manual in place to control the risk derived from outsourcing such functions as our AML/CFT obligations.

Score Range Outsourcing	Control Rating
121 – 150	Satisfactory
91 – 120	Effective
61 – 90	Needs improvement
31 – 60	Poor
0 – 30	Deficient

Table 69: *Outsourcing control score range*

Outsourcing		
Control factors	**Answer**	**Score**
Does the outsourcing negatively prejudice the Company's ability to comply with its obligations at law and the effectiveness of the Company's compliance and audit functions?	Satisfactory	30
Does the third party have the necessary resources, qualifications, skills and authorisations (if required) at its disposal to effectively carry out the measures and procedures to perform on behalf of the Company?	Needs improvement	25
Does the manner in which the third party proposes to implement the General Outsourced Activities on behalf of the Company is in line with all applicable legal requirements and the Company's own policies and procedures?	Needs improvement	25

Initial

DS

Is the third party in good standing? (There being no adverse information in its regard, and it is located and operating from Curaçao, an EU Member State or another reputable jurisdiction)	Yes	30
Is the third party not subject to any obligation that would lead to a breach of any data protection, professional secrecy, confidentiality or non-disclosure obligation to which the Company has to adhere?	Yes	30
Outsourcing control	**Satisfactory**	**140**

Table 70: *Outsourcing control rating*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

4.13 Overall controls

The control scored for each of the above factors assessed have been aggregated to give a final overall control score which is provided in the table below.

Overall Score Range Controls	Control Rating
1581 – 1977	Satisfactory
1186 – 1580	Effective
791 – 1185	Needs improvement
396 – 790	Poor
0 – 395	Deficient

Table 71: *Overall controls score range*

Category of controls	Satisfactory	Effective	Needs improvement	Poor	Deficient
Games		115			
Payment methods		340			
Customer Due Dil.	248				
Delivery channels	60				
Risk Assessment		145			
Transaction monitoring			66		
Internal audit			24		
Record keeping		41			
Training and HR					9
MLRO and compliance			90		
Governance	93				
Outsourcing	140				
TOTAL	**SCORE: 1,371 = CONTROL: Effective**				

Table 72: *Overall rating for controls*

As we can see in the table above (Table 72) some of the controls are satisfactory in mitigating some of the risks of money laundering and terrorist financing to which the Company is exposed, however some of these controls needs improvement.

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

5. Determination of residual risk

The assessment concluded that the Company's total inherent risk is set at **Low-Medium**. This rating is derived from the assessment of the nature of the games offered, the type of payment methods the Company accepts, the type and volume of players it entertains, and the delivery channels it uses to onboard players. The strength of the Company's AML/CFT controls to mitigate such risks were also assessed and rated as **Effective**.

The residual risk is made up of the Company's inherent risk and the controls the Company has in place to mitigate those risks. The residual risk of the Company is presented using the heatmap in Table 73 below which is a standard template used for ML/FT risk assessments. Keep On Entertainment N.V.'s overall residual risk has been determined to be **Low-Medium**.

Inherent Risk	Satisfactory	Effective	Needs Improvement	Poor	Deficient
High	Medium	Medium-High	High	Extreme	Extreme
Medium-High	Low-Medium	Medium	Medium-High	High	Extreme
Medium	Low-Medium	Low-Medium	Medium	Medium-High	High
Low-Medium	Low	Low-Medium	Low-Medium	Medium	Medium-High
Low	Low	Low	Low-Medium	Low-Medium	Medium

Control Effectiveness

Table 73: *Residual risk heatmap*

The residual risk applicable in relation to games, payment methods, jurisdictions and players, delivery channels and risk assessment is broken down in the sections hereunder.

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

5.1 Residual risk – Games

The score for the overall residual risk of games is presented in the table below, taking into consideration the results of the inherent risk and the strength of controls calculated previously in relation to each type of game.

Games	Inherent Risk	Control Strength	Residual Risk
Casino games	Low – Medium	Effective	Low – Medium
Sports betting	Medium	Satisfactory	Low – Medium
Virtual games	Low – Medium	Satisfactory	Low
Overall Residual Risk - Games	**Low – Medium**	**Effective**	**Low – Medium**

Table 74: *Overall residual risk rating - Games*

5.2 Residual risk – Payment methods

Payment methods	Inherent Risk	Control Strength	Residual Risk
Vouchers	Medium – High	Effective	Medium
E-Wallets	Medium	Effective	Low – Medium
Credit and debit cards	Low – Medium	Needs improvement	Low – Medium
Bank transfers	Low	Satisfactory	Low
Crypto payments	Medium – High	Needs improvement	Medium – High
Overall Residual Risk – Payment methods	**Medium**	**Effective**	**Low – Medium**

Table 75: *Overall residual risk rating - Payment methods*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

5.3 Residual risk – Jurisdictions and players

When calculating the residual risk arising from the jurisdiction risk and customer base, the controls in place that relate to customer due diligence, risk management, transaction monitoring and reporting, internal audit, record keeping, training and HR, the strength of the function of the MLRO and the Compliance Department as well as governance were considered. For the inherent risk, the category was grouped under the single heading of 'Jurisdictions and Players'.

Players	Inherent Risk	Control Strength	Residual Risk
Player jurisdictions	Low	Effective	Low
PEPs	Low	Satisfactory	Low
High depositors	Low	Needs improvement	Low – Medium
High risk players	Low	Needs improvement	Low – Medium
Overall Residual Risk – Players	**Low**	**Needs improvement**	**Low – Medium**

Table 76: *Overall residual risk rating - Players*

5.4 Residual risk – Delivery channels

The scoring for the overall residual risk of delivery channels being used took into consideration the results of the inherent risk and the strength of controls calculated previously in relation to the delivery channel.

Delivery channel	Inherent Risk	Control Strength	Residual Risk
Overall Residual Risk – Delivery channel	**High**	**Satisfactory**	**Medium**

Table 77: *Overall residual risk rating - Delivery channel*

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

5.5 Total residual risk

The total residual risk of the games, payment methods, jurisdictions & players, delivery channel have been aggregated to give a final residual risk score which is provided in the table below.

Category of risk	Low risk	Low-Medium risk	Medium risk	Medium-High risk	High risk
Games		X			
Payment methods		X			
Jurisdiction & Players		X			
Delivery channel			X		
TOTAL	**RISK: Low – Medium**				

Table 78: *Overall residual risk range*

Summary of Overall residual risk for:

- Games: Low - Medium
- Payment methods: Low - Medium
- Players & Jurisdictions: Low - Medium
- Delivery channel: Medium

Residual risk is the level of risk left after applying the mitigating measures, policies, controls and procedures to the level of inherent risk identified. Level of inherent Risk - Mitigating Measures = Level of Residual Risk. **Overall residual risk of the business is Low – Medium**.

Initial

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

6. Remediation plan

Keep On Entertainment N.V. is committed to keep working to improve its controls to ensure that the residual risk of the Company is reduced and to also ensure, on a consistent basis, that any gaps identified are remediated as a matter of priority.

A list of action points has been drawn up, outlined in the table below, that the Company will be actioning depending on the priority set to each action point:

HIGH PRIORITY	
Training	The Company should train all relevant staff who will be customer facing. The training can be differentiated between employees / departments, meaning employees with more responsibility can receive more detailed training.

MEDIUM PRIORITY	
Payment methods	The Company should mitigate the risk with some of the payment methods, such as credit/debit cards to integrate limits on how many cards can be used by each customer.
Transaction monitoring	Keep On Entertainment need to improve how they will monitor transactions, especially if the company becomes operational and volumes will increase.
Development of a Compliance team	With Company growth it will be useful to have a separate Compliance Department looking after regulatory compliance.

LOW PRIORITY	
Internal audit	The Company at a later stage (1 year or so from the date they become operational) should either create an internal audit function or seek help with an external audit to check all policies & procedures and carry out a gap analysis in the business to further improve the system and be more compliant.
DPO function	The Company currently has no DPO to oversee how data has been used within the Company. At a later stage (with Company growth) it is highly recommended to hire a DPO to avoid any data leakage.

Initial MC

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

7. Conclusion

This document describes the purpose, scope and methodology used for the business risk assessment of Keep On Entertainment N.V. and provides an overview of its conclusions.

Through the assessment it was concluded that presently the Company faces an overall residual risk of **Low – Medium** which poses a considerable risk in terms of AML/CFT. In this regard there are a number of actions that are considered necessary for Keep On Entertainment N.V. to take to ensure that the Company's processes are brought in line with all its obligations and to safeguard it from being used as a vehicle for ML/FT.

A number of recommendations are therefore being made in this report.

Appendix I – Business Risk Assessment excel sheet (scoring and weighing)

The Appendix can be found on a separate excel sheet, which will be always provided together with this Business Risk Assessment.

Initial MC

DS

Docusign Envelope ID: 78C3A236-0F37-4538-A25F-2F12692A2A71

Board of Directors signature page

DocuSigned by:
215940689FEB429...

16/05/2025

_____

Starkeast Management B.V., Managing Director
By: Menno Jordaan, as director of Starkeast Management B.V.

Signed by:
C844330A35F54B6...

16/05/2025

_____

Mark Cauchi
Key Compliance / MLRO

Initial

DS