

# NEROBLANKO TECH B.V.

## Business Risk Assessment

|                 |                      |
|-----------------|----------------------|
| Version:        | 1.0                  |
| Last Update:    | 2024-09-26           |
| Applicability:  | Neroblanco Tech B.V. |
| Owner:          | MLRO                 |
| Approver:       | CEO                  |
| Security Class: | Internal             |

Revision History

| Version | Date       | Author | Comment       |
|---------|------------|--------|---------------|
| 1.0     | 26.09.2024 | MLRO   | First version |
| 1.0     | 26.09.2024 | CEO    | Approval      |

## Table of Contents

|                                                  |    |
|--------------------------------------------------|----|
| 1. INTRODUCTION                                  | 4  |
| 2. ASSESSMENT METHODOLOGY                        | 4  |
| 2.1. Risk Scoring                                | 5  |
| 2.2. Controls Scoring                            | 5  |
| 3. BUSINESS RISK ASSESSMENT REPORT               | 5  |
| 3.1. Customer Risk Category                      | 5  |
| 3.2. Distribution Channel Risk Category          | 9  |
| 3.3. Geographical and Jurisdiction Risk Category | 12 |
| 3.4. Payment Instruments Risk Category           | 14 |
| 3.5. Product Risk Category                       | 16 |
| 3.6. Internal risk Category                      | 20 |
| 3.7. Conclusion                                  | 22 |

## 1. INTRODUCTION

A business risk assessment ("BRA") for the purposes of AML Compliance Program is a process whereby the Company identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT/FP risks.

The BRA serves as the basis to determine which areas to prioritize in terms of AML/CFT/CFP and ensure that policies, procedures and controls are commensurate to the ML/FT/FP risks that are faced.

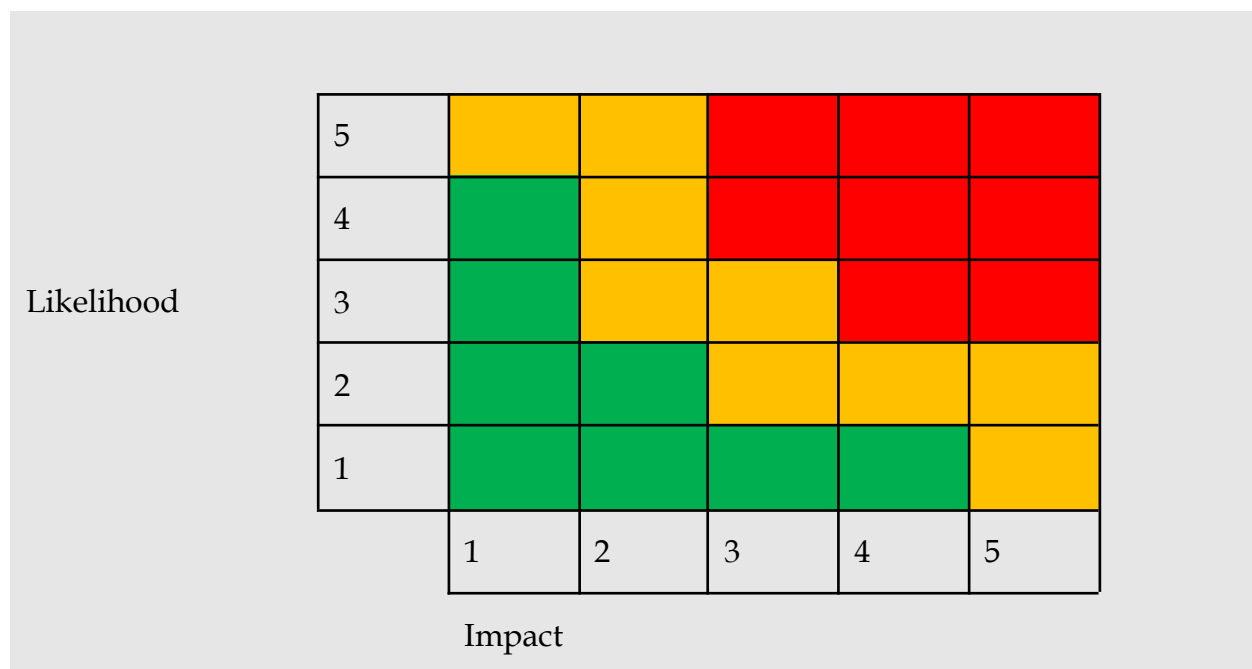
This BRA forms an integral part of the Company's AML Compliance Program. It should be read in conjunction with the Company's AML, CFT and CFP Policy (the "AML Policy").

Terms not otherwise defined herein have the same meaning as in the AML Policy.

## 2. ASSESSMENT METHODOLOGY

The Company has examined the threats and vulnerabilities it faces in its operations and has put in place controls based on the likelihood that a threat will take place, as well as assessed the impact a threat might have on the Company. To this extent a point matrix was used to determine the preparedness of the Company in the event of a threat emerging, as well as how effective each control is in the context of the threat level.

The matrix consists of a 2-axis table measuring the congregation point of likelihood and impact. The "X" axis measures Risk Impact and ranges between a value 1 which describes a negligible impact up to value 5 which describes a very high impact. The "Y" axis describes Risk Likelihood and ranges between a value of 1 which describes an improbable likelihood up to a value of 5 which describes an almost certain likelihood.



*Risk Matrix Chart Visual Representation*

## 2.1. Risk Scoring

The risk score is determined based on both relevant factors and will be obtained by multiplying the likelihood that the risk will occur with the possible impact it will have.

Based on the above-mentioned calculation the following risk ranges are possible:

**LOW** – Between risk score 1 and 4 inclusive

**MEDIUM** – Between risk score 5 and 10 inclusive

**HIGH** – Above 12

## 2.2. Controls Scoring

The measures and controls are broken down into 3 categories that determine how effective they are within their scope and how much of the risk they are able to mitigate. The scores range between 1 which represents a weak mitigation score and only caters to roughly 25% of the inherent risk score, up to 3 which caters to up to 75% of the inherent risk score.

Due to the high-risk nature of the online gambling industry, it will be assumed that it is impossible to fully mitigate an inherent risk therefore the minimum possible residual risk will be 25% of the inherent risk.

The mitigation and controls scores will be described as follows:

**WEAK** – 1 – Mitigates roughly 25% of the inherent risk score

**EFFECTIVE** – 2 – Mitigates roughly 50% of the inherent risk score

**STRONG** – 3 – Mitigates roughly 75% of the inherent risk score

# 3. BUSINESS RISK ASSESSMENT REPORT

## 3.1. Customer Risk Category

The customer risk covers all inherent risks referring to how each typology of customer might maliciously misuse the services offered by Company to attempt to launder proceeds of crime. This risk category analyzes the way unsavory individuals might attempt to bypass the security protocols put in place by the Company in order to further their own agenda.

All remote businesses have the inherent risk of not being able to physically meet the customers with which they engage in a business relationship. To this extent it becomes more difficult to establish the customer's identity as well as making it less comfortable to communicate with the customer as channels involve long-distance communication.

It has been identified that one of the highest risk indicators of money laundering is the probability of gambling anonymously on online gambling websites. This is due to the fast-paced nature and complexity of the transactions that can be processed in the online environment. Even though procedures are put in place to mediate the risk in these situations, they are not sufficient to fully negate the inherent risk of the possibility of ML/FT/FP.

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                                                                                                                                                                                    | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Irregular spending and multiple income streams of a customer make it more difficult to verify the legitimacy of funds used to gamble.                                                                                                 | 3(MEDIUM)         | 5(HIGH)       | 15 (HIGH)              |
| Use of fake documents                                                                                                                                                                                                                 | 3(MEDIUM)         | 5(HIGH)       | 15 (HIGH)              |
| Sanctioned country individuals receiving a Bank ID while living in a country that accepts such verification methods then returning to their home countries and providing the bank id to criminal networks for use in ML/FT/FP actions | 2(LOW)            | 5(HIGH)       | 10 (MEDIUM)            |
| Gambling group using account on behalf of customer                                                                                                                                                                                    | 3(MEDIUM)         | 3(MEDIUM)     | 9(MEDIUM)              |
| Account takeover via different hacking forms                                                                                                                                                                                          | 3(MEDIUM)         | 5(HIGH)       | 15 (HIGH)              |
| Customers illogical and erratic spending habits left unmonitored                                                                                                                                                                      | 4(MEDIUM)         | 5(HIGH)       | 20 (HIGH)              |
| Customers spreading expenditure across multiple gambling platforms                                                                                                                                                                    | 3(MEDIUM)         | 2(LOW)        | 6(MEDIUM)              |
| Customer ongoing monitoring not generating sufficient flags                                                                                                                                                                           | 3(MEDIUM)         | 3(MEDIUM)     | 9(MEDIUM)              |
| Minors having access to their relatives' banking/account/credit information                                                                                                                                                           | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Customer verification data becoming invalid or expired during a business relationship                                                                                                                                                 | 3(HIGH)           | 4(HIGH)       | 12(HIGH)               |

|                                                                                                                                       |        |         |            |
|---------------------------------------------------------------------------------------------------------------------------------------|--------|---------|------------|
| Customers belongs to terror cells and using gambling operators to transfer funds between accounts                                     | 1(LOW) | 5(HIGH) | 5(MEDIUM)  |
| The customer is a not a natural person but an entity / organization / syndicate setup to launder funds or for other nefarious reasons | 2(LOW) | 5(HIGH) | 10(MEDIUM) |
| Customers using sports betting to collude funds using sports betting                                                                  | 2(LOW) | 5(HIGH) | 10(MEDIUM) |
| Customers create multiple accounts and use them to create a more complex transaction history                                          | 2(LOW) | 4(HIGH) | 8(MEDIUM)  |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                                                                                                                                                                                                                                           | Effectiveness |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>SOW and SOF Verification</b> – the Company verifies the SOW and SOF of the customers in all cases of elevated risk. This allows to match spending with income sources and deal with irregular spending and multiple sources of income by detecting and verifying the authenticity of each transaction. This also allows the Company to form expectations as to usual / maximum /typical transactions performed by the relevant customer.           | STRONG        |
| <b>Automated 3<sup>rd</sup>-party information check</b> – Company checks the information gathered on the customers and IPs using specialized software to detect fake identities, fraudulent activities, adverse media etc.                                                                                                                                                                                                                            | EFFECTIVE     |
| <b>On-Boarding and Customer Acceptance</b> – the Company defines the customers that it is willing to form a long term business relationship with, as well as clearly mentions that only customers that are willing to utilize their accounts for the sole purpose it was intended to be used (entertainment) are allowed to enter a business relationship and/or continue said business relationship in case variables regarding customer behavior or | EFFECTIVE     |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| account details (address, bank account, etc) change. The policies also cover the fact that new accounts will be scanned for PEP and Sanction status, and based on results will be treated accordingly (PEP – management approval to continue business relationship etc., Sanctioned individuals – discontinuation of business relationship)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |
| <b>Customer Risk Assessment</b> – All new accounts receive a review of their details based on which an initial risk profile is determined. This allows the Company relevant departments to allocate resources effectively in tackling and mitigating high risk situations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | STRONG    |
| <b>New Customer Identity, UBO, Purpose Verification</b> – Company identifies new customers and verify their identity, perform other CDD measures and scrutinize new accounts for any irregularities in order to update customer risk profiles, as well as check any trends that might occur in the registration process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | EFFECTIVE |
| <b>Ongoing customer activity monitoring</b> – Based on the risk score attached to the customer's profile, as per the Customer Risk Assessment Procedure customers that are deemed to be of a higher risk rating (above Medium Risk) will receive constant manual monitoring performed by the relevant departments on a constant basis to ensure that if any changes in the expected and established customer behavior changes so that the risk profile can be updated accordingly and the changes reported to management. During this monitoring process customers will also be scanned to ensure no change has occurred in their PEP or Sanctioned individual status. Automated monitoring is also implemented to ensure that triggers are set off at specific thresholds (as described in the Prevention of Money Laundering Policy), based on which accounts will be subject to scrutiny and reported either internal or to the relevant authorities if the case arises. | EFFECTIVE |
| <b>MLRO review of suspicious cases</b> – Based on the reporting chapter described in the AML/FT/FP procedure, outstanding cases are reported to the MLRO for in-depth review and a report is generated based on the findings. The report is stored in the customer profile and is referred to in further analysis on the customer's profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | EFFECTIVE |
| <b>External AML Consultants policy and individual case review</b> – Company employs assistance from high rated consultancy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | STRONG    |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| <p>firms that provide assistance as well as input when it comes to high level decision regarding ML/FT/FP procedures and individual cases. The consultants offer effective services to ensure that all policies are up to date and contain all relevant information. In situations where a reported case requires a second specialized opinion the MLRO requests input from the consultants to ensure that all information and documentation was analyzed correctly and in a fair manner.</p>                                                                                                                                                                                                                                                                                         |        |
| <p><b>Relevant departments, MLRO and Management training</b> – All relevant personnel receive periodic training (at least once every 12 months, when there is a change in relevant regulation or when training is deemed necessary) as per the training chapter included in the AML/FT/FP policy. This ensures that relevant employees and departments have the necessary know-how to tackle situations where ML/FT/FP knowledge is required as well as understand the reporting flow to forward the case information to the MLRO and to Management. The MLRO goes through constant training in order to understand the relevant legislation and to apply it in the most effective way. Management receives training to understand the purpose and best solution for escalations.</p> | STRONG |
| <p><b>Duplicate or linked account verification</b> – Company trained employees verify the information on accounts that are suspected of being duplicate or being linked to other accounts. Customers may attempt to create multiple accounts or use the gambling services offered by the Company websites in order to take advantage of the initial interaction bonus offer or take advantage of unknown game vulnerabilities. To this extent accounts are verified using various tools (ip trackers, public online records) to determine whether accounts are linked in order to enable fraud or ML/FT/FP</p>                                                                                                                                                                        | STRONG |

|                                |              |
|--------------------------------|--------------|
| Category Inherent Risk         | 12(HIGH)     |
| Category Control Effectiveness | 2(EFFECTIVE) |
| Category Residual Risk         | 7 (MEDIUM)   |

### 3.2. Distribution Channel Risk Category

The Distribution Channel Risk Category covers the possible risks that can arise when it

comes to the amount of control as well as the level of transparency Company has in regard to the games provided by third parties, as Company do not offer their own gaming individual products (casino games, live casino, sportsbook), instead opting to lease these products from third party distributors. To this extent, the Company goes to great lengths to ensure that the quality of the product offered is up to par with all regulations imposed, as well as ensure that AML/FT/FP regulations are respected.

Taking into consideration the fact that the online ecosystem allows for transactions and financial flows to have a very dynamic nature as well as constantly increase in value, the Distribution Channels also get affected, thus increasing the Risk Factor for this category.

The Distribution channel risk assessment tackles the control Company has over the offered product when it is offered to the customers. In certain situations, this control may be shared with the Gaming Suppliers offering the product, thus the communication between Company and the Gaming Supplier also needs to be assessed within this category.

It has been also taken into account that certain game vulnerabilities may be abused in order for the customer to be able to easier obtain funds in a fraudulent manner thus making it easier for deposited funds to be rolled over (wagered) and withdrawn, thus increasing the risk of money laundering. Another issue taken into account is the fact that malicious individuals may manipulate sports book odds in order to launder money or tip the scales in their favor. This has been taken into account and is being combatted using tight communication with the odds provider.

Additionally, While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still considered as a risk factor for risk of identity fraud or impersonation present in these situations.

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                                                                          | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Gaming suppliers not performing their legal duties in a compliant manner                                                    | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Gaming suppliers not offering the relevant options within the product                                                       | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Gaming suppliers not keeping the relevant records regarding gaming sessions for comparison reasons in case of discrepancies | 2(LOW)            | 3(MEDIUM)     | 6(MEDIUM)              |
| Gaming suppliers' policies and procedures                                                                                   | 1(LOW)            | 3(MEDIUM)     | 3(MEDIUM)              |

|                                                                                                                                                                               |           |           |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|------------|
| not up to date with the latest legislation                                                                                                                                    |           |           |            |
| Abuse of specific game mechanics to enable faster withdrawals or fraudulently make extra winnings                                                                             | 4(HIGH)   | 4(HIGH)   | 16(HIGH)   |
| Customer chat triggers within Live Casino Games that could offer insight on players attempting fraud or money laundering not reaching the relevant departments within Company | 1(LOW)    | 5(HIGH)   | 5(MEDIUM)  |
| Insufficient communication between Company and the Gaming Supplier                                                                                                            | 1(LOW)    | 3(MEDIUM) | 3(LOW)     |
| Sports Betting odds could be manipulated by malicious individuals for the purpose of fraud or money laundering                                                                | 2(LOW)    | 5(HIGH)   | 10(MEDIUM) |
| Identity theft or fraud enabled by the non-face-to-face nature of the delivery channels.                                                                                      | 3(MEDIUM) | 5(HIGH)   | 15(HIGH)   |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                                                                                                                                                                                                                                     | Effectiveness |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Constant communication with Gaming Suppliers</b> – Company has a dedicated Game Management department that keeps constant communication with all the Gaming Suppliers that provide the content customers use on the Company website. These communications include all required information exchange between Company and the Gaming supplier to ensure that there is constant understanding as to what steps need to be followed at all times | STRONG        |
| <b>Effective and Timely CDD measures</b> – Company strives to perform CDD measures and collect the relevant due diligence documentation on an ongoing manner and before the statutory thresholds are reached. This provides effective screening against identity theft and other risks associated with                                                                                                                                          | STRONG        |

|                                                                                                                                                                                                                                                                                                                                                                                        |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| non-face-to-face transactions.                                                                                                                                                                                                                                                                                                                                                         |           |
| <b>Information requests from Gaming Suppliers</b> - Company compliance department and MLRO will, when the need arises request information from Gaming Suppliers on specific play sessions or customers to compare the information with what was gathered internally and ensure that the information collected is correct, and to be able to fix any irregularities in case they appear | EFFECTIVE |
| <b>Internal Product Audits/Checks</b> - Company checks products that are offered through the website to ensure that the products have all functionality and the offer is compliant with current legislation.                                                                                                                                                                           | EFFECTIVE |
| <b>Suspicious activity Reporting</b> - Company staff check and report upon any suspicious activity that might arise from player behavior and if investigation requires it extra information can be requested from the Gaming Suppliers                                                                                                                                                 | EFFECTIVE |
| <b>Customer ongoing sportsbook transaction monitoring</b> - Company specialized sports book staff constantly monitor sports book transactions to ensure that there is no foul play. All suspicious transactions are also checked with the odds provider to ensure that no issues exist platform wide.                                                                                  | EFFECTIVE |

|                                       |               |
|---------------------------------------|---------------|
| <b>Category Inherent Risk</b>         | 9(MEDIUM)     |
| <b>Category Control Effectiveness</b> | 2 (EFFECTIVE) |
| <b>Category Residual Risk</b>         | 5(MEDIUM)     |

### 3.3. Geographical and Jurisdiction Risk Category

Taking into consideration the nature of the Online Gambling industry, a clear factor of risk is the fact that services provided by the Company websites can be accessed from jurisdictions located outside of the scope of the license, even though thorough measures have been taken to ensure that only the customers in targeted jurisdictions have access to the provided gambling services. This may cause operator exposure to potential customers that intend to misuse the services provided in order to forward their own malicious agenda (fraud, money laundering, funding of terrorism).

Another relevant issue is the injection of illicit funds coming from sanctioned jurisdictions.

This is a very relevant issue as it poses a great risk of funds obtained through high-level corruption or violent crime to be laundered through gambling services and then reintroduced in the financial circuit ready to be spent.

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                                                                                                                                                                                                           | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Account registered through legitimate identification information gets used by the customer from a sanctioned jurisdiction, or the customer allows malicious individuals from sanctioned jurisdictions to use their account                                   | 3(MEDIUM)         | 5(HIGH)       | 15(HIGH)               |
| Customers from other jurisdictions than the ones intended use IP-masking technologies to access the services provided by Company                                                                                                                             | 1(LOW)            | 5(HIGH)       | 5(MEDIUM)              |
| Customer accounts being hijacked by malicious individuals from other jurisdictions than the ones intended                                                                                                                                                    | 3(MEDIUM)         | 5(HIGH)       | 15(HIGH)               |
| Customers receive funds in their bank accounts from High-Risk or sanctioned jurisdictions                                                                                                                                                                    | 3(MEDIUM)         | 3(MEDIUM)     | 9(MEDIUM)              |
| Sanctioned country individuals receiving identification and verification details and documentation while living in a low risk jurisdiction then returning to their home countries and providing the bank id to criminal networks for use in ML/FT/FP actions | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                                                                                                                                                                                                     | Effectiveness |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Customer enhanced due-diligence</b> – At specific thresholds, as described in the AML/FT/FP policy, Company will request customers to provide documentation that proves the customer identity as well as source of funds used to deposit. This also holds true in cases of initial high risk as well as suspicion.                                                                                           | EFFECTIVE     |
| <b>Peer-to-peer games not part of the offer</b> – Company does not offer peer-to-peer games as part of its verticals, and thus the products cannot be directly used to transfer funds between players, and thus between jurisdictions                                                                                                                                                                           | STRONG        |
| <b>Automatic and manual IP location check</b> – Company has Iovation in place as a first line of defense against any type of IP masking or fraud. However, if there is any suspicion, as well as part of the due diligence procedure the customer log in IPs will also be checked manually by Company designated employees to ensure that the traffic does not come from a high risk or sanctioned jurisdiction | EFFECTIVE     |
| <b>Suspicious activity Reporting</b> – Company staff check and report upon any suspicious activity that might arise from player behavior (as per the Suspicion reporting Policy) and all findings are reported to the compliance department and MLRO                                                                                                                                                            | EFFECTIVE     |

|                                |              |
|--------------------------------|--------------|
| Category Inherent Risk         | 10(MEDIUM)   |
| Category Control Effectiveness | 2(EFFECTIVE) |
| Category Residual Risk         | 5(MEDIUM)    |

### 3.4. Payment Instruments Risk Category

Payment instruments represent a very important risk factor when it comes to AML/CFT/CFR as this is the point at which any illicit funds can enter the company accounts and begin the process of being laundered. To this extent careful monitoring needs to be done in respect to the payment instruments providers used, as well as careful monitoring of the process of deposit and withdrawal.

This being said, a major difference between land-based gambling and online gambling is the fact that online gambling operators do not accept cash deposits, which greatly reduces the risk of money laundering.

The Company carefully chooses the offered payment solutions ensuring that only providers that have good standing within the European community are employed to provide fund transfers.

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                                                      | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|---------------------------------------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Customers using fake/stolen information to make deposits on the company websites                        | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Customers using multiple bank accounts to make deposits                                                 | 3(MEDIUM)         | 2(LOW)        | 6(MEDIUM)              |
| Customer using a different account for withdrawal than the one used for depositing                      | 1(LOW)            | 3(MEDIUM)     | 3(LOW)                 |
| Customers anonymously transferring funds to their gambling accounts                                     | 1(LOW)            | 5(HIGH)       | 5(MEDIUM)              |
| Payment instruments used to move funds dedicated to financing of terrorism                              | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Masking origin of illicit funds through multiple high velocity transactions                             | 3(MEDIUM)         | 4(MEDIUM)     | 12(HIGH)               |
| Using complicated deposit patterns to mask the final intended deposited amount and bypass risk triggers | 3(MEDIUM)         | 5(HIGH)       | 15(HIGH)               |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Effectiveness |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Use of Closed Loop System</b> - Customers are only allowed to withdraw funds on accounts they have previously used to deposit. Customers are required to have made at least one deposit type transaction from an account verified using Bank ID information to be able to make a withdrawal on said account. Certain exceptions can be made only in cases where the customer has valid reason to request a withdrawal on an account that has not been used for a deposit, and only after satisfactory due diligence has been collected (as per the due diligence policy) regarding the customer and the accounts used. | STRONG        |
| <b>Automatic deposit limit and amount triggers</b> - Company has set up automatic triggers for when customers set monthly deposit limits higher than specified thresholds (detailed in the AML/CFT/CFP policy). Based on the automatic triggers manual review is performed                                                                                                                                                                                                                                                                                                                                                | STRONG        |
| <b>Manual deposit and withdrawal review</b> - Company relevant departments (KYC Department, Customer Support Department) review customer transactions on an ongoing basis (as described in the AML/CFT/CFP policy) checking for any irregularities or patterns that might fall in the Money laundering or terrorist financing category (as described in the reporting policy). Daily reports regarding deposits and withdrawals are also received by the relevant departments. All irregularities are reported to the compliance department, the MLRO and management                                                      | EFFECTIVE     |
| <b>Suspicious activity Reporting</b> - Company staff check and report upon any suspicious activity that might arise from player behavior (as per the Suspicion reporting Policy) and all findings are reported to the compliance department and MLRO                                                                                                                                                                                                                                                                                                                                                                      | EFFECTIVE     |

|                                |           |
|--------------------------------|-----------|
| Category Inherent Risk         | 9(MEDIUM) |
| Category Control Effectiveness | 3(STRONG) |
| Category Residual Risk         | 2(LOW)    |

### 3.5. Product Risk Category

It is mandatory to identify all gambling products which may be used for money laundering or financing of terrorism. Each product shall be identified and the features which make them vulnerable for money laundering and terrorist financing shall be described. To this extent Company has identified that, even though the verticals offered by the company (electronic casino games, live casino games) do not offer the option of customers transferring funds from one to the other, they still pose a high risk of customers either using the games for entertainment purposes using illicitly obtained funds, or attempting to disguise the true origin of the funds through wagering on the company's websites.

This is further amplified by the fact that commercial online gambling is characterized by a high number of transactions, being performed at a high pace with possible high turnover. This raises the risk level of online gambling as the fast pace of the industry may mask transactions performed for the purpose of laundering money or funding terrorism, and enabling malicious individuals to use illegally obtained funds on operator websites.

Furthermore, as described in the Payment Instruments Risk Category, online gambling accounts may be used to store illegally obtained funds, to be on a later date transferred to an account different from the one used to deposit.

It has identified that sports betting poses one of the highest threats due to the possibility of match-fixing. Company has trained their staff to follow customer interaction with the websites in an attempt to detect any breaches of terms of use as well as attempt to impede malicious individuals that may use the sports betting platform to launder funds. Furthermore, Company constantly communicates with their third-party providers in order to cross-check any suspicious activity with the provider aggregated database.

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                                                                                   | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|--------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Opportunity to gamble anonymously (covered in the Customer Risk Category) through the use of stolen/fake information                 | 2(LOW)            | 5(HIGH)       | 10 (MEDIUM)            |
| Masking the origin of illicit funds through wagering on either of the company verticals (electronic casino games, live casino games) | 3(MEDIUM)         | 5(HIGH)       | 15(HIGH)               |

|                                                                                                                                                                                                                          |           |           |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|------------|
| Using vulnerabilities and hacks in casino games to obtain an unfair advantage either when using the bonus funds offered on first interaction or during gameplay                                                          | 2(MEDIUM) | 3(MEDIUM) | 6(MEDIUM)  |
| Using complicated betting patterns to mask use of game vulnerabilities as well as create a difficult to follow gaming history                                                                                            | 3(MEDIUM) | 3(MEDIUM) | 9(MEDIUM)  |
| Using Live Casino Games chat to discuss possible attempts at laundering money and funding terrorism (as described under Distribution Channel Risk Category)                                                              | 3(MEDIUM) | 4(MEDIUM) | 12(HIGH)   |
| Customers pooling funds and depositing under one account in order to use collective knowledge of game vulnerabilities in order to obtain large amounts of money either through bonus abuse or game vulnerabilities abuse | 3(MEDIUM) | 4(MEDIUM) | 12 (HIGH)  |
| Spreading a large amount of illicit funds over multiple related accounts (owned by the malicious individual's acquaintances or family) in order to launder a large amount of illicit funds in multiple transactions      | 2(LOW)    | 5(HIGH)   | 10(MEDIUM) |
| Attempting Money Laundering through match-fixing and/or manipulating or cheating odds                                                                                                                                    | 2(LOW)    | 5(HIGH)   | 10(MEDIUM) |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                           | Effectiveness |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Peer-to-peer games not part of the offer</b> – Company does not offer peer-to-peer games as part of its verticals, and thus the products cannot be directly used to transfer funds between players, and thus between jurisdictions | EFFECTIVE     |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <p><b>Constant communication with Gaming Suppliers</b> – Company has a dedicated Game Management department that keeps constant communication with all the Gaming Suppliers that provide the content customers use on the Company website. These communications include all required information exchange between Company and the Gaming supplier to ensure that there is constant understanding as to what steps need to be followed at all times</p>                                                                                                                       | STRONG    |
| <p><b>Automatic deposit limit and amount triggers</b> – Company has set up automatic triggers for when customers set monthly deposit limits higher than specified thresholds (detailed in the AML/CFT/CFP policy). Based on the automatic triggers manual review is performed</p>                                                                                                                                                                                                                                                                                            | STRONG    |
| <p><b>Manual deposit and withdrawal review</b> – Company relevant departments review customer transactions on an ongoing basis (as described in the AML Policy) checking for any irregularities or patterns that might fall in the Money laundering or terrorist financing category (as described in the reporting policy). Daily reports regarding deposits and withdrawals are also received by the relevant departments. All irregularities are reported to the compliance department, the MLRO and management</p>                                                        | EFFECTIVE |
| <p><b>Manual Gaming History Verification</b> – Upon suspicion of ML/FT/FP (as described in the AML Policy) the customer gaming history will be manually verified by the relevant department and any findings will be escalated to the Compliance department and the MLRO to establish further action</p>                                                                                                                                                                                                                                                                     | EFFECTIVE |
| <p><b>Unusual Transactions Reporting</b> – Company staff check and report upon any suspicious activity that might arise from player behavior (as per the Suspicion reporting Policy) and all findings are reported to the compliance department and MLRO</p>                                                                                                                                                                                                                                                                                                                 | EFFECTIVE |
| <p><b>Duplicate or linked account verification</b> – Company trained employees verify the information on accounts that are suspected of being duplicate or being linked to other accounts. Customers may attempt to create multiple accounts or use the gambling services offered by the Company websites in order to take advantage of the initial interaction bonus offer or take advantage of unknown game vulnerabilities. To this extent accounts are verified using various tools (IP trackers, public online records) to determine whether accounts are linked in</p> | STRONG    |

|                                   |  |
|-----------------------------------|--|
| order to enable fraud or ML/FT/FP |  |
|-----------------------------------|--|

|                                       |              |
|---------------------------------------|--------------|
| <b>Category Inherent Risk</b>         | 10(MEDIUM)   |
| <b>Category Control Effectiveness</b> | 2(EFFECTIVE) |
| <b>Category Residual Risk</b>         | 5(MEDIUM)    |

### 3.6. Internal risk Category

Company strives to ensure that all policies, procedures and implementations targeted towards mitigating external risk of ML/FT are thoroughly updated and respected by relevant staff, however there are still internal risks that need to be taken into consideration when it comes to internal governance.

These risks become even more relevant when we take into consideration the fact that most of the procedures and investigations related to AML/CFT/CFP are performed manually by the company's relevant employees, and although ample training and assistance is provided by internal and external professional sources, situations might still occur when human error could be considered a risk.

These risks are mostly mediated by ensuring that the company has a well-established culture based on compliance as well as making sure that all relevant actions are reported in a transparent manner up the chain of management, and all records kept for future reference (based on the reporting and record keeping policy).

To this extent, the following threats and vulnerabilities have been detected:

| <b>Vulnerabilities and threats</b>                                          | <b>Likelihood</b> | <b>Impact</b> | <b>Risk Assessment</b> |
|-----------------------------------------------------------------------------|-------------------|---------------|------------------------|
| Relevant employees insufficiently trained                                   | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Members of management insufficiently trained                                | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |
| Key roles in combatting ML/FT/FP not filled in by employees with sufficient | 2(LOW)            | 5(HIGH)       | 10(MEDIUM)             |

|                                                                                                                                                                                    |           |           |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|-----------|
| experience                                                                                                                                                                         |           |           |           |
| Employees tipping off suspected customers (voluntarily or not)                                                                                                                     | 3(MEDIUM) | 5(HIGH)   | 15(HIGH)  |
| Relevant employees misunderstanding policies and procedures related to AML/CFT, or mistakenly/deliberately misapplying them                                                        | 2(LOW)    | 4(HIGH)   | 8(MEDIUM) |
| Policies and procedures not receiving sufficient proof reading prior to being approved and implemented, thus generating situations where policy/procedure does not reflect reality | 1(LOW)    | 4(MEDIUM) | 4(LOW)    |
| Automated tools not being properly implemented and monitored causing data processing to be skewed                                                                                  | 3(MEDIUM) | 5(HIGH)   | 15(HIGH)  |

After analyzing the vulnerabilities and threats in this category the following Measures and Controls have been detected, updated and put in place:

| Measure/Control Description                                                                                                                                                                                                                                                                                                                                                                                 | Effectiveness |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Employee and Management training</b> – All employees whose functions relate to AML/CFT/CFP receive periodic training (at least once every 12 months) or training delivered when there is a relevant change in the legislation as well as when a training is deemed necessary due to internal evaluation. The trainings are provided in-house by the MLRO assisted by management and heads of departments | STRONG        |
| <b>Employee performance reviews</b> – Periodic performance reviews are performed on the activity of the relevant employees. Performance reviews will also be performed when it is noticed or reported that unhealthy trends appear within the work ethic.                                                                                                                                                   | STRONG        |
| <b>Employee Screening</b> – All new employees of the Company are screened using online resources to ensure that no negative outstanding actions were taken by the future employee. The                                                                                                                                                                                                                      | STRONG        |

|                                                                                                                                                                                                                                                                              |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| candidate is also required to provide due diligence documentation (copy of ID, proof of address – if not present on id, criminal record) as well as a copy of the cv.                                                                                                        |           |
| <b>Periodic Management meetings</b> – the MLRO will, periodically or when the situations necessitate it, summon a meeting with management as well as with the board of directors to discuss the latest items affecting the company from an AML/CFT/CFP and risk perspective. | EFFECTIVE |
| <b>Staff Numbers</b> – Company ensures that there is permanently enough staff available to tackle all the tasks required to maintain compliance with AML/CFT/CFP requirements.                                                                                               | STRONG    |

|                                       |              |
|---------------------------------------|--------------|
| <b>Category Inherent Risk</b>         | 10(MEDIUM)   |
| <b>Category Control Effectiveness</b> | 2(EFFECTIVE) |
| <b>Category Residual Risk</b>         | 5(MEDIUM)    |

### 3.7. Conclusion

Taking into account the analysis performed above we have the following individual inherent risk scores per risk category:

- Customer Risk Category: 13(HIGH)
- Distribution Channel Risk Category: 9(MEDIUM)
- Geographical and Jurisdiction Risk Category: 10(MEDIUM)
- Payment Instruments Risk Category: 9(MEDIUM)2
- Product Risk Category: 10(MEDIUM)
- Internal risk Category: 10(MEDIUM)

This gives the company an average detected inherent risk score of: 10 (MEDIUM)

The total control effectiveness between all categories is set to: 2 (EFFECTIVE)

The residual risk rating for the company is set at: 5 (MEDIUM)

The company's current residual risk is set to MEDIUM due to the nature of the online gambling industry. The report was also made as such that the risks can never be fully mitigated as to reflect the reality of the risk level faced by online gambling operators.

More work can be done to improve the risk ratings and the Company continuously strives to improve the measures taken to mitigate risks and ensure that the possibility of ML/FT/FP/PF or fraud is kept at a minimum.