

Business Risk Assessment



V2 - 2023

Contents

1	Company Background:	2
1.1.1	Legal Entities	2
1.1.2	Investors and Ultimate Beneficial Owners (UBOs)	2
2	KTO AML & FT Business Risk Assessment:	3
2.1	Inherent Risks.....	4
2.1.1	Country Risk / Geographical Risk	4
2.1.2	Customer Risk	6
2.1.3	Product and Transaction Risk (including means of payment)	6
2.1.4	Interface Risk.....	7
2.1.5	Employee Risk	8
2.1.6	Inherent ML & FT Risk Likelihood	8
2.1.7	Inherent Risk Impact	9
2.2	Quantification Inherent Risk	9
3	Internal controls and measures adopted to mitigate inherent risks.	9
3.1.1	Controls on Geographical & Country risk	10
3.1.2	Customer risk controls	10
3.1.3	Product & Transaction Risk controls.....	12
3.1.4	Controls on Interface Risk.....	14
3.1.5	Controls on Employee Risk.....	15
4	Residual Risk	15
5	Conclusion.....	16

1 Company Background:

1.1.1 Legal Entities

KTO is operated by Bravalla B.V. – A Curacao registered company (company number 147847) & registered address Korporaalweg 10, Willemstad, Curacao. The Company is in possession of a Curacao sub-licence issued by Antillephone, and they operate an online casino and sportsbook using the domain www.kto.com.

Although Bravalla does not have any employees, the operations of the group is supported through employees and contractors of related party companies, namely:

- Winlink Limited – A UK registered company. This serves as the holding company and also act as the treasury company for the Group. The company is also involved in the marketing expenditure of the Group, such as the Affiliate program.
- Winlink Servicos De Gestao De Marcas LTDA – A Brasil registered company and fully owned subsidiary of Winlink Limited. The company serves as the marketing arm of the Group.
- Matlof S.A. – A Uruguay registered company and fully owned subsidiary of Winlink Limited. The company will serve as a tech hub for the Group.

The Group maintains one platform for all its activities and consolidated financial records are maintained and prepared monthly.

1.1.2 Investors and Ultimate Beneficial Owners (UBOs)

The Group was founded by two investors, being the UBOs of the Group:

- Andreas Soren Bardun, a Swedish individual with Passport 35876402, holding 67% shareholding of the Group.
- Fintan Patrick Farrell, an Irish individual with Passport PU9164508, holding 33% shareholding of the Group.

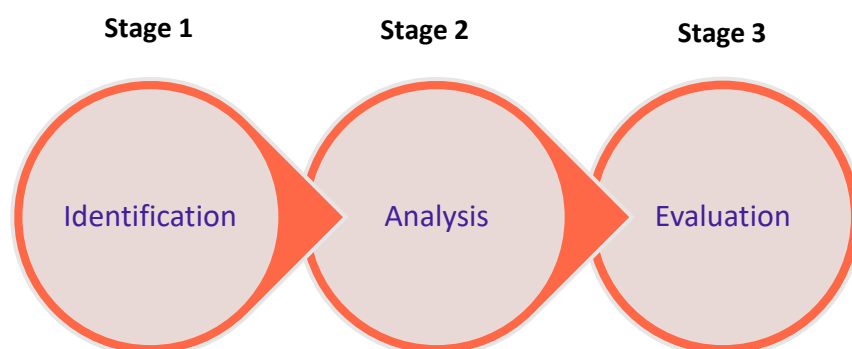
2 KTO AML & FT Business Risk Assessment:

The Group's management was responsible of the drafting of the Business Risk Assessment (BRA), more specifically this was the responsibility of the CFO, MLRO and CEO.

The scope of the BRA is to provide an in-depth insight into the exposure to ML&FT risk faced by the Group. The Group aimed at creating a methodology through which money laundering risk is identified, analysed, and evaluated. The BRA serves as the first step in addressing and mitigating the inherent risks. When assessing inherent risks management assessed:

- Threats: persons, or groups of people, objects, or activities with the potential to cause harm, including criminals, terrorist groups and their facilitators, their funds, as well as past, present and future money laundering activities
- Vulnerabilities: those things that can be exploited by the threat or that may support or facilitate its activities and means focussing on the factors that represent weaknesses in AML systems or controls or certain features of a country, particular sector, financial product, or type of service that make them attractive for money laundering
- Consequences: referring to the impact or harm that money laundering may cause, including potentials fines, and the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally.

The risk assessment process consists of the following stages:



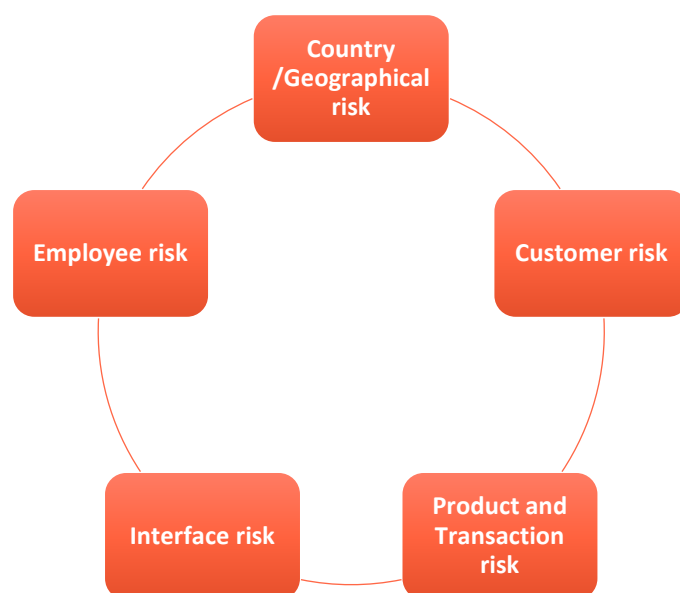
In the identification process a list of ML & FT inherent risk faced by the Group was compiled considering all the risk factors when combating money laundering. Risk factors are the specific threats or vulnerabilities that are the causes, sources, or drivers of money laundering risks.

The analysis stage involved the consideration of the likelihood and impact of the identified inherent risks. The aim of this stage is to gain a comprehensive understanding of each risk, as a combination of threat, vulnerability, and consequence, in order to assign a relative value or importance to each of them. Risk analysis is undertaken with varying degrees of detail, depending on the type of risk and involved an element of judgment that had to be exercised by the management.

The evaluation stage involved assessing the risks analysed during the previous stages to determine priorities for addressing them, considering the purpose established at the beginning of the assessment process. These priorities serve as the foundation for the development of a strategy, policies, and controls to mitigate the inherent risks.

2.1 Inherent Risks

The management believe that the inherent risks of operating an online casino and sportsbook can be summarised into five main categories:



2.1.1 Country Risk / Geographical Risk

Geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship.

As a Group we only offer the possibility for players resident in Brazil to register and play on our website. Brazil presents both opportunities and challenges in this sector. The evolving regulatory

landscape surrounding online gambling, combined with occasional uncertainties and delays in policy implementation, poses a potential risk to our business operations.

The country's historical issues with corruption and the complexity of its financial system also contribute to concerns related to money laundering and fraud. In light of this, it is of utmost importance to adhere to international standards, such as those set forth by the Financial Action Task Force (FATF).

Between 2016 and 2019, the FATF issued a number of statements conveying deep concerns about Brazil's continued failure to remedy the serious deficiencies identified in its June 2010 mutual evaluation report (third round of mutual evaluations), especially regarding terrorism and terrorist financing. In 2019, Brazil addressed most of these deficiencies when it adopted a new framework for identifying and freezing terrorist assets. Brazil has not yet been assessed in the fourth round of mutual evaluations. Due to the COVID-19 pandemic and the pause in the FATF's assessment process, the mutual evaluation of Brazil has been postponed to 2023.

Our Group is committed to aligning with FATF guidelines, closely monitoring changes in legislation, maintaining a proactive dialogue with local regulatory bodies, and implementing robust compliance measures.

In order to determine the risk factor of jurisdictions, the Group refers to the FATF's publication on 'High-risk and non-cooperative jurisdictions. Other factors used in determining Geographic Risk of a customer are:

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Security Council. In addition, in some circumstances, countries subject to sanctions or measures which may not be universally recognised may be given credence by the Group because of the standing of the issue and the nature of the measures.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations, and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

2.1.2 Customer Risk

The risk of ML/FT may vary in accordance with the type of customer and that the assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. For example, a customer having a single source of regular income will pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.

As a remote gaming operator with a focus on the Brazilian market, we usually see high transaction volumes of low amounts (between €5 – €100). Given the intrinsic nature of the business and depositing transactions, it is difficult for the Group to assess the wealth and economic activity of all the players registering on our platform. Consequently, the Group adopts a risk-based approach, with checks and controls varying depending on the risk associated with each player.

Determining the potential money laundering risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework adopted by the Group. Categories of customers whose activities may indicate a higher risk include:

- High spenders: The Group has various thresholds in place to determine the risk level of the players based on their spend. For example, all players depositing more than €25,000 in life-time net deposits, are classified as High Risk.
- Disproportionate spenders: where appropriate, we try to obtain information about customers' financial resources to determine whether customers' spending is proportionate to their income or wealth.
- Customers who appear on international sanctions or PEP lists

2.1.3 Product and Transaction Risk (including means of payment)

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by licensees of specific funding methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that do not always leave, or otherwise complicate, the funds' audit trail, and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual financial assets.

As a Group we do not offer poker in our online casino, which usually is considered as high risk due to the possibility of collusion between players.

As a result, the Management believes that the Product risk in Online Casino is inherently extremely low, given that we currently offer primarily RNG Slots, the outcome of which is generated by computer algorithms. These are primarily luck-based, and players have little control over the results. The Group also offers Live Casino; in remote circumstances this may result in collusion with the Game presenters that might lead to a marginal degree of inherent product risk.

The other vertical offered is Sports betting, which may be considered as being medium-high risk due to the risk of having the athletes betting on the outcomes that they have a direct influence on or colluding with third parties to influence the outcome of a game and a contingent bet.

Although the inherent product risk varies according to the vertical offered, the Group is still exposed to a degree of inherent transaction risk emanating from the deposit method used by the customers. The Management believes the Group faces low inherent transaction risks due to, the majority of player deposits are done through Pix. Pix is an instant payment platform created and managed by the Central Bank of Brazil (BCB). The BCB manages and operates a user address database contains identifying information on the users, including aliases, such as phone numbers, email addresses or randomly generated IDs, used for access to the Pix system and to prevent fraud.

The Management believes that the following may pose inherent transaction risks -

- Acceptance of Boleto – being a cash-based payment system, transactions are often less traceable compared to digital or card-based transactions.
- Acceptance of E-wallets: some e-wallets accept cash on deposit or digital currencies, which pose a higher risk, and some customers may use e-wallets to disguise their gambling.
- Identity fraud: details of bank accounts may be stolen and used on, for example, remote gambling websites, or stolen identities may be used to open bank accounts or gambling accounts.
- Multiple gambling accounts or wallets: customers may open multiple accounts or wallets to obscure their spending levels or to avoid CDD threshold.
- Depositing / Withdrawal activity: criminals may use accounts to deposit criminal proceeds and then withdraw funds with little or no play.

2.1.4 Interface Risk

The channels through which the Group establishes a business relationship and/ or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favour anonymity increase the risk of ML/FT if no measures are taken to address the risk.

Although as an operator we do not permit players to play on our platform without providing basic identification details such as full name and residential address, being a remote gaming operator, where the interaction with the customers takes place on a non-face to face basis, will inherently create an element of interface risk due to the heightened risk of identity fraud or impersonations.

2.1.5 Employee Risk

Management believes that it is not only customers that pose a risk of ML/TF, but employees can also pose a risk to the business either due to human errors, lack of competence or circumvention of controls to abuse the system for their own gain. Having grown rapidly from a small sized operator in some instances the Group lack the ideal segregation of duties and sophisticated automation. Several checks are partly automated or done manually by the employees, resulting in a heightened inherent employee risk. Consequently, the management believes that employee risk is an inherent risk that should be assessed and noted down as part of the BRA, and mitigations are to be established with the aiming of limiting and reducing the employee risk.

2.1.6 Inherent ML & FT Risk Likelihood

Inherent Risks are determined by assessing the likelihood of the Group being exposed to ML&FT and quantifying the maximum financial exposure should the Group be found in breach of ML & FT regulations. The likelihood of ML&FT risk has been calculated by assessing the risk profiles listed above. Each profile was assigned a risk level/score using the following scoring mechanism:

- 20 → Low Risk
- 40 → Medium to Low Risk
- 60 → Medium Risk
- 80 → Medium to High Risk
- 100 → High Risk

The risk score was then weighted using a total percentage score of 100%, across the 5 inherent risk variables to compute a weighted likelihood risk.

Although an element of subjectivity is natural when computing the risk scores and contingent likelihood of the predetermined inherent risks, the risk levels and weightings were intensively debated by various members of the management team to try and limit the subjectivity involved.

	RISK LEVEL	WEIGHTING	WEIGHTED RISK
COUNTRY /GEOGRAPHICAL RISK	40	20%	8
CUSTOMER RISK	60	30%	18
PRODUCT & TRANSACTION RISK	80	30%	24
INTERFACE RISK	40	10%	4
EMPLOYEE RISK	60	10%	6

From the attached table the cumulative likelihood percentage total amounts to 60.

2.1.7 Inherent Risk Impact

As impact, the Group has considered the maximum financial penalty which can be imposed according to the EU Prevention of ML and TF Regulation, which provides that *“a maximum pecuniary fine of at least twice the amount of the benefit derived from the breach or at least €1 million”.*

The management deems that an inherent impact of €1m should be the most conservative figure on which to assess the impact risk of ML&FT. Although in the impact assessment the Group is not taking into consideration the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally, it is assuming that this impact was considered when the legal authorities drafted the maximum fine parameters.

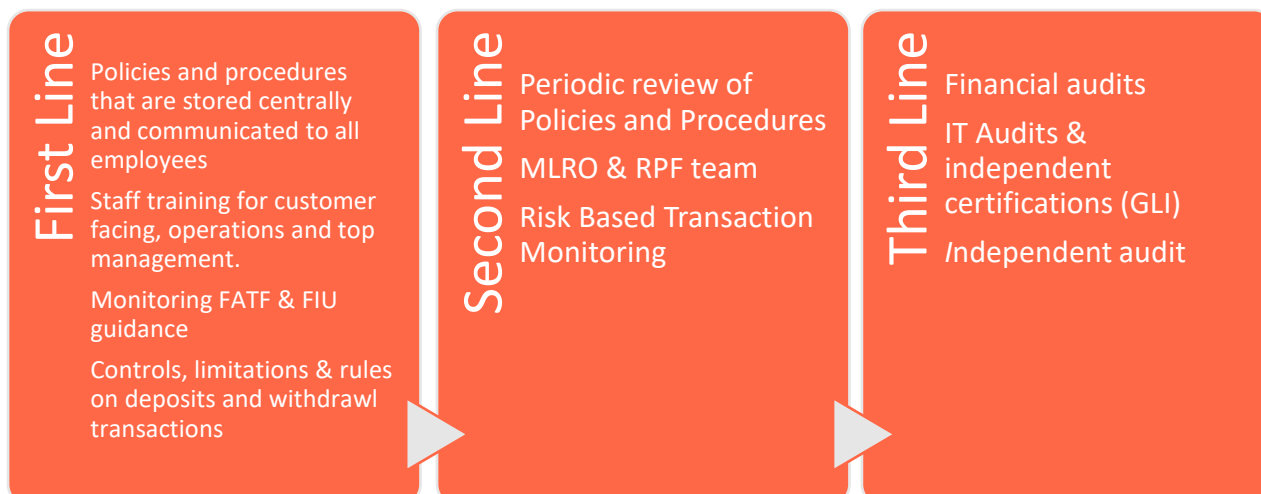
2.2 Quantification Inherent Risk

After determining the inherent risk likelihood and the maximum financial impact, the Group calculated the ultimate inherent risk value of ML&FT at $60\% * €1,000,000 = €600,000$.

This figure is just an indication of the inherent risk the Group is facing before applying the controls. It by no mean implies that this is the maximum or minimum fine that can be imposed by the regulatory authorities but is merely a figure computed using management judgment to quantify the ML&FT risk.

3 Internal controls and measures adopted to mitigate inherent risks.

The Group has various controls in place to reduce the likelihood and limit the impact emanating from the inherent risks of operating an online casino and sport betting. The Group adopts what is commonly referred to as the Three Lines of Defence Model:



3.1.1 Controls on Geographical & Country risk

As a Group we take the necessary measures to check the location of the player or prospective player. This is done to minimise the risk of facilitating illegal gambling in countries where gambling is not permitted and to ensure that gambling is not offered to players residing outside of Brazil. Players from restricted countries would not be able to register on our platform.

This risk is also mitigated by having measures in place to check the user's IP address location. If the IP address from where the user is trying to access our online site is outside of Brazil, registration on the site will be blocked. In addition, we have taken measures together with our Payment Service Providers (PSPs) to ensure that we do not accept deposits from restricted territories.

As part of the customer registration process customers and account verification all players registering with our online site are asked for the CPF. The CPF, Cadastro de Pessoas Físicas, is a unique identifier for each Brazilian citizen and resident. It helps establish a clear and distinct identity for each person, reducing the likelihood of mistaken identity or impersonation. Names, surname, address, date of birth, email and mobile phone are also collected as part of the registration process. the registration profile. By doing so the Group is keeping a log of all the address details of all the players on its database.

As a remote operator apart from country of residence we also check and monitor the customer location when logging in our portal and using a risk-based approach, we also ask for identification documents to verify residential address and nationality.

3.1.2 Customer risk controls

It is critical to determine the potential money laundering and/or terrorist financing risks posed by the players to develop and implement an effective overall risk-based framework. Based on different

criterion, the Group is able to determine whether a particular player poses a higher risk and the potential impact of any mitigating factors on that assessment.

A key risk mitigation strategy is ensuring that the Group holds adequate customer due diligence (CDD) measures on its players. The Group has in place an Anti-Money Laundering (AML) policy that outlines the CDD process applied to players. The AML policy also outlines factors in relation to enhanced due diligence (EDD) including high-risk players and Politically Exposed Persons (PEPs).

To address customer risk the Group takes a risk-based approach and uses a risk score model to determine a ML risk score for all players registering and placing a deposit.

3.1.2.1 Verifying Identity

The Company verifies the CPF for all players upon registration. Furthermore, all players featuring on the risk score model (depositing or withdrawing more than EUR3000, are asked for a photo of the ID plus selfie. Through these measures the company is ensuring that the identity of the players is duly verified.

3.1.2.2 High Spenders

Players classified as high spenders are those players whose net deposits exceed €25,000 over the lifetime of the account.

To mitigate this risk, the Group monitors the player's' activity by using the risk-based approach, so that High Spender are subjected to more checks when compared to lower risk players. High Spenders are asked to fill in a Source of Wealth questionnaire and this can/may be substantiated with corroborative documents like bank statements, payslips, and desktop research.

3.1.2.3 PEPs & Sanctioned Customers

The Group recognises the increased risk in dealing with PEPs, SIPs, and their associates. In addition, the Group recognises the prohibition on dealing with sanctioned individuals and companies.

Politically exposed persons (PEPs) are persons who are entrusted with prominent public functions or are family members or close associates of such persons. Prominent public functions include: heads of state, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties; members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances; members of courts of auditors or of the boards of central banks; ambassadors, charges d'affaires and high-ranking officers in the armed forces; members of the administrative, management or supervisory bodies of State-owned enterprises; Directors, deputy directors and members of the board or equivalent function of an international organisation. These are

classified as a money laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

KTO has a process by which all players are checked and screened against a PEPs/Sanctions database upon registration, maintained by an appropriate third-party supplier (Dilisense). By incorporating these measures, we are not only ensuring compliance with anti-money laundering (AML) regulations but also actively mitigate potential risks associated with individuals who may be susceptible to corruption or illicit financial activities.

PEP and Sanctions checks consists of screening customers against the database provided by Dilisense to determine if they are known fraudsters, drug dealers, terrorists, money launderers or politically exposed persons. Dilisense database includes individuals and entities from all known sanctions and embargo lists around the world, including EU and UN sanctions lists.

Any positive PEP flags are to be checked to make sure the case is not a false positive. If the customer is confirmed to be a PEP, the player account is subject to Enhanced Due Diligence to manage the enhanced risks arising from the relevant person's business relationship or transactions with such a player. Players flagged for sanctioning are not allowed to deposit and play on our site.

3.1.2.4 Identity Fraud

Our Risk and fraud & customer support teams monitors the list of accounts created to identify any account that was manifestly created using wrong details like random characters or fictitious characters. These accounts are blocked immediately upon being identified. Checks on deposits are also maintained, since pix will only allow players using the CPF used at registration phase to deposit.

Using a risk-based approach the Group also verifies the identity of players meeting the CDD threshold by asking for more documents.

3.1.3 Product & Transaction Risk controls

The Group has various internal controls in place to limit ML&FT risk arising from transaction risks.

3.1.3.1 Changes to Financial Institution Accounts

Changing depositing accounts regularly increases the risk that customers will place and layer criminal proceeds through gambling transactions. This risk is mitigated by linking winnings pay-outs with the CPF by which the player deposited to carry out gambling transactions.. The closed loop based on

confirmed account ownership via CPF should always be preferred and where the closed loop is broken, the transactions are being monitored & scrutinized.

Almost all player transactions processed to and from players are done using Pix. This instant payment system introduced by the Central Bank of Brazil, incorporates several features that contribute to its safety against money laundering. While no system is entirely immune to illicit activities, Pix incorporates safeguards that enhance security and mitigate the risk of money laundering –

1. Pix transactions are monitored and overseen by the Central Bank of Brazil, which provides a centralized authority to regulate and supervise the system.
2. To use Pix, individuals must link their accounts to a valid CPF - This requirement ensures that users are identifiable, making it more challenging for individuals to conduct money laundering activities anonymously.

3.1.3.2 Pre-paid Vouchers - Boleto

Players may use cash to purchase pre-paid vouchers. Hence, this payment method poses a high money laundering risk as the purchaser of the vouchers might not be legitimate and it will be difficult to make the same level of cross reference checks on some types of pre-paid vouchers as could be used to perform on financial institutions accounts. This especially since pre-paid vouchers are only used for depositing purposes.

During 2023 the Group stopped using Boleto as a payment method. When Boleto was accepted, to mitigate the risk, the Group used to penalizes players using Boleto when computing the ML risk score by assigning a risk weight of 5 – the maximum score for this variable.

3.1.3.3 Electronic Wallets (e-wallets)

Usually, electronic wallets, which only accept money from financial institution accounts held in the player's name (for instance Skrill), and as a result this will not pose any greater or lesser money laundering risk than funds received directly from the financial institution itself.

Certain e-wallets however do accept deposits via pre-paid vouchers (for instance Neteller) and hence these pose a higher risk as money launders and/or terrorists may choose such payments methods to disguise the origin of their funds or to obstruct the audit trail.

To mitigate this risk, the Group takes due care in choosing which e-wallets it will commit to provide to players, especially since not all e-wallets are licensed in reputable countries. Due diligence checks are undertaken to ensure that the Group is only contracting with reputable companies. We have one

wallet provided to our players, and this is sourced and provided by Pay4fun, an entity licensed by the central bank of Brazil.

The management opted to block cryptocurrency transactions to mitigate against the higher associated risk of money laundering when dealing with cryptocurrency. Cryptocurrencies can provide a degree of anonymity, which raises concerns about potential money laundering and other illicit activities.

The decision to block cryptocurrencies is influenced by a combination of legal considerations, risk assessment, and KTO strategic approach to staying compliant with regulations and providing a secure and responsible gambling environment.

3.1.3.4 Inter Account Transfers

Transferring of funds from one player to player is strictly prohibited and not permitted on our platform. This is also stated in our Terms and Conditions which players are obliged to adhere to in order to be able to register and access their gambling account.

3.1.3.5 Product Risk

As highlighted in section 2 the Management believes that the inherent product risk is low. Nonetheless controls are still in place to further lower the risk. Controls in place include:

- Games are sourced from reputed game providers.
- Gameplay of big winners is always checked with the game provider to ensure no foul play.
- KTO is a member of the International Betting Integrity Association (IBIA).

The above controls, together with the fact that we do not offer poker, reduce the product risk to low levels.

3.1.4 Controls on Interface Risk

The Group, takes several measures to mitigate this inherent risk, making sure that the residual risk is in line with its Risk Appetite. The measures and controls in place to address the inherent risk of identity fraud or impersonation include:

- The Group has a report in place that checks whether different user IDs were created using the same IP address,
- All players are asked to fill in a detailed registration form, so that they can be duly identified.
- An automated report is in place to determine players with multiple accounts.
- Players' Identities are verified on a risk-sensitive basisU (which one?).

3.1.5 Controls on Employee Risk

To safeguard against this risk the Group makes sure that all customer facing, operational and top management employees attend at least one annual training session on the topic. Certificates are kept on record to track the progress of training within the team.

The AML policy is saved in a central database, that is accessible by all the employees. New employees are encouraged to read the new AML policy irrespective of the position held to make sure they are aware of the policies within the Group.

The Group also conducts KYE on the C-level employees, making sure that they are of the right integrity, with a clean conduct and a good reputation.

4 Residual Risk

The residual risk is the ultimate risk to which the Group is exposed after taking into consideration the controls in place.

The management of the Group believes that the Group has a good mix of preventive and detective controls in place that should enable to lower the inherent risks of operating an online casino and sportsbook. Following the application of internal controls, the management believes that the risk score is lower across all risk categories, especially with Product / Transaction risk and Geographical risk.

	RISK LEVEL	WEIGHTING	WEIGHTED RISK
COUNTRY /GEOGRAPHICAL RISK	0	20%	0
CUSTOMER RISK	0	30%	0
PRODUCT & TRANSACTION RISK	20	30%	6
INTERFACE RISK	0	10%	0
EMPLOYEE RISK	0	10%	0

When applying the revised residual weighted risk factor (6%) on the maximum financial impact, the Group calculated the ultimate residual risk value of ML&FT at $6\% * €1,000,000 = €60,000$.

Although an element of residual risk is inevitable, the management is continuously working at improving internal controls and reducing the ML&FT risks.

5 Conclusion

The BRA is a dynamic document that is continuously monitored and revised accordingly when significant developments take place within the environment within which we operate or changes taking place within the business structures or activities.

Continuously monitoring & revising the BRA allow the management to take action to ensure that the measures, policies, controls, and procedures are robust enough to cater for ML&FT risks.