

Risk No	Risk Factor	Vulnerability	Threat	Risk	Stakeholder	Risk summary	Likelihood (1-5)	Impact (1-5)	Inherent Risk	Measures	Controls	Effectiveness of Controls	Likelihood after application of measures	Impact (1-5)	Residual Risk
1	Interface	Customer Identity, Non face-to-face interaction since gaming is done remotely.	Fake registrations and having incorrect data due to being outdated or inputted wrongly.	Compliance	AML Team	Customers registered using fake identities or data no longer valid due to address, identity or other changes.	3	5	15	Checks done on registration. Automatic Verification of Customer Details & Flagging on 1st Financial Transaction. KYC Portal to maintain ongoing monitoring.	KYC and checks carried out to identify if the customer is a real customer.	Strong	2	5	10
2	Customer	PEP Customer	Registration of clients which classified as PEP and assigned as High.	Compliance	AML Team	A PEP or Sanctionable Customer using Company Services	1	4	5	Customers are automatically PEP screened upon registration. Throughout the business relationship the customer is PEP screened periodically.	Monitoring of results / logs from PEP Checks, making sure updates are effected and re-checking effected on periodic.	Strong	1	4	4
3	Customer	Multiple Accounts	Due to multiple account held incomplete visibility to customer activity.	Compliance	AML Team	Customer holding multiple accounts to share activity	1	4	4	Upon registration the details are checked for duplicate accounts. Information checked are name and surname, date of birth, residential address, contact number, e-mail address etc.	Ongoing monitoring to monitor effectiveness & Analyse flagged accounts.	Effective	1	4	4
4	Geographical Risk	Geographical Risk - Customer Access	Customer Geography	Compliance	Compliance Officer and AML Team	Customer originates from high risk country as per sanction list either through registration or accesses the services from high risk locations	2	5	10	High risk FATF countries. Registration form does not include any high risk country. Services not accessible from High risk countries or through anonymising proxies.	IP Range Blocking and monitoring to disallow access from high risk countries, customers logged to access their account from unusual locations to be contacted and considered for EDD.	Effective	1	5	5
5	Geographical Risk	Geographical Risk - Payment Methods	Payments used outside of Geographical area	Compliance / Fraud	Compliance Officer and AML Team	Customers using payment methods that are originating from countries other than their residential country with intent to impersonate funds or remit funds to different countries.	2	4	8	Monitoring of Deposits, Geographical restriction of Payment Methods to suitable countries.	Customer payment methods to be screened at deposit and withdrawal stage to ensure customer is using a payment method that is issued from his country of registration and necessary action taken when mismatches are observed to mitigate this risk	Effective	1	5	5
6	Transaction	Deposit Methods of Funds into a customer account	Proceeds of Crime	Compliance	AML Team	Customers channelling Proceeds of Crime through stolen cards or use of cards which are not under the customers name.	3	5	15	Ownership of Payment method needs to be verified via technological means and documents from clients.	Ownership / Authorisation check through 3DS and PSP Portals.	Effective	2	5	10
7	Transaction	Deposit Amounts into customer accounts	Proceeds of Crime	Compliance	AML Team	Customers channelling Proceeds of Crime through company and triggering Compliance Obligations due to amount deposited	2	5	10	Limits on Deposits until customer is verified, SOW and SOF proof is provided as requested to those customers classified as medium-high.	CDD and/or EDD depending on level of deposits. ongoing monitoring of business relationship through Automated Risk Tools, VIP relationships involving contact with customer via phone or video conferencing.	In-Effective	2	5	10
8	Transaction	Multiple Deposit / Withdrawal Methods	Transferring funds across various payment platforms	Compliance	AML Team	Customers using Company as a layering component	3	5	15	Restrictions on types and number of different payment methods, Manual removal of old payment methods to be confirmed with AML Team	Ongoing monitoring, integrated system in withdrawal screens, withdrawal checks, CDD/EDD obligations	Effective	2	5	10
9	Transaction	Betting Product	Simulation of legitim betting activity	Compliance	AML Team	Customers employing betting platforms to simulate lawful betting actions for layering intentions and potentially altering their pattern subsequently	3	5	15	Betting Platform activity monitored by Risk and Fraud Team and/or Automated Risk Tools to identify abnormal activity patterns, P2P gaming block to randomise opponents, increased monitoring on gaming activity depending on Product Risk - Limits on Platform activity depending on verification status of client	Daily checks on customers with high turnover or low profit or loss	Effective	2	5	10
10	Transaction	Withdrawals from account	Withdrawal of deposited with company	Compliance	AML Team	Customers attempting to send funds to a recipient account in the name of a third party or cash-like withdrawal method in a way which appears that funds were won legitimately	2	5	10	Customers enforced by system to adhere to closed loop policy whereby deposited funds are returned to their original payment method. Where the original payment method does not accept withdrawals, withdrawal must be made to a customer owned bank account in a reputable country. Customer not allowed to do automatic withdrawals above deposit amount for each payment method unless checked.	Withdrawals not going back to source to be sent only to a BA or BA linked card. Ownership of the origin of the deposit in such cases to be confirmed beyond doubt. Verification documents supplied to prove ownership of deposit and withdrawal method.	Strong	1	5	5
11	Internal	Staff Awareness	Overlooking AML/CFT Issues in Error	Compliance	Compliance Officer and Internal Auditor	Staff not aware of responsibilities	2	4	8	Induction Training, make available the policies and procedures and Compliance Officer available to assist and provide training as necessary.	Supervise and review regularly samples of employees work along with an internal exercise.	Strong	1	5	5
12	Internal	Internal AML Attempts	Allow AML/CFT intentionally	Compliance	Compliance Officer and Internal Auditor	Staff member intentionally not observing controls to allow AML/CFT	2	4	8	C Level approval for transaction over a certain threshold	Transactions over the threshold to be processed by approval from C Level and undergo weekly with the Internal Auditor	Strong	1	5	5
13	Internal	Tip off	Tip off intentionally or by error	Compliance	Compliance Officer / AML Team	Tip off a customer about an STR escalation	2	4	8	Train Staff and educate them on such regard.	Monitoring of suspected customer's communications with Customer Service	Strong	1	5	5
14	Product	Risks	Automatic games that have very low wagering such as slot games	AML Team	Compliance Officer and AML Team	Deposit Illicit funds and withdraw them most probably using different payment mechanisms. Such withdrawals will be viewed as casino winnings	3	4	12	Have an account with large deposits and minimal or no gameplay. Such account normally have large amount of withdrawals. Accounts will undergo Enhanced Due Diligence.	On going review on such account.	Effective	2	3	6
15	Product	Risks	Sport Betting on games which have low odds.	AML Team	Compliance Officer and AML Team	Low odds will present that the customer will not lose a big sum of money if she/he loses the bet. This will show that such player is legitamte	3	4	12	Have an account with large deposits and minimal or no gameplay. Such account normally have large amount of withdrawals. Accounts will undergo Enhanced Due Diligence.	On going review on such account.	Effective	2	3	6
16	Product	Risks	Peer to Peer Games Used to Transfer Funds Between Players and Collusion	AML Team	Compliance Officer and AML Team	Using third-party accounts, structuring transactions, or converting illegal funds into legitimate winnings through gaming activities	4	5	20	Implement strict Customer DD to verify source of funding and player identification. Monitor Transactions and Report were necessary. Player Behaviour Profiling. Ongoing Staff Training.	On going review of transactions and player accounts. Independent audits and reviews. Risk Based Monitoring.	Effective	3	3	9