HM Government of Gibraltar

Gambling Division

Assessment of the Money Laundering, Terrorist Financing and Proliferation Financing Risks within the Gambling Industry in Gibraltar

Gibraltar Gambling Commissioner

Suite 912

Europort

Gibraltar

Telephone +350 20064145 Fax +350 20064150

www.gibraltar.gov.gi/new/remote-gambling

Version Control:

Date	Version/Amendments	Controller	Number
09.04.2020	First Release	DW/AL	1.0.2020
22.11.2021	2021 – Review	DW/AL	1.0.2021
09.05.2023	2022/23 – Review	DW/AL	1.0.2023
12.07.2024	2023/24 – Review	DW/AL	1.0.2024
21.05.2025	2025 – Review	DW/AL	1.0.2025

Contents

1. Executive Summary

1.1 The Gibraltar Gambling Commissioner and Gambling Division's (**GGC**) money laundering and terrorist financing risk assessment (**ML/TF**) highlights the principle risks which exist within each of the sectors that comprise the Gibraltar regulated gambling industry.

1.2 The risk assessment is underpinned by quantitative and qualitative data which the GGC obtains in the course of its supervisory activity.

1.3 This risk assessment will be an ongoing concern with emerging vulnerabilities being reviewed and incorporated into future iterations of this risk assessment.

1.4 All sectors below have been assessed and given a risk rating on the basis of the risk scoring matrix (see methodology section) and in the context of the gambling sector in Gibraltar as a whole. The risk ratings in this assessment represent a sector-specific, relative assessment of money laundering and terrorist financing risk within Gibraltar's gambling industry. They take into account both inherent risks and the effectiveness of existing mitigating measures (e.g., supervision, controls, operator compliance).

1.5 As such, these are residual risk ratings, assessed in the context of the local gambling sector, not on an absolute basis.

1.6 The 2025 iteration of this Risk Assessment maintains the existing overall risk ratings across different gambling sectors, reflecting a continued assessment that current controls and sector profiles remain appropriate. These ratings will continue to be kept under review in light of emerging risks and developments.

1.7 The remote gambling B2C sector has been assessed as having a **higher** risk.

1.8 The remote gambling B2B sector has been assessed as having a **low** risk.

1.9 The land-based casino sector has been assessed as having a **higher** risk.

1.10 The betting shop sector has been assessed as having a **medium** risk.

1.11 The lotteries sector has been assessed as having a **low** risk.

1.12 Other: Bingo, gaming machines (outside casinos) sector has been assessed as having a **low** risk.

2. Introduction

2.1 Gibraltar has carried out a National Risk Assessment (**NRA**) which was published by the National Co-ordinator for ML and considered the remote gambling sector in Gibraltar giving It a risk rating of 'medium'. The NRA was revised in 2018 to update and expand on risk factors, and a further iteration of the NRA was produced in 2020.

2.2 This risk assessment is designed to complement the NRA and contribute to its update. It builds upon the NRA and incorporates a more granular consideration of the sectoral threats the GGC has identified. It also serves to inform the GGC's Supervisory Strategy and Policy and the carrying out of its regulatory duties in respect of money laundering and terrorist financing (**ML/TF**), utilising a risk based approach and being led by AML/CFT concerns as recommended by HM Government of Gibraltar.

3. Legal and Regulatory Framework

3.1 The Gambling Commissioner is the regulator for the gambling industry in Gibraltar and is a supervisory body listed under Part 1 of Schedule 2 of the Proceeds of Crime Act (**POCA**) for the purposes of supervising licensed gambling operators' (**Licence Holders**) compliance with relevant Gibraltar laws and regulations for anti-money laundering, countering the financing of terrorism and counter proliferation financing. The Gambling Commissioner works with staff in both the licensing and regulatory spheres.

3.2 Licence Holders have a responsibility under both POCA and the Gambling Act (the **Act**) to be alert to attempted money laundering or the spending of the proceeds of crime and report instances or suspicions of same.

3.3 The Terrorism Act (**TA**) establishes further offences in respect of engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes.

3.4 The Code of Practice for the Gambling Industry (**AML Code**), issued by the Gambling Commissioner, provides further interpretative guidance for Licence Holders in respect of their AML/CFT responsibilities. There are separate codes for the non-remote gambling sector and the remote gambling sector.

3.5 The Financial Action Task Force (**FATF**)'s risk assessment methodology provides the basis upon which the Gambling Commissioner bases its framework for its own risk assessments.

3.6 This Risk Assessment is designed to supplement the NRA and to provide Licence Holders with further context about the existing risks in the sector. This may assist Licence Holders in developing their own risk assessments. The development of such risk assessments is a requirement under POCA and the Code, although Licence Holders must understand the risks within the context of their own operations and not all risks will necessarily apply to a particular Licence Holder.

4. Methodology

4.1 The GGC considers the money laundering risk within the gambling sector to be that either gambling operators come under the ownership or control of organised criminals for the purposes of laundering the proceeds of crime or that the services offered by gambling operators are used as conduits for the spending or laundering of the proceeds of crime.

4.2 The GGC considers the risks as a whole in the various different areas comprising the gambling sector in Gibraltar as well as considering the risks in the context of individual licensees.

4.3 In line with the FATF, the GGC's methodology considers risk to be a function of threat, vulnerability and consequence. The risks may be mitigated by controls put in place.

4.4 The GGC takes into account both quantitative and qualitative information in its risk assessment. These include the findings of the Gibraltar NRA, the EU Supranational Risk Assessment, data collected by the GGC during the course of its supervisory activities, including:

i. The annual AML Questionnaire which obtains data on:

- number of registered and active customers;
- number of dormant accounts;
- jurisdictional splits by % of revenue;
- number of active PEPs and number of PEPs with whom Licence Holders have ceased to do business;
- whether sanctions monitoring is carried out at registration and on an ongoing basis;
- how many confirmed TFS matches there have been;
- the regulatory technology or providers used for the purposes of carrying out PEPs and Sanctions screening;

- whether the Licence Holder accepts custom from FATF identified higher risk jurisdictions;
- if so, what additional measures are put in place in respect of these jurisdictions;
- whether senior management regularly reviews the jurisdictions with whom business is conducted;
- date of the most recent independent audit of the Licence Holder's AML/CFT/CPF systems and controls.

ii. findings from on-site and virtual assessments of gambling operators' AML/CFT/CPF systems and controls including desk-based reviews of Licence Holder policies and procedures;

iii. intelligence reports provided by the Gibraltar Financial Intelligence Unit (**GFIU**);

iv. the knowledge and expertise of staff members; and

v. any other relevant information which may come to light during the course of the GGC's supervisory activity.

4.5 The overall risk is calculated by the formula: **probability X impact = overall risk**. When considering likelihood and impact, the GGC also takes into account the controls in place which function as mitigating factors.

- **Threat** – this encompasses individuals, groups and/or particular activities which have the potential to introduce criminal elements into the gambling sector. This can manifest itself in various respects including criminal groups or individuals seeking ownership or control of gambling operators for illegal purposes; the intentional laundering of funds through gambling operators or simple criminal spend; and operators not being fully aware of or negligent in respect of their responsibilities.

- **Probability** – the chance that a money laundering risk materialises is to be considered in the context of realistic threats existing and their potential to exploit existing vulnerabilities.

- **Vulnerabilities** – this refers to the inherent aspects of gambling operators' services which are open to potential exploitation for the purposes of supporting or facilitating money laundering and/or terrorist financing.

These can generally be sub-divided into the following categories:

i. Internal Control Vulnerabilities;
ii. Licensing and Integrity Vulnerabilities;
iii. Customer Related Vulnerabilities;
iv. Product Related Vulnerabilities;
v. Payment Method Vulnerabilities.

- **Description and Comments** – This is a summary of the potential consequences of a given risk materialising based on the GGC's understanding and information obtained by the GGC through various means, including GFIU intelligence reports, Licence Holder volunteered information, supervisory activity, questionnaires and regulatory returns.

- **Mitigating factors** – There is a requirement for controls to be put in place in order to effectively mitigate the possibility of risks materialising. Controls can mitigate vulnerabilities where these are applied in an effective manner. Licence Holders are responsible for implementing controls in the form of AML/CFT risk assessments, policies and procedures and their effective maintenance and revision.

  The GGC's licensing procedures and supervisory approach can also constitute a mitigating factor.

Risk Scoring Matrix:

Probability	Very High - 5	5	10	15	20	25
	High - 4	4	8	12	16	20
	Medium - 3	3	6	9	12	15
	Low - 2	2	4	6	8	10
	Very Low - 1	1	2	3	4	5
		Insignificant - 1	Minor - 2	Moderate - 3	Major - 4	Severe - 5
	Impact					

The overall risk is considered in terms of:

i. The possibility of money laundering or terrorist financing taking place due to the vulnerability in question;
ii. The seriousness of the impact on the industry;
iii. The severity of compliance or legal violations, if they were to occur, and whether these could be easily addressed;
iv. The time and cost involved in implementing the required changes to AML/CFT controls;
v. Whether there is the potential for any reputational damage;
vi. The impact on the operator's business operations.

Very Low Risk (Dark Green) – There is only a remote potential for ML/TF exploitation of vulnerabilities. Any violations would be very minor and self-limited in nature with any remedial actions required unlikely to involve any costs to implement.

Low Risk (Light Green) – There is little potential for ML/TF exploitation of vulnerabilities. Any violations would be minor and easily addressed with some compliance action and potential cost involved. Only a minimal impact on non-core operations.

Medium Risk (Yellow) – There is some potential for ML/TF exploitation of vulnerabilities. There is a potential for more significant breaches which could take time and effort to address with long-term action required and more substantial costs involved.

Higher Risk (Orange) – There is a higher potential for ML/TF exploitation of vulnerabilities. Breaches are likely to require substantial time and effort to address and the costs to remedy the situation will be significant.

High Risk (Red) – There is a very high potential for ML/TF exploitation of vulnerabilities. Breaches will have a severe impact on operations and reputational damage and the costs involved will be substantial.

4.6 This Risk Assessment will be kept under review and updated on an ongoing basis in light of emerging risks and developments.

5. Money Laundering and Terrorist Financing Risk

5.1 The Money laundering and terrorist financing risk within the gambling sector can be attributed primarily to two concerns. In respect of ML the risks lie both in the potential criminal ownership and control of gambling operators and in the potential use of gambling services offered by said operators being used as conduits for the laundering or mere spend of the proceeds of crime.

5.2 The GGC does not consider the TF threat to be of significant likelihood although the impact would be severe. Intelligence provided to the GGC and information obtained during the course of its supervisory activities do not lead us to believe that the TF threat has materialised although there are certain products that could lend themselves to the potential passing of funds destined for terrorist activities between one customer and another. In this respect the primary risk has been determined to be that of poker and the possibility of peer-to-peer transfers between users of the poker platform. This can occur either as transfers involved in 'staking' players or through the deliberate losing of funds (so-called "chip dumping") by one player to another. Through our thematic work, we consider inter-account transfers between players to be a particular area of vulnerability due to the risk appetite of players, operational staff and affiliates in the poker sector and the fact that historically this has not been an area where every operator has had proportionate controls over such transfers.

5.3 The other potential TF issue lies in a sanctioned player utilising the services of a gambling operator.

5.4 Similarly the risk of the gambling sector being utilised for the purposes of financing the proliferation of weapons of mass destruction is considered low although the impact if it was to happen would be severe. Licence Holders should therefore remain mindful of the need to monitor unusual activity and transactions, in particular in respect of any peer-to-peer transfers and to maintain effective screening programmes in relation to their customer base. This is particularly the case in respect of indirect financing which could contribute to the proliferation of chemical, biological, radiological and nuclear weapons, through the use of peer-to-peer gambling services.

5.5 The GGC considers that the foremost means in which ML activity takes place within the gambling sector is through the simple spending of the proceeds of crime for leisure purposes by lifestyle criminals, or due to an association with problematic gambling (theft from employer or breach of position of trust), rather than the traditional laundering of funds *per se*. Whilst an operator's own risk management and fraud controls may substantially reduce the opportunity for traditional money laundering to take place, departures from best practice and failure to follow internal policy and process still create residual risk and the opportunity for criminal exploitation. For example, allowing significant and sustained wagering on short priced favourites without requisite and proportionate levels of customer due diligence The Gambling Division has seen some evidence that such gambling activity, which may be evidence of traditional money laundering techniques (i.e. placement, layering and integration), is not being flagged sufficiently early to prevent possible abuse of a licensees' services for the purposes of money laundering.

5.6 The B2B sector does not fall under the provisions of the POCA regime due to not dealing directly with customer funds. Nevertheless, it remains an important factor in assisting in keeping financial crime out of the gambling sector as a whole due to B2B operators' ability to monitor customer gameplay for any potential red flags and alert the relevant B2Cs where necessary. The GGC therefore continues to expect the B2B sector to play a role in general AML efforts.

6. Regulatory Action & Learning Points

6.1 The following learning points are based on recent enforcement activity and reflect the Commissioner's current expectations of Licence Holders. These have informed the development of the GGC's AML Supervisory Strategy and Licence Holders are expected to take these into account when considering their own risk frameworks and controls.

- **EDD & SOF/SOW**: EDD must be applied promptly and proportionately for high-risk customers, avoiding over-reliance on open-source checks or self-declarations. Reluctance to provide SOF/SOW should be treated as a red flag.

- **Risk Profiling & Monitoring**: Dormant accounts and younger customers warrant enhanced scrutiny. Transactional activity should inform ongoing risk assessments. Operators must detect suspicious patterns such as chip dumping or financial inconsistencies.
- **Suspicious Activity Reporting**: SARs must be filed with the GFIU, even if reported elsewhere. Technical breaches or delays can trigger enforcement action.
- **Audit & Internal Controls**: Periodic independent audits are essential and deficiencies must be remediated without undue delay.
- **High-Risk Customer Discrepancies**: Income and tax information must be reconciled. Voluntarily supplied tax documents must align with financial profiles. Inconsistencies without adequate explanation may necessitate SARs.
- **Governance & Oversight**: AML oversight must be embedded at senior management level. Compliance functions must coordinate effectively, with documented decision-making processes.
- **Regulatory Engagement**: Self-disclosure, cooperation with reviews, and integration of sectoral learning into risk frameworks are expected. Remedial actions taken in good faith may mitigate any potential sanctions.

7. Emerging Risks

While the current risk ratings reflect known vulnerabilities and observed typologies, the Commissioner recognises several emerging risks that warrant close monitoring. These include:

- Potential misuse of cryptocurrency or unregulated third-party payment providers;
- Growing threat from AI drive potential for falsified documentation in remote on-boarding;
- Use of multiple cards and innovative payment methods.

These emerging risks will inform future risk-based supervision priorities.

8. Risk Assessment by Sector

i. Remote B2Cs

Background

6.1 The B2C remote gambling market operates in different but complementary sectors: betting, betting intermediary (exchange), gaming, including slots, bingo and poker, and other products (lottery bets, exchange bets). The majority of B2C licensees provide a full suite of products (fixed odds sports betting, casino products, slot games). For a list of current licensees see here: https://www.gibraltar.gov.gi/finance-gaming-and-regulations/remote-gambling

6.2 The majority of B2C licensees have the UK as their dominant market and a large proportion of the British remote gambling market is supplied by Gibraltar operators. Approximately 72% of gambling activity undertaken in respect of Gibraltar licences is UK and Ireland facing activity, with 28% representing rest of the world business. The UK focus is increasing as various jurisdictions introduce their own licensing regimes and operators are encouraged to take up licences in those jurisdictions.

6.3 Given the importance of the remote gambling sector in Gibraltar and its comparative size in relation to other gambling sectors, the regulatory regime in Gibraltar is primarily focussed on the needs and challenges of remote operations, in particular in respect of AML/CFT and social responsibility issues.

6.4 Within the Remote B2C sector various risk categories have been identified. The threats which exist within the remote B2C sector are that criminals may come to own or control an operator in order to launder funds and that individual users may use the services of a licensed entity in order to spend or launder the proceeds of crime.

6.5 POCA identifies non-face-to-face gambling as being of higher risk. Nevertheless, the fact that customers use payment cards to fund gambling enables Licence Holders to easily track a customer's transactions. However, the quality of data analysis, senior management risk appetite and the expertise of customer due diligence staff (as well as compliance resource allocation) all impact on this area.

6.6 All B2C Licence Holders are subject to the obligations in POCA and the AML Code.

Sector summary

6.7 **The Remote B2C sector is rated a higher risk sector.**

Internal Control Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Failure to apply appropriate controls to mitigate the risk of ML/TF occurring – Higher (High x Major)**

- Description and Comments:

- Non-compliance with the relevant laws and guidance can lead to lapses in the quality of AML/CFT controls. In the course of its supervisory activity, the GGC has encountered evidence that the required standards are not always been met. This can increase the risk of ML/TF activity taking place. Senior management risk appetite, appropriate risk/compliance governance frameworks, appropriate levels of compliance resourcing and the setting of the correct compliance culture is key to ensuring robust controls against potential ML/TF. Failure to implement adequate ongoing monitoring, with appropriate threshold levels for additional checks, is one of the main risk factors encountered by the Gambling Division during the course of its supervisory activity and therefore forms the core of its supervisory approach in respect of conducting in-depth reviews of customer accounts.
- Furthemore, Licence Holders should be mindful of the need to ensure that appropriate due diligence is conducted on high depositing customers, irrespective of whether or not their losses are high. These failures to conduct adequate due diligence have resulted in regulatory settlements with Licence Holders in lieu of a financial penalty being imposed.

- Mitigating Factors:

- All Remote B2C operators are required to abide by the obligations under POCA and the AML code, and must therefore implement systems and controls to mitigate the possibility of their services being used for the purposes of ML/TF. They must also ensure that they have appropriate risk assessments, policies and procedures in place to combat ML/TF and to risk assess new products before they are launched.
- Licence Holders also generally have in place automated systems which trigger alerts in respect of unusual or suspicious activity and all customer transactions are electronically logged and can be tracked and identified.
- Appropriate training of staff.
- CDD and EDD processes are undertaken and PEPs and sanctions screening takes place.
- The GGC's licensing process, ensuring that key individuals are fit and proper, and its supervisory activity, in the form of desk based reviews and on-site visits, help to mitigate the possibility that Licence Holders are not putting in place the required systems and controls to prevent their services being used for ML/TF.
- Enforcement action against Licence Holders where failings have been identified results in tightening of controls and remediation action on the part of the Licence Holder which serves to improve overall compliance.
- While B2C remote gambling remains a higher risk, the trend in failings the GGC has identified is towards more isolated breaches rather than systemic ones which helps to demonstrate that controls are generally becoming more effective.

Licensing & Integrity Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Operator controlled by criminals – Medium (Very Low x Major)**
- **Employee risk – collusion with criminal elements – Medium (Medium x Moderate)**

- Description and Comments:

- While the risk of a remote gambling operator coming under the ownership or control of criminal elements is a recognised risk, the relatively small number of Licence Holders in the jurisdiction, together with the GGC's robust licensing process render this a more theoretical risk, although one that must always be taken into account. The identification of beneficial owners/controllers is paramount.
- Employee collusion remains a risk that Licence Holders must be vigilant of. The GGC has not encountered cases in which key individuals were colluding with criminals for the purposes of ML/TF, however, examples of lower level employees acting in their own interests and not in accordance with the expected standards exist and thus the potential risk of a more significant case of employee collusion must be taken into account.
- There nevertheless remains a risk that, due to inadequate training, staff may inadvertently facilitate the use of the proceeds of crime by not being adequately attentive to red flags.

- Mitigating Factors:

- Licence Holders must all undergo a stringent licensing process by the GGC, ensuring that all key individuals are fit and proper, undergoing background checks for previous criminal conduct and a comprehensive due diligence process.
- Licence Holders are required to vet and train their staff and to be vigilant against the potential risks that their own employees may pose. They have a vested interest in ensuring their systems minimise any potential damage which may result from an employee not acting with the required integrity and are under an obligation to adequately train their staff to a level commensurate with their role
- Key individuals must satisfy the GGC that they are fit and proper.

Customer Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Non-face-to-face nature of remote gambling – Higher (Medium x Moderate)**
- **False Documentation – Medium (Medium x Moderate)**
- **PEPs using remote B2Cs in order to launder the proceeds of crime – Low (Low x Moderate)**
- **Customers on international sanctions lists laundering illicit funds – Medium (Low x Major)**
- **Customers from High Risk Jurisdictions laundering funds – Low (Low x Moderate)**
- **Customers whose occupation may present a higher risk of theft from employer to fund their gambling – Higher (High x Major)**
- **Younger customers in the 18-24 age group (Medium x Moderate)**

- Description and Comments:

- The non-face-to-face nature of remote gambling is recognised as a higher risk in POCA. However, this is largely mitigated by CDD and EDD measures and the ability of remote gambling operators to effectively access and monitor a full audit of transactions and other data including IP addresses, device identifiers, etc.
- The possibility that customers may attempt to use fraudulent or stolen identification documents is an extant one, however, the GGC's supervisory activity has revealed that Licence Holders generally have effective measures in place to be able to identify fraudulent documents although some instances have also escaped

the notice of due diligence teams, and some have proved themselves to be more adept than others. The increasing sophistication of criminals in using false or stolen IDs presents a constant challenge to operators.

- While Licence Holders do have PEPs on their books, there is limited evidence that they are using the services of remote gambling operators to launder the proceeds of crime; this is underscored by the very limited number of SARs relating to PEPs that have been submitted by the remote gambling sector. Furthermore, the data collected by the GGC indicates that the number of PEPs who have been on-boarded is not large and there is also some evidence of de-risking in this area.
- The evidence in respect of customers on international sanctions lists using remote gambling operators for the purposes of ML/TF is likewise limited, with Licence Holders reporting that any 'matches' are in fact false positives.
- GGC data obtained from Licence Holders suggests that the numbers of registered customers from high-risk jurisdictions are small and there is limited evidence that these are laundering the proceeds of crime through gambling operators.
- There is evidence that some customers will illicitly acquire funds from their employers in order to fuel their gambling.

- Mitigating Factors:

- All Licence Holders are obliged to comply with the provisions of POCA and the AML Code.
- POCA stipulates that non-face-to-face customers are higher risk and thus must undergo enhanced due diligence measures.
- All customers must register an account with remote B2Cs and electronic software is readily available to assist in automatic electronic verification of customers while manual methods can be resorted to where necessary.
- All transactions are electronically recorded and can be monitored.
- Licence Holders have systems in place to screen customers against international sanctions lists, to check whether they are PEPs and to risk assess them based on their jurisdiction; these are assessed in the course of the Gambling Division's supervisory activity.
- Licence Holders are required to conduct CDD measures in respect of all customers and should take into account varying factors, including age, when establishing a customer profile.

Product Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Peer-to-peer gaming (poker) – Higher (High x Moderate)**
- **Low-odds betting - Medium (Medium x Moderate)**

- Description and Comments:

- The possibility of collusion between players in online poker is a higher risk. 'Chip dumping' is considered by the GGC to be one of the primary ways in which TF could potentially occur within the remote gambling sector although GGC intelligence suggests the risk remains a largely theoretical one at present. 'Chip dumping' does occur but is typically for a variety of other reasons which do not involve ML or TF although it is still a prohibited practice according to operators' terms and conditions.
- Inter-account transfers between poker players/affiliates is a key area of ML, TF, and PF vulnerability which requires appropriate levels of control and additional due diligence measures. Poker players generally have a high-risk appetite and can themselves be exploited as facilitators in the movement of criminal funds.
- Where a customer recycles or attempts to recycle criminal funds or a proportion of such funds through gambling facilities either through engaging in minimal or very low risk activity such as low-odds sporting events.

- Mitigating Factors:

- Licence Holders implement systems to assist in detecting and preventing collusion (so-called 'chip dumping', i.e. deliberately losing to another player for the purposes of transferring one's funds to them).
- Licence Holders have systems in place to monitor unusual betting activity.

Payment Method Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **E-Wallets masking origin of funds – Medium (Medium x Moderate)**
- **Pre-paid cards (cash funded) masking origin of funds – Medium (Medium x Moderate)**
- **Use of crypto-currency – Medium (Medium x Moderate)**

- Description and Comments:

- E-Wallets, the use of betting shops to fund online accounts in operators that have both a land-based and online presence and the use of pre-paid cards can lead to difficulties in determining the provenance of funds in particular where cash is used to fund these. Nevertheless, multi-channel operators have systems in place to be able to link these (single view of the customer) and this helps mitigate the risks.
- Furthermore, Licence Holders must conduct due diligence in respect of source of funds and wealth and undertake ongoing transactional monitoring to reduce the likelihood of the risks materialising.
- Risks also arise in the form of crypto-currencies although, to date, their use has only been minimally adopted by Licence Holders, and the GGC continues to require Licence Holders to present credible AML/CFT policies and procedures in respect of their adoption before it is accepted. There remains some risk that E-Wallets and pre-paid cards are funded by crypto-currencies. The GGC monitors the extent of crypto use by Licence Holders.

- Mitigating Factors:

- Licence Holders implement systems to enable them to link multi-channel accounts.
- Licence Holders are required to identify and verify the identity of their customers which helps mitigate issues in respect of payment methods such as e-wallets and pre-paid cards which may render identifying where the source of funds more problematic.
- On-going monitoring of transactions and checks on source of funds and wealth.
- Alerts in respect of mismatches between registered customer details with a Licence Holder and those registered with the E-Wallet provider.
- Relationship between Licence Holders and merchants providing the services in order to provide support and information.

ii. Remote B2Bs

Background

6.8 The B2B sector provides B2C companies with access to their bespoke gaming software.

6.9 Each new partner proposal is an AML/CFT engagement within a wider regulatory assessment as they must present due diligence material and receive formal approval before engaging in business. A B2B operator can have several approved partners. A list of current B2B licensees can be found at: https://www.gibraltar.gov.gi/finance-gaming-and-regulations/remote-gambling

B2B operators do not deal directly with customer funds and therefore fall outside the purview of POCA provisions. Nevertheless, in the context of the gambling system as a whole in Gibraltar, B2B operators form an important part of the ecosystem and therefore the Gambling Commissioner expects them to fulfil a role, proportionate to their capacity, in helping to prevent the gambling sector being used for the purposes of financial crime. This is due to their role in providing a window into the gameplay and betting patterns of customers even where they do not have access to the customer's details or control their funds. Where a B2B (e.g. Poker network provider, games provider) is involved in supplying services to monitor and reduce fraud and operator risk on behalf of customer facing operators, then the Gambling Commissioner expects that B2B to carry out those functions in an effective manner. This will include identifying suspicious activity/transactions and escalating to reporting B2C partners. Where systemic or market wide risk has been identified then a report should also be made to the Gambling Commissioner. Failure to monitor for fraud, risk, money laundering or potential TF by B2B providers, in line with contractual and regulatory oblations could be considered a breach of fitness and propriety standards applicable to all licensees.

Sector summary

6.10 **The Remote B2B sector is rated a low risk sector.**

Internal Control Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Non-implementation of relevant legislation (POCA) and guidance from the supervisor (AML Code) – Medium (Medium x Moderate)**

- Description and Comments:

- While B2B Licence Holders are not exposed to the same risks as customer-facing operators, they are nevertheless under an obligation to monitor customer behaviour on their servers for AML/CFT purposes, in particular because the nature and style of play taking place is not visible to the B2C operator. B2B operators may sometimes consider the absence of customer data or deposits into their systems as meaning they have no obligation to monitor customer behaviour. This responsibility is elaborated upon in the AML Code.

- Mitigating Factors:

- B2B Licence Holders are subject to the provisions of POCA and the AML Code (insofar as it relates to them).
- The GGC's licensing process, ensuring that key individuals are fit and proper, and its supervisory activity, in the form of desk based reviews and onsite visits, help to mitigate the possibility that Licence Holders are not putting in place the required systems and controls to prevent their services being used for ML/CFT.
- B2Bs must have due diligence procedures in place in respect of the partners they do business with and must monitor customer behaviour on their servers in accordance with the AML Code.
- Use of regulatory technology to mitigate risks arising from acceptance of cryptocurrency.

Licensing and Integrity Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Operator controlled by criminals – Medium (Very Low x Major)**
- **Employee risk – collusion with criminal elements – Medium (Medium x Moderate)**

- Description and Comments:

- While the risk of a B2B operator coming under the ownership or control of criminal elements is a recognised risk, the relatively small number of Licence Holders in the jurisdiction, together with the GGC's robust licensing process render this a more theoretical risk, although one that must always be taken into account. Furthermore, the B2B partner approval process entails further scrutiny of a B2B's approach.
- Employee collusion remains a risk that Licence Holders must be vigilant of. The GGC has not encountered cases in which key individuals were colluding with criminals for the purposes of ML/TF, however, examples of lower level employees acting in their own interests and not in accordance with the expected standards exist and thus the potential risk of a more significant case of employee collusion must be taken into account.

- Mitigating Factors:

- Licence Holders must all undergo a stringent licensing process by the GGC, ensuring that all key individuals are fit and proper, undergoing background checks for previous criminal conduct and a comprehensive due diligence process.
- B2B Licence Holders are required to submit their proposed business relationships to the GGC for approval.
- Licence Holders are required to vet and train their staff and to be vigilant against the potential risks that their own employees may pose. They have a vested interest in ensuring their systems minimise any potential damage which may result from an employee not acting with the required integrity.
- Key individuals must satisfy the GGC that they are fit and proper.

Customer Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Business relationships leading to AML/CFT exposure – Low (Low x Moderate)**

- Description and Comments:

- B2B Licence Holders are required to implement due diligence procedures in respect of their business partners in order to ensure that they do not enter into relationships with unsuitable entities which may present an ML risk. The GGC's approval process provides oversight into the processes implemented by B2B Licence Holders and it has sometimes been observed that the comprehensiveness of the due diligence conducted varies between Licence Holders; on such occasions the Licence Holder is subject to remedial action on a compliance basis in order to increase standards.

- Mitigating Factors:

- Requirement for B2Bs to apply internal due diligence processes to potential business partners including obtaining information on the ultimate beneficial ownership and control of those partners wishing to use their systems.
- The GGC also requires that all customer facing 'joint venture' B2B relationships are submitted for approval and are subject to ongoing monitoring by the Licence Holder to ensure the service is being used as envisaged at the time of approval.

Product Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Lack of visibility in relation to player data and gambling activity – Higher (High x Moderate)**

- Description and Comments:

- In most technical arrangements of B2B 'table game' supply, the B2C operator does not have access to real time game play or game performance statistics. The requirement for the monitoring of table games for potential money laundering or terrorist financing methods applies equally to B2B games suppliers as it does to B2C operators' in-house table games, otherwise suspicious gameplay on B2B servers may be concealed from the B2C operator. The parties should therefore, when negotiating their commercial arrangements, agree the method by which table games will be monitored in real time for recognised money laundering or terrorist financing 'gameplay' methodologies and reported to the B2C operator in a timely and proportionate way should they occur, allowing for possible interventions in funds transfers or withdrawals.
- Given the evolving nature of ML/TF methodologies it is expected that the details of the monitoring which will be carried out will be agreed between the parties from time to time and need not be set out in precise detail at the outset. Once agreed, however, these should be documented and made available to the Gambling Commissioner as and when required. While some methodologies are transparent and easy to identify (e.g. repeated low risk bets in roulette), P2P transfers can be highly sophisticated, shielded and complex.

- Mitigating Factors:

- B2B Licence Holders are under an obligation to monitor customer activity and alert their B2C partners of suspicious gameplay.

iii. Casino (Land-based)

Background

6.11 There is currently one licensed land-based casino operator in Gibraltar. Its offering consists of slot machines, table games and bingo and poker events (rare). It is a relatively low turnover/margin business where high value customers are should be quickly apparent and subject to close supervision by the casino.

Sector summary

6.12 **The Casino (Land-based) sector is rated a higher risk sector.**

Internal Control Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Non-implementation of relevant legislation (POCA) and guidance from the supervisor (AML Code – Non-Remote) – Medium (Medium x Moderate)**

- Description and Comments:

- A failure to implement adequate controls could lead to casino services being used for the purposes of money laundering.
- There is only one licensed casino operator in the jurisdiction. This is a well-known, established multi-national operator which is nevertheless subject to the same robust due diligence process as remote operators.

- Issues relating to the challenges of monitoring slots play.

- Mitigating Factors:

- Casinos are subject to the provisions of POCA and the AML Code for the non-remote sector and must implement systems and controls in order to mitigate the possibility of ML/TF occurring through their premises.
- The GGC's licensing process, ensuring that key individuals are fit and proper, and its supervisory activity, in the form of desk based reviews and on-site visits, help to mitigate the possibility that Licence Holders are not putting in place the required systems and controls to prevent their services being used for ML/CFT.

Licensing and Integrity Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Operator controlled by criminals – Medium (Low x Major)**
- **Employee risk – collusion with criminal elements – Higher (Medium x Major)**

- Description and Comments:

- While the risk of a casino coming under the ownership or control of criminal elements is a recognised risk, the fact there is only one casino licence holder, together with the GGC's robust licensing process render this a more theoretical risk, although one that must always be taken into account.
- Employee collusion remains a risk that Licence Holders must be vigilant of. The GGC has not encountered cases in which key individuals were colluding with criminals for the purposes of ML/TF, however, examples of lower level employees acting in their own interests and not in accordance with the expected standards exist and thus the potential risk of a more significant case of employee collusion must be taken into account.

- Mitigating Factors:

- Licence Holders must all undergo a stringent licensing process by the GGC, ensuring that all key individuals are fit and proper, undergoing background checks for previous criminal conduct and a comprehensive due diligence process.
- Licence Holders are required to vet and train their staff and to be vigilant against the potential risks that their own employees may pose. They have a vested interest in ensuring their systems minimise any potential damage which may result from an employee not acting with the required integrity.
- Key individuals must satisfy the GGC that they are fit and proper.

Customer Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Use of 'smurfing' in order to bypass threshold reporting requirements – Medium (Medium x Moderate)**
- **Use of proxies – Low (Low x Moderate)**
- **False Documentation – Higher (High x Moderate)**
- **PEPs using casinos to launder corrupt funds – Low (Low x Moderate)**
- **Customers on international sanctions lists laundering illicit funds - Low (Low x Moderate)**

- **Customers from high risk jurisdictions using the casino's services to launder the proceeds of crime - Low (Low x Moderate)**
- **Proximity to organised crime groups - Higher (Medium x Major)**

- Description and Comments:

- Casinos are required to implement effective controls against ML/TF and the GGC's supervisory activity suggests that it does so. However, this may not always be up to the more sophisticated standards of remote gambling operators with less in the way of the use of software to help establish and verify identities as well as ongoing monitoring of customer spend.
- The jurisdiction's proximity to organised crime groups presents another risk as identified in the National Risk Assessment and the casino must be on guard against customers linked to such organisations using the proceeds of crime in the casino for leisure purposes.
- The practice of smurfing and the use of false identification documents are recognised as risks by the FATF in the non-remote casino sector.
- There is little evidence that PEPs, people on international sanctions lists or from high risk jurisdictions use the casino for the purposes of laundering the proceeds of crime. It is in general a domestic trade supplemented by some tourist activity.
- There is also little evidence of the use of proxies or agents in the casino although this remains a theoretical risk.
- The casino services a destination tourist market, but also a local market where over familiarity with that local market could foster a false sense of security and false assumptions about the legitimacy of the source of player funds. This could lead to under-reporting of suspicious activity
- Cross-border risks in relation to foreign nationals and illegal activity in the "Campo de Gibraltar" area.

- Mitigating Factors:

- Casinos are under an obligation to abide by the requirements of POCA and the AML Code – Non-Remote. This includes undertaking CDD, including enhanced due diligence and ongoing monitoring.
- POCA requires casinos to establish and verify a customer's identity where gambling chips with a value of 2000€ or more are purchased or exchanged.
- Casinos are required to comply with requirements in respect of PEPs, international sanctions lists and high risk jurisdictions.
- Casinos implement measures such as use of CCTV and table monitoring which can help identify suspicious activity.

Product Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Peer-to-peer gaming (Poker Tournaments) – possibility of collusion – Higher (High x Moderate)**
- **Slots – Higher (High x Moderate)**
- **Electronic Roulette - Medium (Medium x Moderate)**

- Description and Comments:

- When hosting poker tournaments, there is a risk that participants will collude with each other for the purposes of transferring illicit funds.
- Slots present an issue in respect of monitoring funds that are spent in them.
- Electronic roulette entails reduced customer interaction with members of staff and the use of ticket in ticket out (TITO) facilities.

- Mitigating Factors:

- The casino uses CCTV and staff monitoring to reduce the risk of collusion taking place.

- There has been a substantially reduced level of activity in respect of poker tournaments and the possibility of any risks materialising are therefore also reduced.
- There is some monitoring of slots activity through signing up to the membership scheme and use of CCTV, together with human intervention as well as the possibility of monitoring any spikes which occur in individual machines.
- Automatic redemption of TITO at machines is limited to a low amount, otherwise requiring human interaction.

Payment Method Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Cash Transactions - Higher (High x Moderate)**
- **Foreign Currency Exchanges - Higher (High x Moderate)**
- **TITO – Higher (High x Moderate)**

- Description and Comments:

- Cash is recognised as being a method of payment attractive to criminals involved in ML/TF due to difficulties in respect of tracing it, the ease with which it can be transferred and the fact it helps facilitate anonymity.
- As recognised by the FATF, casinos carry out certain services such as foreign currency exchanges which are akin to a financial institution.
- TITO systems have the potential to allow criminals to launder the proceeds of crime by feeding TITO machines with low denomination cash with the ticket then cashed at the cashier's desk after minimal play and for higher denomination notes.
- Potential weaknesses in cash desk control and player monitoring.
- Monitoring of receipt and exchange of high denomination Euro notes and cumulative quantities of Euros.

- Mitigating Factors:

- Casinos are fully regulated and must comply with requirements under POCA and the AML Code – Non-Remote.
- Controls are in place in respect of enforcing membership and obtaining CDD where transactions over a certain threshold are met.
- Foreign currency exchange without membership and the CDD that membership entails is only permitted in lower amounts below a certain threshold; source of funds is required where buy-ins are made in a foreign currency by bank transfer.
- Automatic redemption of TITO at machines is limited to a low amount, otherwise requiring human interaction.

iv. Betting Shops

Background

5.11 There are currently two betting shops and one sports bar (physically linked to the casino) in Gibraltar; these are licensed and regulated by the GGC for betting purposes. This licence was awarded to a long-standing and experienced licensee. These are not high turnover businesses.

Sector Summary

6.12 **The Betting Shop sector is rated a medium risk sector.**

Internal Controls Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Non-implementation of relevant legislation (POCA) and guidance from the supervisor (AML Code) Medium (Medium x Moderate)**

- Description and Comments:

- A failure to implement adequate controls could lead to betting shops not effectively mitigating the risk that their services are used to spend the proceeds of crime.

- Mitigating Factors:

- Betting shops are subject to the provisions of POCA and the AML Code for the non-remote sector and must implement systems and controls in order to mitigate the possibility of ML/TF occurring through their premises.
- The GGC's licensing process, ensuring that key individuals are fit and proper, and its supervisory activity, in the form of desk based reviews and on-site visits, help to mitigate the possibility that Licence Holders are not putting in place the required systems and controls to prevent their services being used for ML/TF.

Licensing and Integrity Vulnerabilities

- **Operator controlled by criminals – Medium (Very Low x Major)**
- **Employee risk – collusion with criminal elements – Medium (Medium x Moderate)**

- Description and Comments:

- While the risk of a betting shop coming under the ownership or control of criminal elements is a recognised risk, the betting shops in the jurisdiction (of which there is only one in addition to a sports bar offering some betting facilities) are under the control of an already existing licensee. The GGC's robust licensing process render this a more theoretical risk, although one that must always be taken into account.
- Employee collusion remains a risk that Licence Holders must be vigilant of. The GGC has not encountered cases in which key individuals were colluding with criminals for the purposes of ML/TF, however, examples of lower level employees acting in their own interests and not in accordance with the expected standards exist and thus the potential risk of a more significant case of employee collusion must be taken into account.

- Mitigating Factors:

- Licence Holders must all undergo a stringent licensing process by the GGC, ensuring that all key individuals are fit and proper, undergoing background checks for previous criminal conduct and a comprehensive due diligence process.
- Licence Holders are required to vet and train their staff and to be vigilant against the potential risks that their own employees may pose. They have a vested interest in ensuring their systems minimise any potential damage which may result from an employee not acting with the required integrity.
- Key individuals must satisfy the GGC that they are fit and proper.

Customer Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Anonymous Customers - Medium (Medium x Moderate)**
- **False Documentation – Higher (High x Moderate)**

- Description and Comments:

- There is some risk in the fact that anonymous customers are able to place bets at betting shops.
- The use of false identification documents is a potential risk.
- Gibraltar has a high concentration of (industry) sports traders who may exploit inside information and seek to circumvent risk controls.

- Mitigating Factors:

- The use of CCTV and employee interaction assists the betting shop in building a profile of its customers and they are then able to further monitor any higher spending customers.
- The risk of any substantial money laundering is mitigated by the limits set by the betting shop in respect of how much may be staked over the counter, the nature of the business which comprises low level leisure betting from locals and holiday makers and this limits the level of risk posed.
- The size and nature of the betting shop in Gibraltar, in respect of the number of customers frequenting it, and the level of bets that may be placed substantially limit the risks posed.

Product Related Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Betting terminals - Medium (Medium x Moderate)**

- Description and Comments:

- Betting shops host betting terminals in which customers can place bets in lieu of transacting with a member of staff. This increases the potential for such activity to go unmonitored and for potentially anonymous customers to place repeated bets which could go unnoticed.

- Mitigating Factors:
-
- The use of CCTV and employee interaction assists the betting shop in building a profile of its customers and they are then able to further monitor any higher spending customers as they utilise the betting terminals.
- Risk management systems permit Licence Holders to monitor unusual betting activity and large amounts or atypical betting patterns are able to be picked up.

Payment Method Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Cash transactions - Higher (High x Moderate)**

- Description and Comments:

- Cash is recognised as being a method of payment attractive to criminals involved in ML/TF due to difficulties in respect of tracing it, the ease with which it can be transferred and the fact it helps facilitate anonymity.

- Mitigating Factors:

- The use of CCTV and employee interaction assists the betting shop in building a profile of its customers and they are then able to further monitor any higher spending customers. The relatively small number of customers also assists in respect of staff awareness of customers and their betting profiles.

v. Lotteries

Background

6.13 Gibraltar only operates one state run lottery and the risk of ML through the purchase of winning tickets is considered low due to the relative low pay-outs of the lottery, making this unattractive for large scale ML. Smaller scale 'raffles' may take place in social clubs and organisations but these are for charitable purposes and do not present a risk of ML/TF as they are low stake, low frequency and small prize gambling. Small-scale lotteries such as these are authorised by the Licensing Authority. The Gibraltar Government Lottery is run by the Treasury Department of the Government of Gibraltar.

6.14 Being a state run lottery entails there is no risk of criminal elements gaining ownership or control of a lottery operator and there are no large-scale, privately run, non-remote lottery operators.

Sector Summary

6.15 **The lotteries sector is rated a low risk sector.**

Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Anonymous customers – Very Low (Low x Minor)**
- **Criminals acquiring lottery tickets - Low (Low x Moderate)**
- **Cash transactions – Low (Low x Minor)**

- Description and Comments:

- Customers do not need to present ID when purchasing tickets which may present an increased risk.
- There is a theoretical risk that a criminal may acquire a winning lottery ticket in order to present this as a means to justify unexplained wealth which has been accrued through criminal activity.
- Cash is recognised as being a method of payment attractive to criminals involved in ML/TF due to difficulties in respect of tracing it, the ease with which it can be transferred and the fact it helps facilitate anonymity.

- Mitigating Factors:

- Customers are predominantly from the local community and therefore known to the sellers.
- While this may present a risk it should be reiterated that the evidence suggests this remains a theoretical risk and not one that has materialised. Furthermore the maximum prizes involved in respect of the lottery are not such that they would be attractive to criminal elements engaged in large-scale money laundering.
- There are typically only small sums of money being exchanged in respect of the state lottery.

vi. Other Sectors: Bingo, Gaming Machines (outside Casino Premises)

Background

6.16 The licensing of gaming machines outside casinos was brought under the GGC's remit as from 1 April 2016. Both the suppliers of gaming machines and businesses which keep gaming machines on their premises must apply for a licence. There are approximately 220 machines active in cafes, pubs, bars and similar commercial premises throughout Gibraltar at any given time. This number has historically been strictly controlled by the Government of Gibraltar whose policy it is to ensure that there is no significant proliferation of gaming machines in the community.

6.17 In respect of bingo tournaments outside casino premises, these are typically limited, low-level events in clubs and associations for charitable purposes; premises may on occasion seek to host a 'one off' event for which they must seek the GGC's approval.

Sector Summary

6.18 **The other: bingo, gaming machines (outside casino premises) sector is rated a low-medium risk sector.**

Vulnerabilities

- Vulnerabilities and Risk Rating (Probability x Impact):

- **Bingo – Low (Low x Minor)**
- **Gaming Machines - Low (Medium x Low)**

- Description and Comments:

- There is a potential risk that bingo operations are used in order to facilitate the spending of the proceeds of crime in premises.
- Gaming machines are permitted in various locations such as bars, restaurants, pubs and clubs and also betting shops. While these machines do not permit stakes or offer prizes on the same scale as those which can be found in casino premises, there is nevertheless a risk that laundering may take place through the use of these machines; this is a vulnerability that is aggravated by the ability to remain anonymous. In respect of gaming machine suppliers, they are B2B operators and have no direct customer facing engagement.

- Mitigating Factors:

- Smaller clubs and associations may hold bingo events but these are small-scale and for charitable purposes; they also require prior approval from the GGC. These would not be an attractive avenue for large scale ML and the GGC has seen no evidence that ML has taken place during such events.
- Gaming machines are subject to licensing and must be monitored by staff or through the use of CCTV. They are not high stake machines. In respect of gaming machine suppliers, they are B2B operators and have no direct customer facing engagement.

End.