AML/CFT Guidance

For OGRA Licence Holders with Network Services Permissions

V1 – October 2025

Ground Floor, St George's Court | Myrtle Street, Douglas | Isle of Man, IM1 1ED
+44 (0)1624 694331 GSCAMLInspections@gov.im
www.isleofmangsc.com

Contents

Version Control

This version of the guidance is effective from October 2025.

Version	Date published	Comments
1.0	October 2025	AML/CFT guidance published for OGRA licence holders with Network Services Permissions.

1.0 General

1.1 Abbreviations

AML/CFT/CPF	Anti-money laundering and countering the financing of terrorism (also incorporates countering proliferation financing). Throughout this document inspection of AML is to be read as inclusive of AML/CFT/CPF
AML Guidance	AML Guidance for Operators
AML Forum	Regular forum hosted by the GSC for Nominated Officers and MLROs, DMLROs and AML/CFT Compliance Officers
ATCA	Anti-Terrorism and Crime Act 2003
CFT	Countering the financing of terrorism (where this term is used it also includes the countering the financing of proliferation)
FATF	The Financial Action Task Force
FT	Financing of terrorism (defined in the Code as including the financing of proliferation)
IOM FIU	Isle of Man Financial Intelligence Unit
FRSB	FATF Style Regional Body
Gambling Act	Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018
GSC	The Isle of Man Gambling Supervision Commission which includes the Board of Commissioners and the Inspectorate
IOM	Isle of Man, "The Island"
MLRO	Money Laundering Reporting Officer
ML	Money Laundering
MONEYVAL	The committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism
Network Permission Holder	Any OGRA licence holder with the approved permission 8a) Network Services
NRA	National Risk Assessment
OGRA	Online Gambling Regulation Act 2001
Operator	A holder of a licence issued under the Isle of Man Online Gambling Regulation Act 2001
PEP	Politically exposed person
POCA	Proceeds of Crime Act 2008
PF	Proliferation Financing – providing funds or financial services that in some way assist the manufacture, acquisition, possession, development, transport, export etc of nuclear, chemical, biological, or radiological weapons
The Code	The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism Code 2019) (including a minor amendment to the AML/CFT Officer requirements via the AML/CFT (General and Gambling) (Amendment) Code 2019)
Tipping off	An offence committed by anyone within a regulated business of disclosing a suspicion of ML or FT/PF to the suspect or a third party where that information is likely to prejudice an investigation
TOCFRA	The Terrorism and Other Crime (Financial Restrictions) Act 2014

1.2 About this Document

This document has been prepared by the Gambling Supervision Commission (GSC) and provides guidance to support the development of a framework for compliance with the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019. It is intended to assist licence holders operating network models in interpreting and applying the Code in a manner that reflects the nature of their services and operational arrangements.

Further information on network models can be found in the GSC's licence application guidance: www.isleofmangsc.com/media/fd3nmwma/online-gambling-guidance-for-making-a-licence-application-v1-16.pdf

The guidance seeks to directly connect the Code and guidance issued by the GSC with the recommendations of the Financial Action Task Force (FATF). Accordingly, FATF's Recommendations and observations are referenced throughout the document where relevant.

In compiling this guidance, the GSC has also considered literature relating to anti-money laundering, countering the financing of terrorism, and countering proliferation financing published by MONEYVAL, as well as findings from the Isle of Man's National Risk Assessment (NRA) and National Risk Appetite Statement (NRAS):

https://www.gov.im/about-the-government/departments/cabinet-office/national-risk-assessment.

https://www.gov.im/media/1388810/national-risk-appetite-statement-egaming-financial-crime-may-2025.pdf

Throughout this document, readers will find guidance on AML/CFT/CPF policy, FATF Recommendations, and relevant provisions of the Code. The contents of this guidance should not be construed as legal advice.

1.3 About the GSC

The GSC is responsible for regulatory oversight of the gambling sector including Operators' compliance with legislation such as the Gambling Acts and the Code. The GSC is an independent statutory board of Tynwald and comprises the Inspectorate and the board of the GSC.

For more information about the GSC, its structure and its statutory functions, please visit the GSC's website www.isleofmangsc.com/gambling.

Supervision

The GSC has produced guidance on its Supervision Methodology and Inspection Procedures which can be found on the AML Inspections page - https://www.isleofmangsc.com/gambling/anti-money-laundering/aml-cft-inspections/

Further to these high level documents, detailed AML Guidance is issued separately by the GSC and can be found here http://www.isleofmangsc.com/media/zhnhounf/aml-cft-guidance-for-gambling-operators-v1-3.pdf

Supervision is carried out using a risk-based approach, all Operators are subject to regular inspections, the cycle being informed by both—

- **Inherent risks** - factors that do not change as often such as type of business model, products offered and customer risks; and
- **Dynamic risks** – factors that can change such as compliance history.

Inspections will primarily focus on the period between either licensing or the date of the previous inspection where relevant, and the beginning of the current inspection.

An AML inspection is split into three distinct stages—

- **Desk-top Review** – An Operator will be asked to provide pre-visit documentation which includes relevant policies and procedures, training logs etc and a date for an onsite visit will be agreed. The GSC will also review supervisory information provided during the period to be supervised such as quarterly and annual returns;

  During this period Operators will be supplied with a self-assessment template to fill in as well as a Network Partner Sample sheet. The review of this information alongside supporting documentation allows the Inspectorate to test the Operator's technical compliance of its AML framework (i.e. its policies and procedures). This also forms part of the preparation of areas tested during the onsite stage of the inspection;
- **Onsite** – The AML inspections team will, accompanied by the lead general inspector for the Operator, visit an Operators premises in person to look at the effectiveness of the mechanisms reported under the self-assessment and through the pre-inspection documents (i.e. how well measures are applied in practice). An onsite matrix will be used to ask standard format questions however these are tailored to the business model and are informed by the desk top review findings;
- **Post Onsite Review & Report** – following the onsite inspection the AML inspections team will request any outstanding documents and/or additional information identified to evidence compliance and ensure a fair and accurate assessment; and
- Once reviewed a draft report is issued covering both technical findings from the self-

assessment and practical findings from the onsite. A final report is then issued following a review of factual accuracy by the Operator at which point the inspection is concluded.

The results of any compliance findings are fed back into the ongoing risk assessment process to determine the frequency of ongoing inspections. Lower risk and/or more compliant licence holders being inspected with less frequency and conversely multiple compliance failings will result in higher risk ratings and more frequent inspections.

Where the outcome of any inspection includes remedial actions, the Operator will be expected to form a remediation plan and these remediation actions will be monitored for completion and follow up visits may be more targeted to these areas. Compliance failings that meet the criteria for enforcement, for instance they are widespread, deliberate, material in nature, repeated etc will result in an escalation to the enforcement team for consideration and more information can be found on the AML Guidance page in the enforcement Strategy outlined on page 5 of the GSC Guidance on the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018.

2.0 The Financial Action Task Force and MONEYVAL

The FATF is an intergovernmental policy-making body which aims to set standards for AML and generate the necessary political will to adhere to those standards.

As a body it sets international standards, known as the FATF Recommendations, for AML and to promote the effective implementation of those standards. It also has a role to identify deficiencies at the national level. Where significant and sustained deficiencies are identified, the FATF publishes lists to warn others of weaknesses in those countries which adversely effects business and encourages compliance.

The body which currently scrutinises the IOM's compliance with FATF's recommendations is an associate member of FATF known as a FSRB (FATF-style regional body) called the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL for short).

The FATF also works closely with independent organisations which have a role to play in combating ML/FT; these organisations are called observers and include the International Monetary Fund, Interpol, The World Bank, United Nations Committees and several regional financial institutions and development banks.

The FATF regularly reviews and updates its Recommendations to ensure they remain up-to-date and relevant.

2.1 The FATF's Recommendations and Methodology

Originally created in 1990 to combat the misuse of financial systems by persons laundering drug money, the FATF's mandate was broadened in 2001 to include the interception of terrorist financing. Forty Recommendations and eight, (later nine) Special Recommendations were endorsed by over 180 countries as the international standard.

The latest Recommendations from the FATF (40 in total) were first published in February 2012 and are known as the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". Alongside the Recommendations sits the FATF Methodology that sets out the criteria for assessing countries' compliance with the Recommendations.

Recommendation 1 of this set of international standards states that countries must identify and assess the risks of ML and FT that could occur within their jurisdiction and take the measures described in the standards to address those risks.

The principal laws of the IOM to combat FT/ML are:

- ATCA;
- POCA;
- TOCFRA; and
- Financial Intelligence Unit Act 2016 (FIU Act).

2.2 MONEYVAL and its Evaluation of the Island

MONEYVAL assesses its members' compliance in the legal, financial and law enforcement sectors through a peer review process of mutual evaluations, including assessing the effectiveness with which measures to tackle ML and FT are implemented in practice. The Committee also makes recommendations to national authorities to improve their systems.

In 2016, a group of MONEYVAL experts carried out an assessment of the Isle of Man. The assessment looked at the technical framework in place (legislation, policies and procedures) and the effectiveness with which these measures were implemented.

The findings of this assessment were published in the IOM's Fifth Round Mutual Evaluation Report (MER) and highlighted areas where improvements were required.

The IOM was placed into an 'enhanced follow-up' process with MONEYVAL, to monitor progress in improving its AML regime.

The IOM Government, regulatory and law enforcement authorities have undertaken a considerable amount of work since the publication of the MER in 2016, to address the findings and numerous recommended actions of the in-depth assessment.

In 2020, a review report was published by the IOM Government on the progress, which has been made in relation to tackling ML and combatting FT. The review demonstrated that the IOM had made significant progress and highlighted what work has been completed since the MONEYVAL evaluation took place, providing a more detailed analysis of actions taken against each of the recommendations made in the MER.

The IOM is now positively marked in 39 out of the 40 FATF Recommendations, which puts the it amongst a select group of leading nations in the world for technical compliance in AML measures.

Please see the FATF and MONEYVAL section of our AML Guidance webpage for more information.

3.0 Financial Crime

One of the GSC's three primary objectives is to keep the gambling industry crime free.

Operators in the gambling sector in the IOM are regulated entities. This means that they must adhere to obligations placed upon them by law to combat ML/FT. Collectively these requirements are known as AML controls.

See the GSC's AML Guidance for definitions of ML, FT and PF.

The GSC is the regulator that supervises the island's regulated gambling sector's compliance with AML and plays a key role in maintaining the IOM as a well-regulated jurisdiction.

Criminals, including terrorists, attempt to use the world's financial systems to benefit from crime or fund projects designed to further their causes, sometimes resulting in further criminality or acts of terror. Some terrorist organisations have an interest in obtaining weapons of mass destruction (so called chemical, radiological, biological and nuclear devices) for the purposes of terrorism and so the failure to prevent terrorist financing can have particularly serious consequences for society as a whole. Financial Crime also includes tax evasion, an illegal activity in which a person or an entity deliberately avoids paying a tax liability, and bribery and corruption.

To combat this activity, an alliance of the world's governments cooperates on initiatives to counter ML/FT/PF. The compliance of each nation is monitored and those that fail to cooperate may be subject to international sanction.

The IOM first standalone Terrorist Financing National Risk Assessment (TF NRA) was released in July 2025 and provides a focused analysis of terrorist financing risks relevant to the IOM. May 2025 the IOM also published a NRAS outlining the Island's stance on acceptable levels of risk. License holders offering Network services are expected to be familiar with the findings of these documents and incorporate them into their risk assessments and AML frameworks.

Key Messages

Key Messages

- One of the GSC's primary objectives is to keep the gambling industry crime free;
- Licence Holders offering network services must stay alert for the possibility that their services and products could be used to facilitate financial crime;
- Financial crime includes ML, FT, PF, Bribery and Corruption and Tax Evasion; and
- Definitions pertaining to, and the offences of, ML, FT and PF in the IOM context are found within POCA, ATCA and TOCFRA.

3.1 Licence Holder's Role in Combatting Crime – Network Services

Schedule 4 of the Proceeds of Crime Act 2008 (known as the Business in the Regulated Sector Order) outlines that the Code applies to businesses conducting online gambling within the meaning of the Online Gambling Regulation Act 2001 (OGRA), ensuring that appropriate controls are in place to identify and manage risks related to money laundering and the financing of terrorism. While the application of the Code varies depending on the nature of the licence holder's activities, licence holders are expected to maintain effective oversight of their operations and ensure that AML obligations are met across their network.

All licence holders may be held liable where they fail to report knowledge or suspicion of criminal conduct. The GSC expects all Operators to uphold the reputation of the sector and the Isle of Man by complying with the conditions of their licence and acting with integrity. It is therefore essential that Operators with network permission understand how gambling services delivered through network arrangements may be exploited for criminal purposes and take steps to mitigate those risks.

Examples of potential typologies relevant to network models are provided at the end of this document.

3.2 Expectations

By seeking to be licensed, the Operator is committing to a high standard of governance, integrity, and regulatory oversight. OGRA Licence Holders with Network Permissions are subject to the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019 and specific AML derived OGRA licence conditions. While the practical application of certain provisions may vary depending on the nature of the services provided, all relevant requirements must be understood, assessed, and appropriately implemented. The relevant Code requirements are outlined in the self-assessment matrix issued by the GSC Inspectorate.

Maintaining a framework to assist in the prevention and detection of ML/FT/PF will assist in maintaining the reputation of licence holders, the licensing framework, the sector and ultimately the jurisdiction for the benefit of all.

Consequently, the GSC focuses in this guidance on the its expectations regarding areas of the framework that Licence Holders with network permissions should have in place. This guidance should be used to supplement the full guidance provided in AML Guidance for Gambling Operators. This guidance focusses on—

- Risk Based Approach;
- AML Staff;
- Suspicious Activity Reporting;
- AML Training; and
- AML Compliance Culture.

This guidance will also touch on customer due diligence, enhanced due diligence and monitoring measures as they relate to relevant business partners such as network partners and controls in place that align with specific licence conditions for network permissions. Please note this guidance relates to the treatment of activity conducted under L8 licence permission Network Services and other guidance should be consulted for other activity.

Network Permission Holders are free to implement further controls that suit their business and more information on the areas can be found further on in this guidance. The GSC will inspect and test against the controls outlined in this guidance and where referenced licence holders are encouraged to consult the relevant sections of the AML Guidance for more detailed information and best practice.

Red Flag Indicators

As outlined in the TF NRA, network activity although not business to customer gambling, may be deemed to be higher risk for terrorist financing due to the interaction with customers of online casino business known as Network Partners. In considering relationships with third parties that act as casinos, a licence holder should have consideration to its assessment of risk and that of any national risk appetite and have commensurate controls in place to mitigate such risks. Whilst not exhaustive, please see below a list of possible red flag indicators for ML/FT/PF:

- Business partners that: -
  - Are unwilling to provide due diligence (or enhanced due diligence);
  - Are based within a jurisdiction with known poor AML/CFT controls;
  - Have customers / target jurisdictions posing geographical risk such as that noted in the NRAS or those neighbouring or connected to conflict zones;
  - Have overly complex structures;
  - Involve nominee shareholders;
  - Change ownership on corporate structures without rationale (could be a way to avoid imminent financial sanctions);
- Source of funds/wealth from a higher risk jurisdiction (see the IOM Department of Home Affairs jurisdiction list that can be found here);
- Discrepancies in source of funds (for e.g. invoice payments);
- Unexplained third-party payments;
- Use of correspondent banks for payments through jurisdictions with poor AML standards or no direct relationship with respondent's customer's customer;
- Business owners or controllers who are or may be nationals or dual citizens of proliferating states; and
- Use of crypto currencies for payments – further information can be found on the AML Guidance page.

When there are possible red flag indicators then it is important that further checks are carried out and documented, and where necessary appropriate reporting takes place. More information can be found in the AML Guidance on best practice in relation to the importance of Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring all of which can be utilised when forming business relationships with third parties.

Key Messages

Key Messages

- Network activity involving third party casinos may present elevated TF risk, especially where customer interaction occurs, and risk assessments and controls should reflect this;
- Red flags include opaque ownership structures, reluctance to provide due diligence, and links to high-risk jurisdictions, all of which warrant enhanced scrutiny;
- Unusual payment behaviours, such as unexplained third-party transactions or use of correspondent banks, or crypto payments, may signal ML/TF/PF concerns; and
- Where red flags are identified, further checks and documented actions are essential, including potential reporting - refer to AML Guidance for best practice.

4.0 Risk Based Approach

4.1 Risk Assessment

It is important to understand the risks within a business to put in policies and procedures to mitigate risk and establish appropriate internal controls.

Under the Gambling AML Code 2019 OGRA Licence Holders with Network Permissions must carry out and document an AML Risk Assessment of their own business that must take into consideration the following—

- The vulnerabilities of products, goods or services to ML/FT/PF abuse;
- The jurisdictional risks when forming third party relationships[3;]
- The level of due diligence that should be undertaken when forming contractual relationships;
- What further checks should be carried out on third parties where potential risk has been identified, such as adverse media, sanctions check etc; and
- Assessment of technological developments for vulnerability to ML/FT/PF use.

In addition, the risk assessment should include a consideration of those risks posed by third parties such as Network Partners to ensure appropriate risk-based controls. Any assessment should take into consideration the factors that may deem third party business partners as higher risk. These include –

- Unregulated gambling activity, which dependant on the jurisdictions involved, may link to various criminal ML typologies which are described in UNODC reports
- Connections to, flow of funds from or customers located in jurisdictions identified as higher risk. They may be identified as higher risk by designation through the DHA lists, the IOM's NRAS or other reports such as the UNODC for example.;
- Obfuscated beneficial ownership through complex structures or opaque arrangements;
- Beneficial owners or controllers who are higher risk such as Politically exposed persons, (PEPs), dual nationals associated with higher risk and/or sanctioned countries;
- Complex or less regulated payment systems;

- Unusual contractual arrangements or agreements with no clear plausible economic rationale;
- Operator or associated entities are subject of adverse media regarding precious regulatory failings and/or allegations of illegal gambling, fraud, hidden beneficial ownership or association with bad actors; and
- Frequent changes in ownership or control.

Any risk assessment should be regularly reviewed and contain risks specific to the business. For further guidance on conducting business risk assessments please see the AML Guidance.

Network Permission Holders should consider the findings of the Isle of Man's 2020 NRA in respect of network activity and updates including the 2025 TF NRA, which identified a medium-low overall risk of the Island being used as a conduit for terrorist financing, with the highest exposure in transit TF. This reinforces the importance of assessing jurisdictional and structural risks when forming network relationships and implementing AML controls.

Additional documents, such as the NRAS issued by the Isle of Man Government or the competent authorities such as GSC must also be given documented consideration within your business risk assessment.

4.2 Due Diligence and Monitoring

Network permission holders are required by licence conditions to ensure systems are in place to detect ML/TF/PF or fraudulent activity alongside systems to detect and protect the vulnerable, problem gambling, excluded players and underage gambling. In practice, this means having assurance frameworks in place that test and validate the adequacy of a partner's controls. In order to evidence compliance with the Operators specific licence conditions, it is recommended that the below is undertaken and documented to ensure effective measures are being operated: —

- Partner due diligence and onboarding checks;
- Ongoing monitoring / screenings for adverse media, regulatory warnings, PEPs and sanctions;
- Independent assurances for instance regulatory reports or third-party assessments around AML frameworks and controls;
- Understanding of frameworks and policies in how AML is conducted within the entity;
- Understanding of regulated status and if that regulation is aligned with international standards; and
- Means of testing and monitoring of frameworks to ensure they are sufficiently carried out.

Network Permission holders may engage with a variety of third parties to resell, purchase or supply products used by business to customer Operators, both in the Isle of Man and other jurisdictions. Gambling is defined both by FATF and under Europe's 4th Anti-Money Laundering Directive as higher risk for ML and FT and therefore subject to regulatory oversight. By interacting with business in a sector subject to higher risk it is important that all Network Permission Holders undertake steps to establish the integrity of any third parties and are alert to red flags.

It is important that the findings of the business risk assessment inform a policy of due diligence and monitoring of these business relationships especially where there is a direct customer interface such as agreements for the provision of network services.

Where a network partner is responsible for conducting customer due diligence, the Network Permission Holder must ensure that the partner meets the standards required under the Code. This includes confirming that the network partner operates in accordance with AML standards that are consistent with those expected in jurisdictions recognised as having equivalent measures. Before any activity takes place, the Network Permission Holder is required to ensure that contractual arrangements are in place confirming that full customer due diligence has been conducted and that the network partner will make the underlying documentation available immediately upon request. Further information on testing is given in section 5.2 of this guidance.

Steps around due diligence determinations should be documented and regularly reviewed, further information on best practice is contained in the AML Guidance, including a summary of requirements for customers that act by way of business or are legal persons. A non-exhaustive list of Red Flags is outlined in Section 3.3 above.

The 2025 TF NRA highlights the Isle of Man's exposure to transit risk. Network permission Holders should take this into account when conducting due diligence on network partners, particularly where cross-border arrangements or complex ownership structures are involved.

By fully understanding who a business is interacting with and monitoring that relationship for ML/FT/PF risks a Network Permission Holders will ensure that they play their part in demonstrating good governance and oversight, upholding their reputation and that of the sector and licensing regime and play a part in a global initiative to reduce financial crime and the harm it poses to society.

Key Messages

Key Messages

- Network permission holders should understand the risks associated with its business and controls should be in place to mitigate any risks identified;
- Consideration to relevant factors outlined in publicly available documents such as National Risk Assessment or the National Risk Appetite Statement should be made and documented;
- A business risk assessment must consider risks relevant to the business;
- Network permission holders should read the AML Guidance for best practice on carrying out a risk assessment;
- Business, third party and Technology Risk Assessments should be documented, regularly reviewed and updated; and
- Due diligence should be carried out on third parties, documented and regularly monitored and updated. It should be informed by the business risk assessment with clearly documented rationales as to the level of risk vs level of due diligence carried out.

5.0 Compliance Culture

5.1 Procedures and Controls

In addition to the general requirements outlined in Part 2 of the AML Guidance, licence holders offering network services should implement enhanced procedures and controls that reflect the complexity and risk profile of network arrangements. These should include:

- **Specific Risk Considerations and Training Requirements**
  OGRA licence holders with network permissions must assess the unique risks associated with network operations, including jurisdictional variances, customer onboarding practices, and transaction monitoring. Staff involved in compliance functions should receive tailored training that addresses these risks, including typologies relevant to networked gambling environments and red flags for suspicious activity;

- **Assessment of Network Partner AML Policies**
  Network permission holders should conduct a documented review of each network partner's AML/CFT policies and procedures to ensure alignment with Isle of Man standards. This includes verifying that partners have effective customer due diligence, ongoing monitoring, and suspicious activity reporting mechanisms in place;

- **Documenting and Reporting Concerns**
  Any concerns arising from the assessment of a network partner's compliance framework, such as gaps in policy, inconsistent application of controls, or failure to report suspicious activity, must be documented and escalated appropriately; and

- **Retrieval and Retention of Records**
  Where agreements between the Network Permission Holder and network partners include record access as a control or mitigation, Network Permission Holder should ensure that relevant records can be retrieved promptly upon request

5.2 Monitoring and Testing

In addition to the expectations set out in the general AML guidance, licence holders offering network services should consider whether further monitoring and testing measures are appropriate within the context of their specific arrangements. These are particularly relevant where network agreements include compliance related controls or mitigations.

Licence holders should carry out targeted reviews of network arrangements and AML controls in response to findings from National Risk Assessments. These reviews should help determine whether existing controls are still fit for purpose and whether any additional mitigation measures might be needed.

Key Messages

Key Messages

- Network permission holders should consider additional procedures and controls where these are relevant to their specific arrangements, in line with Part 2 of the AML/CFT guidance;
- Risk-based training and tailored oversight may be appropriate where network complexity introduces distinct AML/CFT risks; and
- Network permission holders should ensure that, where record access is part of the agreement, relevant records can be retrieved promptly upon request.

6.0 Summary

This guidance is for Network permission holders who have no other category on their licence in meeting their requirements under the code. Where other categories are held on an OGRA licence alongside network services the relevant [AML Guidance] should be referred to for a full overview of requirements.

While certain provisions may not be applicable in practice due to the nature of network services, Network Permission Holders must ensure that all relevant requirements are understood, assessed, and appropriately implemented.

By applying good practice in relation to ML/FT/PF risks, businesses can—

- Decrease the regulatory burden by ensuring compliance and avoiding enhanced supervision and remediation;
- Increase the positive reputation of the sector which in turn will grow business opportunities;
- Meet social responsibility goals by contributing to the safety of the community;
- Support global initiatives to reduce crime and terror; and
- Safeguard the business and employees against risk and employees and criminal; liability.

7.0 Further Resources

The GSC produces full guidance on our website for all licence holders.

In September 2016, the GSC established the IOM Online Gambling Money Laundering Reporting Officers Forum. This has since been re-branded as the AML Forum and the mailing list now includes AML Compliance Officers and Nominated Officers (as well as MLROs and DMLROs.

The forum typically meets twice a year and provides a mechanism for the sharing of AML news, typologies, best practices and discussion on policy change.

Although there is no obligation to attend, the GSC strongly encourages Operators to send a representative to the meetings. Persistent non-attendance could call into question the capacity of the Operator's AML function and reasons for non-engagement.

This document is not the only source of information on AML. Below is a list of hyperlinks to other useful resources.

FATF Home

Moneyval

Mutual Evaluation Report IOM 2016

IOM National Risk Assessment 2020

IOM National Risk Appetite Statement

GSC's AML/CFT Guidance Documents

IOM Government - FATF and MONEYVAL

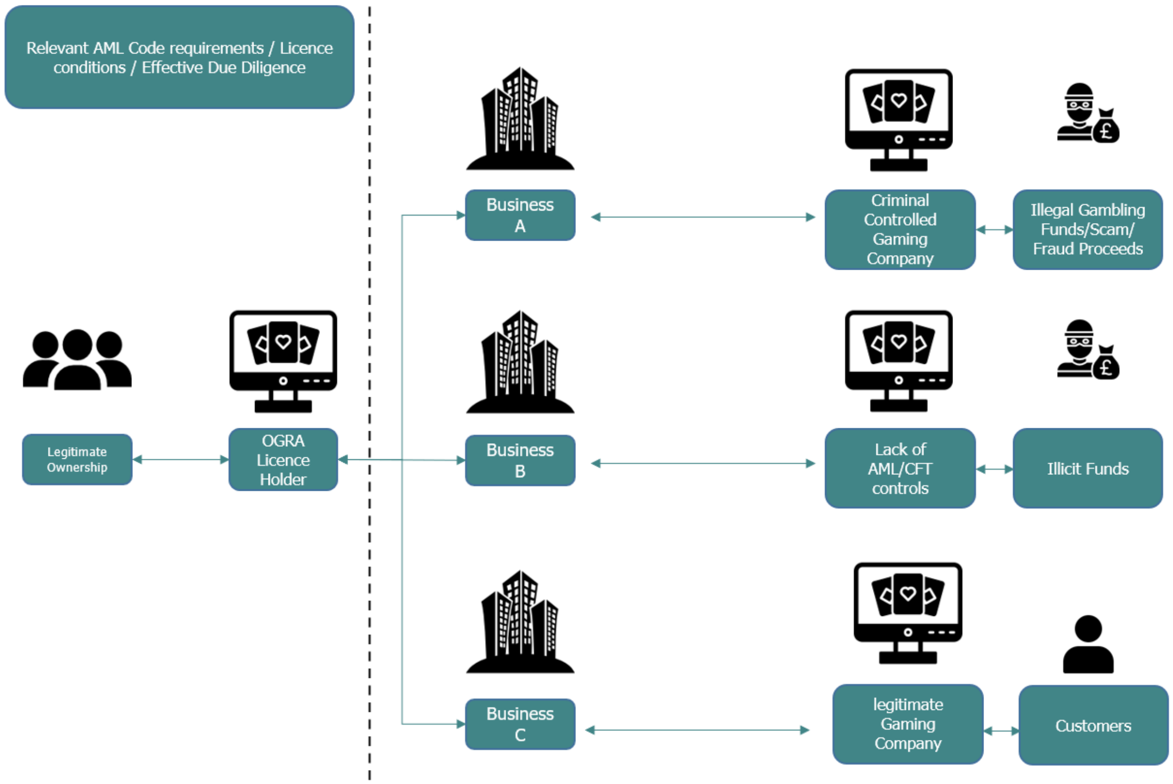
IOM - Sanctions and Export Control

IOM GSC - Home Page

FIU Typology Document for the Online Gambling Sector

Appendix One

Case Study 1 – Network Supply Model



In this example a legitimate owner operates a network supply model.

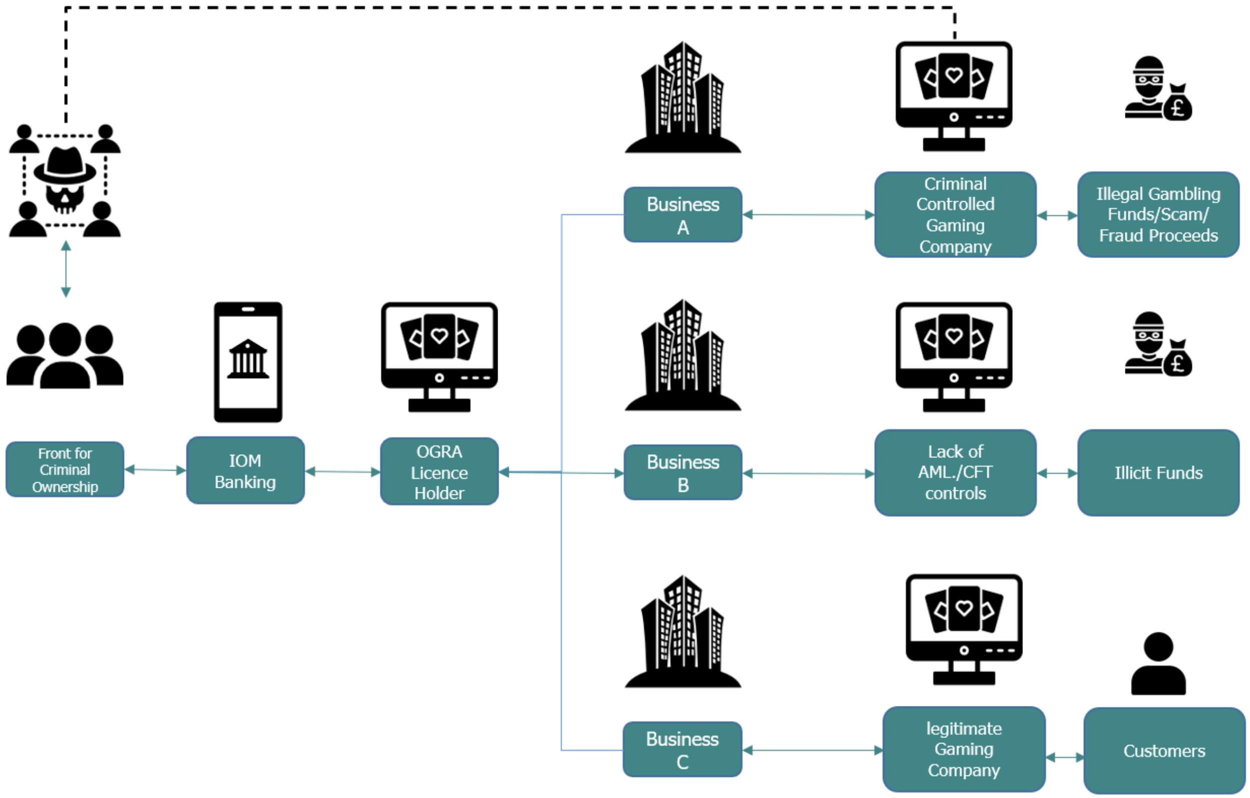
The OGRA Licence Holder has three network partners and has undertaken a minimal level of due diligence at the start of the relationship, but no screening or OSINT research has taken place. The Licence Holder has contractual obligations on their NWPs to operate AML/CFT controls for their customers however no monitoring mechanisms to test the NWPs controls are being operated. Failure to undertake a proportionate level of due diligence has allowed Business A to launder illegal funds on a platform provided by the licence holder. By not testing the AML/CFT controls operated by Business B both legitimate and illicit funds are accepted on a platform provided by the licence holder.

Red Flags may include–

- Unwillingness by NWPs to provide beneficial ownership documents / Source of Funds / Source of Wealth documents;
- Higher risk payment methods such as virtual assets;
- Unwillingness to provide customer sample information to test contractually required AML/CFT controls;
- A flow of funds / income that exceeds that forecasted;
- Third parties with limited online presence or unsophisticated websites.

Case Study 2 – Network Supply Model (OCG)

In this example the network supply model is fronted by an apparent legitimate owner(strawman) but is actually owned by an organised crime gang (OCG).



The OGRA Licence Holder has three network partners. No contractual agreements exist that require the NWPs to implement any AML/ CFT controls. Business A is owned by the same OCG and serves as a structure to launder proceeds of various frauds and scams disguised as an NWP fee to the Isle of Man Operator allowing access to the IOM banking system. Business A provides the Operator with 90% of its income. Business B, whilst being a legitimate gaming company, does not implement any AML/CFT controls on its customers accepting both legitimate and illicit funds.

Red Flags may include–

- Beneficial owners or business structures with links to countries listed in the Cabinet Office’s National Risk Appetite document;
- B2B relationships with online gambling Operators active in under regulated jurisdictions;
- B2B payments through money transmission services, particularly when doing so is commercially questionable (higher cost than bank-to-bank transfers);
- Business proposals or OGRA licence applications from people with a lack of experience in the industry and/or lack of technical expertise.