AML/CFT Guidance

For Software Suppliers

V1.4 – June 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 3
1.0 General 4
1.1 Abbreviations 4
1.2 About this Document 5
1.3 About the GSC 6
2.0 The Financial Action Task Force and MONEYVAL 8
2.1 The FATF's Recommendations and Methodology 8
2.2 MONEYVAL and its Evaluation of the Island 9
3.0 Financial Crime 10
3.1 Software Supplier's Role in Combatting Crime 11
3.2 Expectations 11
3.3 Red Flag Indicators 12
4.0 Risk Based Approach 13
4.1 Risk Assessment 13
4.2 Due Diligence 13
5.0 AML Staff 16
6.0 Training 17
6.1 Training & Procedures 17
6.2 Tipping Off 17
7.0 Suspicious Activity Reporting 18
7.1 Reporting 18
8.0 Summary 20
Appendix One 21

Version Control

This version of the guidance is effective from August 2024.

Version	Date published	Comments
0.1	N/A	Draft circulated to AML Forum and terrestrial gambling operators for comment 25/11/2020.
1.0	Dec 2020	AML/CFT guidance published for OGRA Software Suppliers
1.1	April 2024	Formatting and general updates in line with new branding and stakeholder consultation feedback
1.2	August 2024	Formatting review and update
1.3	March 2025	Formatting review and update
1.4	June 2025	Updated following publication of Isle of Man National Risk Appetite Statement on eGaming

1.0 General

1.1 Abbreviations

AML/CFT	Anti-money laundering and Countering the Financing of Terrorism (also incorporates countering proliferation financing)
AML Guidance	AML CFT Guidance for Gambling 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 2023
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
GSC	The Gambling Supervision Commission which includes the Board of Commissioners and the Inspectorate
IOM	Isle of Man
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
Nominated Officer	An employee nominated by a Software Supplier to be the point of contact for AML/CFT matters
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
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
Software Supplier	Any OGRA licence holder with the approved category L9a/L9b Software Supply and/or L9b Software Supply (Token-based)
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 GSC and contains guidance for Operators licensed under the Online Gambling Regulation Act 2001 (OGRA) approved for the supply of software only.

Software Suppliers are exempt from requirements set out under the Code in relation to AML/CFT.

The guidance seeks to provide best practice for businesses that have no obligations under the Code but could still face the risk of liability for a substantive ML and/or FT offence.

In order to protect the reputation of the sector and facilitate good business practice, Software Suppliers must comply with an additional licence condition outlined in Schedule 5 of their licence stating that the licensee shall disclose directly to the IOM FIU –

- Any knowledge or suspicion of ML under the Proceeds of Crime Act 2008 (POCA);
- Any knowledge or suspicion of terrorist financing under the Anti-Terrorism and Crime Act 2003 (ATCA);
- Information regarding unusual activity that may assist the IOM FIU in undertaking its functions under the Financial Intelligence Unit Act 2016.

AML/CFT guidance has been produced for OGRA licence holders who are obliged under the Code i.e. those that offer sports betting or casino products plus bookmakers and casinos. Whilst Software Suppliers are exempt from the requirements set out in the Code, Software Suppliers will find some useful information in the OGRA Guidance as a bridge between the Code and the FATF Recommendations. It can be found in the AML Guidance section of our website.

Throughout this document you will find AML/CFT guidance and key messages.

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 Commission.

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 Visit Procedures (which includes AML/CFT Supervision) which can be found on the General Supervision page - https://www.isleofmangsc.com/gambling/general-supervision/

Supervision is carried out using a risk-based approach, all licensed entities 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, customer risks
- 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 – A licence holder will be asked to provide pre-visit documentation which generally 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 licence holders will be required to fill in and return a self-assessment template to establish their AML framework in order to test the framework during the onsite portion of the Inspection. Self-assessment templates are provided upon licensing to allow licence holders time to familiarise themselves with the requirements fully and identify any issues prior to any inspection beginning. Where these have already been provided to the GSC an update will be requested.

- Onsite – The AML/CFT team will, accompanied by the lead general inspector for the licence holder, visit a licence holder's premises in person to look at the effectiveness of the mechanisms reported under the self-assessment and through the pre-visit documents. For Software Suppliers this will be in the form of a business meeting to discuss any points raised in the desk top review. 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 the AML/CFT team will request any further outstanding documents and issue a report covering both technical findings from the self-assessment and practical findings from the onsite. Following a draft report being issued the AML/CFT team will issue a final report at which point the Inspection is concluded.

Following supervision, 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 visited 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, these 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/CFT 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/CFT 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).

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

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, 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 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 vehicles 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 IOM. 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, in order to monitor progress in improving its AML/CFT regime.

The IOM Government, regulatory and law enforcement authorities have undertaken a considerable amount of work since the publication of the MER in 2016, in order 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 Island 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 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/CFT controls.

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

The IOM GSC is the regulator that supervises the IOM gambling sector's compliance with AML/CFT 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 in order 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.

Key Messages

Key Messages

- One of the GSC's objectives is to keep the gambling industry crime free.
- Software Suppliers 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.
- Definitions pertaining to, and the offences of, ML, FT and PF in the IOM context are found within POCA, ATCA and TOCFRA.

3.1 Software Supplier's Role in Combatting Crime

Schedule 4 of POCA outlines that the Code applies to businesses conducting online gambling within the definition of OGRA, ensuring that business have controls in place to identify ML/FT risks and deal with them accordingly. However, Schedule 4 does not apply where business is being carried out by a software supplier.

Any business could have liability where they have failed to report any suspicions or knowledge of an offence and as a licence holder, the GSC would expect any business to maintain the reputation of the sector and the island and comply fully with all licence conditions. It is therefore important to understand how legitimate businesses could be used for ML and FT.

Some examples are provided of potential typologies at Appendix One.

3.2 Expectations

By seeking to be licensed, Software Supplier businesses are demonstrating that they have a high level of integrity and have sought out oversight to provide industry wide assurance as to their high standards of governance and compliance.

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.

In order to do so the GSC outlines in this guidance a framework that licensed Software Suppliers should implement to ensure those controls are in place. This includes—

- Risk Based Approach
- AML Staff
- Suspicious Activity Reporting
- AML Training

Software Suppliers 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 supervise 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.

3.3 Red Flag Indicators

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 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 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);
- Use of correspondent banks for payments
- Business owners or controllers who are or may be nationals or dual citizens of proliferating states
- Use of crypto currencies – 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

- Software Suppliers should consider the findings of the National Risk Assessment, and any associated documents such as the National Risk Appetite Statement.
- Software Suppliers must understand how their business could be used for ML/FT/PF.
- Further checks should be made when there are possible red flag indicators.
- Software Suppliers should refer to the AML Guidance on the importance of Customer Due Diligence/Enhanced Due Diligence and ongoing monitoring and look to apply the principles to third party checks.

4.0 Risk Based Approach

4.1 Risk Assessment

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

It is recommended that Software Suppliers carry out and document an AML/CFT Risk Assessment of their own business that could 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 checks etc.
- Assessment of technological developments for vulnerability to ML/FT/PF use.

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.

Certain documents, such as the National Risk Appetite Statement issued by the Isle of Man Government or the competent authorities such as GSC may be applicable to your business and should be considered in your risk assessment.

4.2 Due Diligence

Software Suppliers do not engage in business to customer (B2C) gambling directly so are not required to carry out due diligence on end users of gambling products. However, they may engage with third parties to resell, purchase or supply products used by B2C gambling operators 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 TF and therefore subject to licensing and supervision. By interacting with the sector subject to higher risk it is important that licence 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 informs a policy of due diligence required where agreements for software supply are entered into. Key areas to look at include—

- Are those third parties based in a jurisdiction compliant with FATF recommendations?
- Is there any adverse media in relation to the third party that may imply illicit flow of funds, sanctions, PEP involvement, criminal activity etc?
- Are the beneficial owners of the business understood and due diligence carried out to establish the ownership and control including corporate due diligence?
- Is the relationship and due diligence subject to ongoing monitoring to make sure that it is up to date and that nothing has changed that could impact on the risk of doing business with the third parties?
- Any further area informed by business specific risks highlighted in the business risk assessment.

[3] Please see IOM DHA Jurisdiction list

Steps around due diligence determinations should be documented and regularly reviewed, further information on best practice is contained in the AML Guidance. A non-exhaustive list of Red Flags is outlined in Section 3.3 above.

By fully understanding who a business is interacting with and monitoring that relationship for ML/FT/PF risks a licence holder 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

- Software Suppliers 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.
- A business risk assessment must take into account risks relevant to the business
- Software Suppliers should read the AML Guidance for best practice on carrying out a risk assessment
- Risk assessments should be documented, regularly reviewed and updated.
- 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 AML Staff

5.1 Nominated AML/CFT Officer

Software Suppliers are required through Schedule 5(6) of licence conditions to nominate an individual to be the focal point for any ML and FT concerns, fulfil any reporting requirements, consider staff training and undertake risk assessments. It is important that the Nominated Officer meets the following requirements—

- Competent – has knowledge and understanding, ideally with experience of AML/CFT and reporting
- Sufficiently resourced and supported – can implement appropriate internal control mechanisms and has sufficient oversight and time to carry out any duties
- Seniority or sufficient access – the Nominated Officer must be able to make and implement recommendations in line with the business risk assessment.

The Nominated Officer is expected to be able to demonstrate understanding of suspicious activity reporting requirements and ML/FT/PF risks faced by their business.

5.2 Role

The Role of the Nominated Officer is to act as the main point of contact for reporting internally and externally, ensuring that reporting is carried out appropriately, within a reasonable timeframe and decision around reporting documented.

The Nominated Officer should also to a greater or lesser extent based on the size and risk profile of the business—

- Ensure staff are aware of their responsibilities
- Provide input into training, policies and procedures
- Provide input into business risk assessments
- Monitor and test the effectiveness of the AML/CFT framework
- Be free of commercial responsibilities

Key Messages

Key Messages

- The Nominated Officer should be competent, have sufficient resources and be sufficiently senior within the business
- The Nominated Officer should have a thorough understanding of the ML/FT/PF risks faced by their business and provide input into the AML/CFT framework

6.0 Training

6.1 Training & Procedures

All staff within a business can report suspicions or knowledge and it is essential that all staff including at a senior level understand what ML/FT/PF and sanction breaches could look like, how to report and who to report to within a business.

It is important to document any training to evidence that it is relevant, kept up to date and covers the requirements of the Isle of Man as a jurisdiction along with how internal and external reports can be made. Training should be refreshed at least annually and should also include an overview of tipping off alongside red flags and any specific risks highlighted in the business risk assessment. Further information on best practice in training can be found in the AML Guidance.

Reports of suspicious or unusual activity should be made in a timely manner, documented and any decisions around externalising reports clearly recorded. Documented procedures should be in place to inform staff of how to make a disclosure and to inform how decisions to externally disclose are made and what timeframes these should be made within to be reasonable. It is recommended that licence holders have a whistleblowing policy or mechanism in place where concerns of staff can be reported and appropriately dealt with. This should include information about how to contact the GSC with any concerns.

6.2 Tipping Off

All businesses should put in place procedures to ensure that the subject of any report or suspicion is not alerted to the suspicion (this is known as tipping off). Although Software Suppliers may not be held liable under POCA for a tipping off offence due to their status, they could still be held accountable for prejudicing an investigation if tipping off were to occur.

Key Messages

Key Messages

- All staff should undergo regular training to recognise ML/FT/PF and sanction breaches
- Operators must have procedures in place to ensure that all staff know how to report and who to report to if they have suspicion or knowledge of ML/FT/PF and sanction breaches. A process for whistleblowing should be in place and documented.
- All staff must be made aware of what "tipping off" means and have clear procedures in place to make sure it they do not prejudice an investigation.

7.0 Suspicious Activity Reporting

7.1 Reporting

Through its licence conditions, Software Suppliers are required to report:

- Any knowledge or suspicion of ML under POCA;
- Any knowledge or suspicion of FT under ATCA; and
- Any other information pertaining to unusual activity that may assist the IOM FIU in undertaking its functions under Section 24 of Financial Intelligence Unit Act 2016.

Software Suppliers are also required to report;

- Any knowledge or suspicion of PF under TOCFRA; and
- Any potential or actual sanctions breaches.

Best practice for reporting would be to have a policy and procedure in place to ensure that any reports are made in a timely manner and appropriately documented. Such reports must be made directly to the IOM Financial Intelligence Unit. For further information on reporting, please find a link to the FIU's webpage here.

The FIU's designated reporting platform is "THEMIS" and THEMIS can be accessed here. It is recommended that Software Suppliers register on THEMIS to avoid any unnecessary delays in reporting. Reports should always be made within a reasonable time frame.

THEMIS is also used by the FIU to communicate advisory notices and other important information, so it is recommended that at least one staff member (the Nominated Officer) is registered on THEMIS at all times to avoid any delays in reporting.

A THEMIS user guide is available via the FIU's website https://www.fiu.im/themis-guide/.

The FIU have published guidance and good practice documents for the submission of SARs – these can be found here.

Under Section 141 of POCA, a person commits an offence by acquiring criminal property, using criminal property or having possession of criminal property. It is also an offence under section 139 of POCA to conceal, disguise, convert, transfer or remove criminal property. This means that if a Software Supplier were to accept payment from a company where they suspect criminality or reasonably should have suspected then they themselves would be committing a ML offence.

It should be noted that ML is not only confined to transactions involving money but can also include any benefit of crime including assets. Businesses would have a defence against any liability where knowledge or suspicion of a crime had been reported appropriately and consent obtained for any transaction to continue.

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at such people and things in a particular country or territory, or some organisation or element within them.

All persons in business or a profession in the Island, including Software Suppliers, must check whether they maintain any account, or otherwise hold or control funds or economic resources, for individuals or entities named in the published lists having effect in the Island and, if so, they should freeze the account, funds or economic resources and report their findings. Further guidance on sanctions breaches can be found here.

Any business could have a liability where they have failed to report any suspicions or knowledge of an offence and as a licence holder, the GSC would expect any business to maintain the reputation of the sector and the island and comply fully with all licence conditions.

Key Messages

Key Messages

- Software Suppliers have an obligation to report knowledge and suspicion of ML, FT and PF and suspected or actual breaches of sanctions
- Software Suppliers are also required to report activity that may assist the FIU in undertaking its functions
- Reporting should be made to the FIU directly and within a reasonable time frame
- It is recommended that Software Suppliers register on THEMIS and have reporting policies and procedures in place.

8.0 Summary

This guidance is for Software Suppliers who have no other category on their licence. Where other categories are held on an OGRA licence alongside software supply the AML Guidance should be referred to for a full overview of requirements.

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;
- Safeguard the business and employees against risk and employees and criminal; liability.

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/CFT 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/CFT 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/CFT function and reasons for non-engagement.

This document is not the only source of information on AML/CFT. 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 – Money Laundering

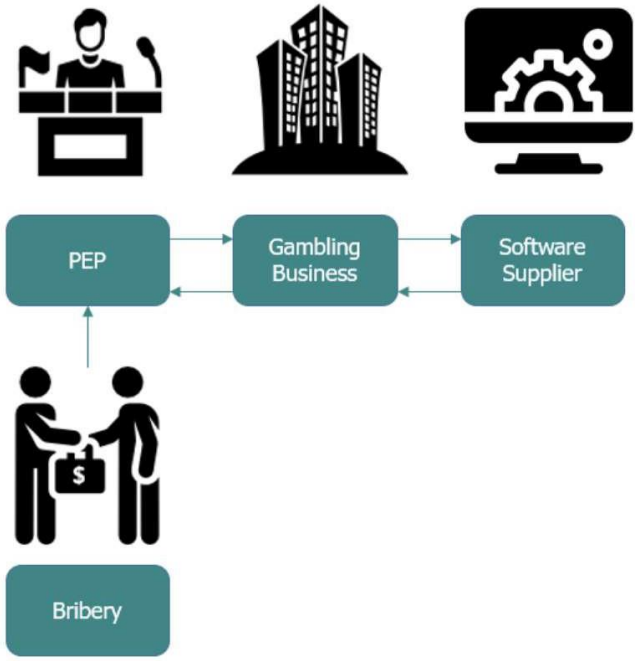
In this example, illicit funds are provided to a professional money launderer who utilises a gambling business to conceal and layer the proceeds of crime, or a criminal owner appoints a nominee to run a gambling business in their name using the proceeds of crime to fund the business. In order to further create a legitimate business cover in each case they engage with a software supplier directly.

Red flags may be –

- An unwillingness to provide beneficial ownership details or information
- A lack of market presence incongruous with the profile presented of the business
- Invoice payments being made by unrelated third parties, adverse media around the beneficial owner
- A lack of understanding of the gambling industry
- Limited activity that is incongruous with normal business
- Complex structuring of companies or ownership with no clear rationale
- Higher risk payment methods such as cryptocurrency which may sit outside of the normal financial services.

Case Study 2 - Tax Evasion/Bribery

In this example, one of the beneficial owners of a group that includes both gambling businesses and a licensed software supplier is an active politician within their jurisdiction and is therefore considered a PEP. A staff member within the software supplier notices that recent recharges through the software company have increased however the financial flow doesn't link to the expected revenue from games content utilised by the group company. After raising this internally they note a reluctance to investigate. The staff members utilise the whistleblowing mechanism to raise their concerns internally however there is still a reluctance to investigate, so they whistle blow directly to the regulator.



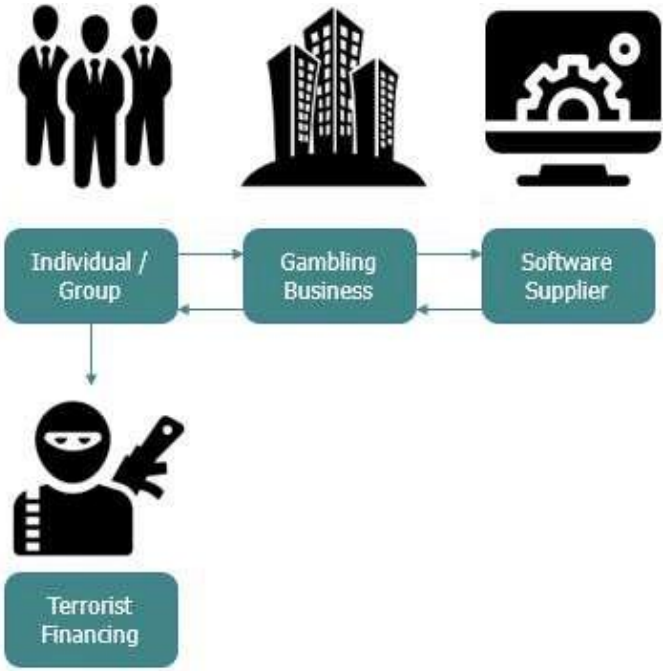
Red flags may be—

- PEP matches or PEP by association matches when conducting screening and open-source searches on related parties
- Adverse media relating to current affairs in the jurisdiction or around the individual such as political unrest, bribery and corruption or tax evasion
- Complex corporate structures moving flows of funds from less regulated jurisdictions with poor AML controls
- Intergroup payments or recharges that seem unusual, or are at odds with expectations
- Irregular intergroup contractual terms.

Case Study 3 - Terrorist Financing

In this example, an individual or group of beneficial owners have set up an online gambling operator which has engaged with a software supplier for the provision of a website and back-office platform.

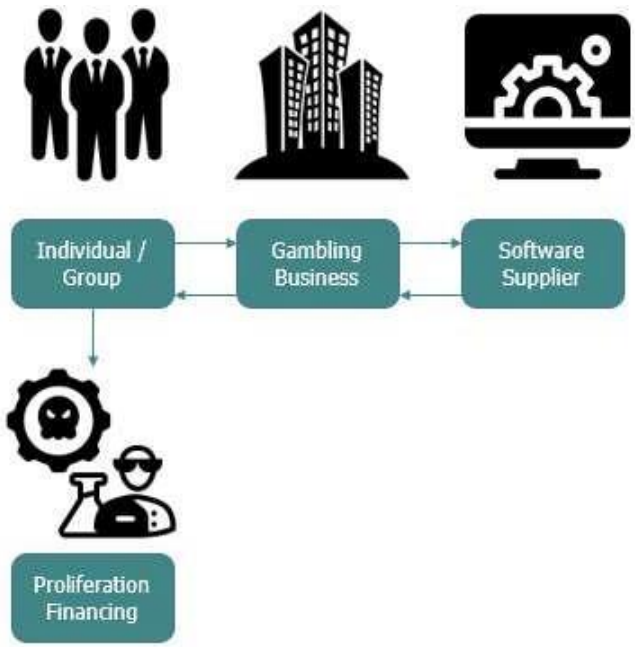
The profit generated by the operator is fed back to the shareholders who then decide to provide these funds to a Non-Profit Organisation that funds training and equipment for a terrorist group. It is important to remember that a predicate offence is not necessarily required in order to finance terrorism unlike with ML. Funds derived from legitimate business activity can be used for FT.



Red flags may include—

- Complicated payment or invoicing arrangements that may sit outside of the regulated financial system or come via third parties
- Resistance in providing information on beneficial ownership
- Any open-source media linking beneficial owners or group companies to any business operating in countries that are deemed to have with weak measures in combatting terrorist financing or close links with flagged jurisdictions
- Links to sanctioned countries, entities or individuals

Case Study 4 - Proliferation Financing



In this example, an individual or a group of beneficial owners has set up an online gambling operator which has engaged with a software supplier for the provision of RNG slot games. The shareholder's other interests include the manufacture of technology used for navigation and guidance of drones. The software supply company in doing some third-party due diligence notes some adverse media in relation to potential links between the shareholders' other interests and supply of missile guidance systems and drones to DPRK.

As with FT, it is important to remember that a predicate offence is not necessarily required in order to finance proliferation unlike with ML. Funds derived from legitimate business activity can be used for PF.

Red flags to be aware of include—

- The use of complicated payment or invoicing structures
- Resistance in providing information on beneficial owners
- Any open-source media linking shareholders to any business operating in jurisdictions of proliferation concern such as the Democratic People's Republic of Korea (DPRK) or Iran
- Links to sanctioned countries, entities or individuals, payments originating from non-regulated financial institutions or jurisdictions with weak financial safeguards.
- Links to industries known to be at risk of producing dual use goods or associated with proliferation, i.e. sensors, lasers, navigation and avionics, aerospace and propulsion, electronics, satellites, chemicals etc.