GSC GAMBLING

AML/CFT Guidance for Gambling Operators

V1.1 (April 2024)

Contents

Version Control

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	Replaces the 2015 Guidance and 2018 Supplementary guidance; Based on the 2019 Code For online gambling (excl. software supply only), casinos, bookmakers
1.1	April 2024	Industry and stakeholder review and new branded template.

Introduction

Abbreviations

AML	Anti-Money Laundering
ATCA	Anti-Terrorism and Crime Act 2003
B2B	Business to business
BRA	Business Risk Assessment
CDD	Customer due diligence
CFT	Countering the financing of terrorism
Code	The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019
CPF	Countering proliferation financing
CRA	Customer Risk Assessment
DHA	Isle of Man Department for Home Affairs
DNFBP	Designated non-financial business or professional
DPO	Data Protection Officer
EDD	Enhanced due diligence
FATF	The Financial Action Task Force
FIU	Isle of Man Financial Intelligence Unit
FSRB	FATF-style regional body
FT/TF	Financing of terrorism/terrorist financing
GDPR	General Data Protection Regulations
GSC	The Gambling Supervision Commission which includes the Board of Commissioners and the Inspectorate
IOM	Isle of Man
IOMFSA	Isle of Man Financial Services Authority
ML	Money laundering
MLRO	Money Laundering Reporting Officer
MONEYVAL	The Council of Europe's Committee of AML/CFT Experts, an FSRB
MVTS	Money/value transmission service
NRA	National Risk Assessment
OFAC	US Office of Foreign Asset Control
PEP	Politically exposed person
POCA	Proceeds of Crime Act 2008

PF	Proliferation Financing
SOF	Source of funds
SOW	Source of wealth
TRA	Technology Risk Assessment

About this Document

This document has been prepared by the Gambling Supervision Commission and contains all of the guidance necessary to operate a framework for compliance with the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019.

The guidance seeks to directly connect the Code and guidance issued by the GSC with the Financial Action Task Force Recommendations. For this reason, FATF's Recommendations or observations are noted in each section of the document.

In compiling this document, the GSC has also recognised anti-money laundering, countering the financing of terrorism and proliferation financing literature from MONEYVAL and the Island's National Risk Assessment https://www.gov.im/about-the-government/departments/cabinet-office/national-risk-assessment/.

Throughout this document you will find details on AML/CFT/CPF guidance and policy, FATF recommendations and Code requirements.

The contents of this guidance should not be construed as legal advice.

Useful Links

This document is not the only source of information on AML, CFT and CPF. Other sources include

- Isle of Man Gambling Supervision Commission - Home Page;
- Isle of Man Gambling Supervision Commission - Legislation;
- Isle of Man Gambling Supervision Commission - Anti-Money Laundering Guidance;
- FATF;
- Isle of Man Government - FATF and MONEYVAL; and
- Isle of Man Government - Sanctions and Export Control.

About the GSC

The GSC is responsible for licensing and regulatory oversight of the gambling sector including compliance with legislation such as various gambling acts and where applicable the Code. The GSC is an independent statutory board of Tynwald and comprises the Inspectorate and the board of the Commission. The GSC refers to those under regulatory scrutiny as "operators" throughout this guidance.

The board of the Commission consists of independent members drawn from various professions and backgrounds. The board of the Commission conduct monthly hearings into all matters that pertain to gambling in the IOM and are supported by their Inspectorate.

In 2023 the Commission has made AML an institutional priority for the GSC – this was announced to the industry during the 20th AML Forum in January 2024.

The Inspectorate is managed by the Chief Executive of the GSC. The GSC supervises AML compliance through AML inspections, which include a technical assessment (self-assessment) and practical assessment including an onsite inspection. The GSC has produced guidance for an AML inspection which can be found at https://www.isleofmangsc.com/gambling/aml-cft-compliance-inspections/.

The Commission also participates in national initiatives to continually assess the risk of

ML/FT/PF within the sector as well as evaluation exercises, conducted by external teams of assessors, which check the IOM's national commitment and performance against international standards.

The GSC is available 9:00am to 5:00pm Monday to Friday and can be contacted via phone on +44 (0)1624 694331, via e-mail on gscamlinspections@gov.im or at the postal address below—

Ground Floor,
St. George's Court,
Myrtle Street,
Douglas,
Isle of Man,
IM1 1ED

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

The Financial Action Task Force

FATF leads global action against ML, FT and PF. They conduct research into how money is laundered and terrorism is funded, promote global standards to mitigate the risks, and assess whether countries are taking effective action. As an inter-governmental body they set international standards that aim to prevent illegal activity and the harm it causes to society. As a policy-making body, the FATF works to bring about national legislative and regulatory reforms in these areas.

The FATF Recommendations are also often referred to as the FATF standards, for AML, CFT and CPF 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 and a so called FSRB 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, FT and PF; 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.

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 these set of international standards states that countries should identify, assess and understand the risks of ML, FT and PF 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 ML, FT, and PF are the:

- Anti-Terrorism and Crime Act 2003;
- Proceeds of Crime Act 2008;
- Terrorism and Other Crimes Financial Restrictions Act 2014 (TOCFRA); and
- Financial Intelligence Unit Act 2016 (FIU Act).

The AML Code is made under Sections 157 of POCA and 68 of TOCFRA and give direction to regulated businesses in relation to the prevention and handling of ML, FT and PF.

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/FT/PF 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 that 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/CPF 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 and PF. 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 IOM amongst a select group of leading nations in the world for technical compliance in AML measures.

More information can be found at the Cabinet Office's AML/CFT Policy webpage https://www.gov.im/about-the-government/departments/cabinet-office/fatf-and-moneyval/.

AML/CFT Legislation Applicable to Operators

The FATF Recommendations apply to Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs) which includes casinos, bookmakers and online casinos. The FATF Recommendations, unlike the European Union (EU) Money Laundering Directives, do not currently apply to other forms of gambling.

Online gambling operators (excluding those that only provide software supply), bookmakers and casinos all fall under the remit of the Code. The majority of the Code requirements apply equally to each type of operator however there are slight differences in respect of customer due diligence.

The Code seeks to ensure compliance with the following AML/CFT legislation as defined by the Code:

- Section 7 to 11 and 14 of ATCA;
- Part 3 of POCA;
- Parts 2 to 4 of the Terrorism and Other Crime (Financial Restrictions) Act 2014; and
- The Code.

Operators are also obliged to comply with financial sanctions which have effect on the Island. The IOM Customs and Excise Division is responsible for the implementation of United Nations (UN) and United Kingdom (UK) financial and economic sanctions and export and trade licensing controls in the IOM. More information can be found at https://www.gov.im/categories/tax-vat-and-your-money/sanctions-and-export-control/.

For consolidated versions of current Primary and Secondary legislation please visit https://legislation.gov.im/cms/.

Financial Crime

One of the GSC's regulatory objectives is the prevention of gambling from being used to support crime. 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.

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

What is Money Laundering?

ML is the processing of criminal proceeds to disguise their illegal origin. Criminals do this by disguising the source, changing the form, or moving the funds to a place where they are less likely to attract attention.

Criminally derived property can be laundered by using a wide range of methods involving gambling and traditionally the ML process comprises of three stages:

Placement	Layering	Integration
Where criminal property is placed into the financial system	By using a number of complex transactions, the criminal ownership of the criminal property is hidden	Where the laundered criminal property is reintroduced into the legitimate economy

This is the "traditional" ML model, there are more "modern" methods of ML now beginning to emerge. Rather than getting caught up in trying to establish whether the activity relates to a particular phase of the traditional model, the relevant person should ask themselves – "Do I know or have reasonable grounds to suspect that the property in question is criminal property?"

What is Terrorist Financing?

TF provides funds for terrorist activity. It may involve funds raised from legitimate sources such as personal donations and profits from businesses and charitable organisations, as well as from criminal sources such as drug trafficking, fraud, smuggling of weapons and other goods, kidnapping and extortion.

TF will often come from legitimate sources of funds but there will be an attempt to disguise the destination of these funds (in the same way that a money launderer will attempt to disguise the source of proceeds of crime).

What is Proliferation?

Proliferation is defined by FATF following UN Security Council Resolution 1540 as "the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations". It includes technology, goods, software, services or expertise.

What is Proliferation Financing?

PF is defined by FATF as referring to "the act of providing funds or financial services that are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

PF can also be —

(a) Terrorism financing - where it provides financial support to terrorist organisations that would want to acquire and/or use a Weapon of Mass Destruction (WMD); or

(b) Financing from a state, or a state-controlled or state-sponsored entity with the aim of providing a state with a WMD, or to enhance, improve or replace and existing one.

More information on Proliferation or PF can be found in the IOM Customs & Excise Notice 1009 MAN, Proliferation and Proliferation Financing Risk.

The Role of Operators in Combatting Crime

Operators do not have access to databases of intelligence relating to criminals and terrorists but do have an opportunity to observe the day-to-day activities of their customers and business partners.

Law enforcement does not have unlimited resource to monitor every transaction performed in the financial framework by every individual but does have access to privileged information relating to known or suspected criminals and terrorists.

The FATF framework is designed to match the respective strengths of each party to achieve two key effects:

Strategically, as a result of increased detection and prosecution success, the framework raises the cost of ML, FT and PF and subsequently reduces the profitability of crime;

Operationally, it-

- Disrupts criminal operations by freezing laundered funds;
- Slows down the rate at which laundering can occur by setting caps;
- Puts assets beyond the use of criminals through seizure;
- Improves the quality of evidence available for prosecutions; and
- Creates tension and schisms between criminal/terrorist financiers and the operational/tactical arms of their organisations leading to weaknesses that can be exploited by the authorities.

In the absence of being able to positively determine whether a customer is a person of interest to the authorities, it may be that a proportion of suspicious activity reports (SARs) will result in no further action. It is important to note that the effort to report suspicious activity must not be considered wasted. The submission of useful and detailed information allows the authorities to cross-refer reported individuals with intelligence databases and when matches do occur, the authorities gain valuable opportunities to exploit the information.

Operators can assist the authorities by ensuring that the reports they submit and the records they keep refer to credible suspicions and are detailed enough to allow the authorities to efficiently bracket individuals on their databases and to establish audit trails of the suspects' transactions.

The GSC's AML Forum

In September 2016, the GSC established the IOM Online Gambling MLRO Forum. This has since been re-branded as the AML Forum and the mailing list now includes AML/CFT Compliance Officers and Nominated AML/CFT Compliance Officers (for software only operators) as well as MLROs and Deputy MLROs (DMLROs).

The forum typically meets twice a year and provides a mechanism for the sharing of AML/CFT/CPF news, typologies, best practices and discussion on policy change. It also provides a forum to provide AML supervision feedback with the aim of having a positive impact on compliance.

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/CPF function and reasons for non-engagement.

Guest speakers are arranged around topics requested by Forum members and surveys take place to garner suggestions for subjects of interest.

Key Messages

Introduction - Key Messages

- ✓ GSC guidance has been prepared to assist operators in operating a framework for compliance under the Code.
- ✓ The Guidance connects the Code and FATF Recommendations.
- ✓ One of the objectives of the GSC is to keep the gambling industry crime free and to do this, the IOM cooperates on initiatives to combat ML, FT and PF. Failure to do so may lead to an international sanction.
- ✓ The IOM's AML/CFT/CPF framework of legislation and guidance is drafted to the FATF AML/CFT Standards.
- ✓ Operators play a key role in combatting ML, FT and PF by reporting suspicions and keeping detailed records so that the authorities can efficiently bracket individuals to establish audit trails of suspects.
- ✓ Operators are strongly encouraged to attend the GSC's AML Forums where they can keep up with AML/CFT/CPF news, typologies, best practices and discussion on policy change.

Part 1: Interpretation

1.1 Terrestrial Operators

Paragraph 3 of the Code (Interpretation) provides a long list of defined terms used in the Code and spans pages 3-10.

This part of the guidance highlights 3 concepts drawn from the Code interpretations that are key to understanding how the Code applies to bookmakers and casinos (collectively known as terrestrial operators).

GSC Guidance and Policy

1 - "Customers"

The term customer is used throughout the Code and the guidance for ease and consistency rather than punter, player, gamer, gambler, participant, etc. Customers include those that attempt to carry out a transaction or start a customer relationship.

2 - "Ongoing customer relationships" and "occasional transactions"

All customer activity is split in two; ongoing customer relationships and occasional transactions. These two terms are particularly important as the requirements for CDD, etc. vary depending on this distinction-

An **ongoing customer relationship** is where an account is opened for a customer.

An **occasional transaction** is a single transaction or multiple linked transactions that take place where no account is opened.

For bookmakers, all activity is considered an occasional transaction therefore, requirements relating to ongoing customer relationships do not apply.

For casinos, both may apply because they can have members/account holders and walk-in customers that do not hold membership/an account.

3 - "Thresholds"

Ongoing customer relationships and occasional transactions each have an applicable "threshold"-

The **qualifying transaction threshold** applies to ongoing customer relationships and is EUR 3,000 (or equivalent) in 30 days.

The **occasional transaction threshold** is EUR 3,000 (or equivalent) in a single or several linked transactions.

For clarity, both thresholds are EUR 3,000 in wagers or EUR 3,000 in collected winnings.

Occasional transactions include-

(*a) the wagering of a stake, including*

(i) the purchase from, or exchange with, the casino of tokens for use in gambling at the casino; and

(ii) payment for use of gaming machines;

(b) the collection of winnings, and need not take account of winnings from a previous transaction which had not been collected from the operator but are being re-used in the transaction in question.

The table below summarises Code requirements that apply all the time, for customers that exceed the occasional transaction threshold or for customers that exceed the qualifying transaction threshold:

Requirement	Occasional transactions (bookmakers & casino walk-ins)		Ongoing customer relationships (account holders)	
	Applies all the time	Applies to customers over the occasional transaction threshold	Applies all the time	Applies to customers over the qualifying transaction threshold
Procedures and controls (paragraph 4) • For all things required by the Code • Risk based & approved by management • Register on Themis	✓		✓	
Business risk assessment (paragraph 6) • Regularly reviewed, updated and recorded • Cover all of the listed risk factors	✓		✓	

Technology risk assessment (paragraph 7) • Regularly reviewed, updated and recorded • Before implementation or development of new products, business practices, delivery methods and technology • Cover all of the listed risk factors	✓		✓	
Customer risk assessment (paragraph 8) • Regularly reviewed, updated and recorded • Cover all of the listed risk factors • Adhere to the "may be" and "must be" high risk factors		✓	✓	
Identify customer and source of funds (not source of wealth) (paragraph 10)		✓	✓	
Verify customer's identity (paragraph 11)		✓		✓
Periodic check that customer's identity and verification are satisfactory (paragraph 12)		✓	✓	
Check if customer is a PEP and, if so, identify source of wealth and get senior management approval		✓	✓	
Carry out EDD on high risk customers, including source of wealth and enhanced monitoring (paragraph 14)		✓	✓	
Reasonable measures to identify customers that exceed the occasional transaction threshold	✓		N/a	N/a

Ongoing monitoring of customer (paragraph 15) • CDD • Transactions • Sanctions		✓	✓	
Record keeping (paragraph 16) • Record everything the Code requires you to do	✓		✓	
Record retention (paragraph 17) • Keep for 5 years (even if no longer licenced) • Keep longer any records relating to a ML/FT/PF investigation	✓		✓	
Format and retrieval of records (paragraph 18) • Hard copy on-Island - without delay • E-copy - without delay • Hard copy off-Island - 7 days	✓		✓	
Registers of disclosures (paragraph 19) • Create registers of internal and external SARs • Required even if nothing recorded yet	✓		✓	
Register of ML/FT/PF enquiries (paragraph 20) • Create a register for enquiries from the authorities • Required even if nothing recorded yet	✓		✓	
Appoint MLRO (paragraph 21) • Responsible for reporting procedures, internal & external disclosures • Sufficiently senior & access to board • Sufficient time & resource • Consider Deputy MLRO	✓		✓	

Reporting procedures, Internal Disclosures, external disclosures (paragraph 22-24)	✓		✓	
Appoint AML/CFT Compliance Officer (paragraph 25) • Can be the same person as the MLRO • Responsible for monitoring and testing compliance • Sufficiently senior & access to board • Sufficient time & resource	✓		✓	
Monitoring and testing compliance (paragraph 25) • Ensure compliant procedures for all Code requirements • Test effectiveness • Remedy deficiencies • Annual (at least) report to board	✓		✓	
Integrity checks on new staff (paragraph 26)	✓		✓	
Staff training (paragraph 27) • New staff, at least annual & when requirements change • Cover all aspects listed • Recorded	✓		✓	
Fictitious, anonymous and numbered accounts (paragraph 28) • Don't set up or continue for customers over the threshold			✓	
Foreign branches and majority owned subsidiaries (paragraph 31) • Apply IOM standard to branches and subsidiaries (those below the IOM entity in the group structure)	✓		✓	

1.2 Interpretation - Online Gambling

Paragraph 3 of the Code (Interpretation) provides a long list of defined terms used in the Code and spans pages 3-10.

This part of the guidance highlights some of the key terms and important definitions rather than copying all of the interpretation section.

GSC Guidance and Policy

The term "**customer**" is used throughout the Code and the guidance for ease and consistency rather than punter, player, gamer, gambler, participant, etc. Customers include those that attempt to engage with an operator.

The terms "**occasional transaction**" and "**occasional transaction threshold**" apply only to bookmakers and casino walk-ins so should be overlooked by online gambling operators.

"**Ongoing customer relationship**" is the applicable term for online gambling business as this means a customer account.

"**Qualifying transaction**" means deposits or withdrawals and is an important term as customers that exceed the "**qualifying transaction threshold**" of EUR 3,000 (or equivalent) in 30 days must have their identity verified. For clarity, the threshold is EUR 3,000 in deposits or EUR 3,000 in withdrawals.

"**Beneficial owner**" is a term used throughout the CDD sections of the Code and is defined as -

a natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is being conducted and includes—

a) *in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) 25% or more of the shares or voting rights in the legal person;*

b) *in the case of any legal person, a natural person who otherwise exercises ultimate effective control or significant influence over the management of the legal person;*

c) *in the case of a legal arrangement, the trustee or other person who exercises ultimate effective control or significant influence over the legal arrangement; and*

d) *in the case of a foundation, a natural person who otherwise exercises ultimate effective control or significant influence over the foundation.*

"**Senior management**" means *the officers or any other persons who are nominated to ensure that the operator is effectively controlled on a day-to-day basis and who have responsibility for overseeing the operator's proper conduct.*

Part 1: Key Messages

- ✓ Definition of Customer refers to punter, player, gamer, gambler, and participant.
- ✓ Customer activity is split into two: ongoing customer relationships and occasional transactions.
- ✓ An ongoing customer relationship is where an account is opened for a customer.
- ✓ An occasional transaction is a single transaction or multiple linked transactions that take place where no account is opened.
- ✓ For bookmakers, all activity is considered an occasional transaction therefore, requirements relating to ongoing customer relationships do not apply.
- ✓ For casinos, both may apply because they can have members/account holders and walk-in customers that do not hold membership/an account.
- ✓ Thresholds refer to EUR 3,000 in wagers or EUR in collected winnings.

Part 2: General Requirements

2.1 Procedures and Controls (Paragraph 4)

The FATF Requirement

FATF Recommendation 1 (Assessing risks and applying a risk-based approach) states that obliged entities should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.

The policies, controls and procedures should be approved by senior management and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

The 2019 Code

4 Procedures and controls

(1) An operator must not enter into or carry on an ongoing customer relationship or carry out an occasional transaction with or for a customer unless the operator institutes, operates and complies with the systems, procedures, record-keeping, controls and training required in order to comply with the following provisions:

- (a) Part 3 (Risk-based Approach);
- (b) Part 4 (Customer Due Diligence);
- (c) Part 5 (Record-keeping and Reporting);
- (d) Part 6 (Staffing, Training and Monitoring Compliance); and
- (e) Part 7 (Miscellaneous).

(2) The procedures and controls referred to in sub-paragraph (1) must:

- (a) have regard to the size and risks of the operator;
- (b) apply to foreign branches and majority-owned subsidiaries (in accordance with paragraph 31 (foreign branches and majority-owned subsidiaries); and
- (c) be approved by the senior management of the operator.

(3) An operator must register on the designated reporting platform as provided by the Financial Intelligence Unit[1]

(4) The ultimate responsibility for ensuring that customer due diligence complies with this Code is that of the operator, regardless of any outsourcing.

[1] As required by sections 142 to 144 of the Proceeds of Crime Act 2008 and sections 11, 12 and 14 of the Anti-Terrorism and Crime Act 2003.

GSC Guidance and Policy

It is imperative that operators have policies, procedures and controls in place prior to going live.

Once procedures have been established, the onus is on the operator to ensure all staff members are aware of their roles and responsibilities, through a robust training programme. (See 6.3 Staff training (Paragraph 27)).

All procedures and controls should be risk-based and in line with the business risk assessment (see 3.3 Business risk assessment (Paragraph 6)). They should also apply to all foreign branches and majority owned subsidiaries (See 7.4 Foreign branches and majority owned subsidiaries (Paragraph 31)).

The Code requires AML/CFT/CPF procedures and controls to be approved by senior management. The GSC expects approval from the following:

- The AML/CFT Compliance Officer;
- The MLRO (for those relating to suspicious activity reporting); and
- At least one Director.

The designated reporting platform for reporting to the FIU is 'Themis'. The platform can be assessed at the following link: https://disclosures.gov.im.

All operators must have at least one staff member (the MLRO) registered on Themis at all times. This is to avoid delay in reporting due to the need to set up an account. Further, Themis is used by the FIU as a messaging system and repository for guidance and other useful information.

Where an operator outsources any aspect of CDD to third parties (e.g. to a customer service center) the operator must ensure that the third party complies with the requirements of the Code. In other words, the operator remains responsible for AML/CFT/CPF compliance.

Best Practice

- Documents include a version control detailing the version number and date, changes made, author and approval
- Procedures are not overly technical, can be understood by all staff members and applied to their roles
- Documents are kept in an online library so that staff members can easily access current versions

Terrestrial Operators

Printed copies of procedures should be made available for staff members without easy access to computers

Key Messages

Procedures and Controls - Key Messages

- ✓ Operators must have Policies and Procedures and controls in place prior to going live.
- ✓ All Staff must be aware of their roles and responsibilities trough a robust training programme.
- ✓ All procedures and controls should be risk-based and in line with the BRA and apply to all foreign branches and majority owned subsidiaries.
- ✓ Procedures and controls are to be approved by senior management.
- ✓ Where outsourcing any aspect of the operators compliance programme, the operator remains responsible for AML/CFT compliance.

2.2 Prohibitions (Paragraph 5)

The FATF Requirement

N/A

The 2019 Code

5 Prohibitions

(1) Terrestrial gambling operators must not enter into an ongoing customer relationship with, or carry out an occasional transaction for, a customer that is known to be conducting gambling by way of business.

(2) An online gambling operator may enter into an ongoing customer relationship with a customer that is known to be conducting gambling by way of business subject to the requirements of sub-paragraph 10(3)(c) (customers acting by way of business).

(3) An online gambling operator must not carry out occasional transactions.

GSC Guidance and Policy

Gambling activities can be categorised or split in various ways, including -

Occasional transaction vs. ongoing customer relationship; and

Retail vs. "by way of business".

"Occasional transaction" is defined in the Code, and describes a single or several linked transactions outside of an ongoing customer relationship.

"Ongoing customer relationship" is defined in the Code, and describes an operator-customer relationship where an account is opened.

"Retail" describes activities by a customer that is a natural person gambling as a recreational activity.

"By way of business" describes gambling activities that are business related rather than a recreational activity and may be undertaken by a natural person or legal person (e.g. a company) or arrangement (e.g. a syndicate). Business activities include junkets, professional gamblers, agents, affiliates and businesses to business (B2B) transactions.

For more detail on categorisation of gambling activities and their related risk factors (see 3.6 Risk Factors – Gambling Customer Categories/Types).

- **Terrestrial gambling operators**

  Terrestrial (land-based) gambling activities are considered retail operations and, as such, the Code prohibits the carrying out of transactions where the customer is known to be acting by way of business. Transactions that are carried out on behalf of another person are permitted only where this does not constitute business activity. In such cases additional CDD requirements apply (the person on whose behalf the activity is being conducted is classed as the beneficial owner of the customer.

  The GSC understands it may not be clear to the operator from the outset of the activity that it is being conducted on behalf of another person or by way of business. However, the GSC would expect a terrestrial operator to arrange training for front line staff, giving them the required tools to help identify a potential scenario where a customer may be acting by way of business.

Prohibitions - Terrestrial Gambling Operators

Look out for…

- Attempts to use accounts of a third party to fund bets or receive winnings
- Customers who refer to phone, text or written instructions shortly before placing bets
- Betting slips in other people's handwriting
- Betting slips in other people's names

❖ **Online gambling operators**

Are not permitted to carry out occasional transactions. All activity must be linked to an account (an ongoing customer relationship). If a customer wanted to carry out a 'one-off' transaction, an account must still be established and the relevant CDD requirements must be carried out. Online gambling operators are also allowed to accept gambling that is by way of business however additional due diligence requirements apply (see 4.3 Summary of requirements).

Key Messages

Prohibitions - Key Messages

- ✓ Online gambling operators are not permitted to carry out occasional transactions and all activity must be linked to an account.
- ✓ Terrestrial gambling operators must not enter into an ongoing customer relationship with, or carry out an occasional transaction for, a customer that is known to be conducting gambling by way of business.
- ✓ Online gambling operators may enter into an ongoing customer relationship with a customer that is known to be conducting gambling by way of business subject to the requirements of sub-paragraph 10(3)(c).

Part 3: Risk-Based Approach

3.1 Why Adopt a Risk-Based Approach to AML/CFT/CPF?

The risk-based approach recognises that there are finite resources available to combat ML, FT and PF. The concept behind the risk-based approach is therefore summarised as-

"If we have limited resources, let us at least use them wisely."

If an analogy is warranted then one can imagine a police force with 100 traffic officers charged with reducing speeding, dangerous driving and so forth. It can deploy them evenly throughout its district – or – it can station them on roads that are straight, near built up areas and schools and where accidents have been noted in the past. It if uses the latter strategy then it has adopted a risk-based approach.

Naturally, if the police force is so well resourced that it can station an officer on every road, then it need not resort to the risk-based approach. This will be an exceptional situation.

There are essentially four limbs to the FATF's risk-based approach –

- National Risk Assessment;
- Business Risk Assessment;
- Technology Risk Assessment; and
- Customer Risk Assessment.

For business, technology and customer risk, the Code lists "relevant" risk factors that must be considered. It should be noted that there are elements of crossover with each of these and, as such, the guidance is structured to explain the Code requirement for each type of assessment with more detailed guidance on particular risk factors later in the section.

3.2 National Risk Assessment (Paragraph 6(3))

The FATF Requirement

FATF Recommendation 1 (Assessing risks and applying a risk-based approach) requires a jurisdiction to assess its own ML/FT/PF risks and take action to coordinate efforts, apply appropriate resources and effectively manage risks. This NRA is the foundation for risk-based measures across each of the FATF Recommendations.

The 2019 Code

3 Interpretation

(1) In this Code—

…

> "National Risk Assessment" is a jurisdiction's evaluation of its ML/FT risks which aims to ensure that actions are co-ordinated domestically to combat ML/FT and proliferation, as required under the FATF Recommendations;

…

6 Business risk assessment

…

(3) The business risk assessment must have regard to all relevant risk factors including—

…

> (b) any relevant findings of the most recent National Risk Assessment relating to the Island;

…

GSC Guidance and Policy

In 2016, the IOM was one of the first countries to publish the results of an NRA under Recommendation 1, using the World Bank NRA Self-Assessment Tool.

The NRA identified the highest domestic and non-domestic ML/FT threats to the IOM. In addition, it also set out detailed analysis of each financial and non-financial sector in the IOM, the size and significance of that sector to the economy, the relevant ML/FT threats and vulnerabilities for each sector and the nature of the controls in place to frustrate this happening.

The IOM Government has since published an updated risk assessment of ML/FT, the NRA 2020, which builds upon the 2015 assessment and the findings of the MONEYVAL Mutual Evaluation Report of 2016.

The NRA 2020 was developed through cross-government participation, including the police, financial intelligence, customs, the courts, prosecutors and the regulators. The process also included industry involvement, with representatives from professional bodies and associations of relevant sectors contributing to the development of the NRA.

The NRA 2020 is available at:

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

It concludes that online gambling presents a Medium ML risk and terrestrial gambling presents a Medium Low risk. Both present a Low FT risk.

All operators must study the relevant parts of the NRA 2020 as there is a Code requirement for the NRA to be considered as part of an operator's risk assessment of its own business (see 3.3 Business risk assessment (Paragraph 6).

3.3 Business Risk Assessment (Paragraph 6)

The FATF Requirement

FATF Recommendation 1 (Assessing risks and applying a risk-based approach) states that obliged entities should identify, assess and take effective action to mitigate their ML/FT risks.

The 2019 Code

6 Business risk assessment

(1) An operator must carry out an assessment (a "business risk assessment") that estimates the risk of ML/FT posed by the operator's business and customers.

(2) The business risk assessment must be—
- (a) undertaken as soon as reasonably practicable after the operator commences business;
- (b) recorded in order to be able to demonstrate its basis; and
- (c) regularly reviewed (details of any review must be recorded) and, if appropriate, amended so as to keep the assessment up-to-date.

(3) The business risk assessment must have regard to all relevant risk factors including—
- (a) the nature, scale and complexity of the operator's activities;
- (b) any relevant findings of the most recent National Risk Assessment relating to the Island;
- (c) the products and services provided by the operator;
- (d) the manner in which the products and services are provided including whether the operator meets its customers;
- (e) the involvement of any third parties for elements of the customer due diligence process;
- (f) technology risk assessments carried out under paragraph 7 (technology risk assessment); and
- (g) customer risk assessments carried out under paragraph 8 (customer risk assessment).

GSC Guidance and Policy

What? The Code requires an operator to formally undertake and document a BRA in order to estimate the risk of ML/FT/PF posed by its own business and its customers.

Why? The purpose of the assessment is for the operator to understand its inherent risks and vulnerabilities so that it may tailor its AML/CFT/CPF controls accordingly. The BRA should form the basis of the operators risk based approach and once the relevant risk factors have been assessed, the operator should be in a position to set a 'risk appetite', allowing the operator to decide on how much risk they are prepared to tolerate. A risk-based approach will determine how systems and controls are applied to mitigate risks.

Having a clear, documented BRA and risk appetite should assist an operator in establishing and maintaining a positive compliance culture.

When? The Codes specifies that the risk assessment process must be conducted as soon as reasonably practicable after the operator commences business. There is also a requirement to review the assessment regularly, to detail reviews undertaken and make amendments to keep it up-to-date. BRAs should be updated where there are significant changes to risk factors (e.g. a new and significant target market or product) or in the absence of such changes, at least annually.

Who? The assessment should include input from staff members, AML/CFT experts such as the MLRO and AML/CFT Compliance Officer, and subject matter experts regarding the operator's customer base, products and services.

How? A BRA is unique to each operator and based on considerations of the "relevant risk factors" as listed in the Code. The relevant factors are explored in more detail below.

- **A - Nature, scale and complexity of activities**

  Operators are in the best position to identify the areas of their business that present the greatest risks of ML/FT/PF and therefore those that should be the focus of their attention. Assessing the nature of gambling activities, the size of their operations, and any complex activities that may need additional scrutiny, will help an operator identify specific threats or vulnerabilities that exist in ML/FT/PF.

  "Nature" of activities refers to the category/types of gambling, each of which has a unique set of characteristics and risks (see 3.6 Risk factors; Gambling Customer Categories/Types).

  "Scale" of activities refers to the volume and value of activities and the geographical spread.

  "Complexity" of activities is a risk factor because overly complex models can be abused in order to disguise the source or destination of funds or criminal ownership.

- **B - National Risk Assessment**

  The latest NRA provides an overview of the online gambling sector's vulnerabilities and threats, which may be relevant to an operator and therefore considered as part of the BRA. The GSC would expect an operator to be aware of the typologies reported in the latest NRA, giving consideration where necessary if they are applicable to their business, and when they are, apply mitigating strategies to combat the risk of ML/FT/PF.

- **C - Products and services**

  A BRA should include a review of the products and services provided by an operator. Peer-to-peer gambling that allows one individual to play directly against another, such as poker, may be considered higher risk due to the associated risks of collusion and chip dumping. Gambling products, such as roulette, baccarat and craps may be considered lower risk as they don't offer a high rate of return, however due to the high likelihood of winning, this form of gambling could form part of a ML scheme (see 3.7 Risk factors; Gambling Products and Services/types).

- **D - The manner in which the products and services are provided**

  This aspect refers to the delivery and transaction methods and covers a broad range of considerations; whether the customer and operator meet face-to-face, what payment methods are available and transactions types (see 3.7.1 Risk factors; Delivery and transaction methods).

❖ **E - The involvement of third parties**

Consideration must be given to the involvement of third parties in the CDD process. Third parties generally fit into one of two categories –

- Agents or introducers that provide CDD to the operator; and
- Entities that an operator outsources functions to.

In both categories, the operator remains responsible for obtaining and maintaining satisfactory CDD. Where CDD is not provided directly by the customer there is an increased risk that it may not be complete, accurate and up to date. Where third parties carry out CDD functions, the risk is that the third party does not meet the Code requirements and/or that training and compliance monitoring is insufficient.

❖ **F - Technology Risk Assessment**

Each current TRA should factor into the BRA (see 3.4 Technology Risk Assessment (Paragraph 7)).

❖ **G - Customer risk**

Consideration should be given to the risk of the operator's customers base, including -

- The proportion of high risk customers;
- The proportion of politically exposed customers;
- Countries where significant proportions of customers reside or transactions originate from; and
- Typical customer transaction volume, size and type.

This need not include a review of each and every customer except where the operator has only a small number of customers.

Best Practice

- BRAs should clearly demonstrate an understanding of the ML/TF/PF risk factors faced by the business
- Includes consideration of threats; likelihood and impact plus actions taken to address
- Does not confuse AML/CFT/CPF risks and commercial risks
- Consideration is also given to parts (i.e. gambling, payment services) of other countries' NRAs
- Particular attention is paid to the NRAs of countries where significant portions of the customer base reside
- Setting a particular date for each calendar year for a periodic BRA to take place
- Clear version controls

Key Messages

Business Risk Assessment - Key Messages

- ✓ BRAs must be recorded.
- ✓ BRAs must be formally undertaken and recorded.
- ✓ BRAs must estimate the ML/FT/CPF risks faced by its own business and its customers.
- ✓ BRA is integral in determining a business risk appetite.
- ✓ BRAs must be conducted as soon as "reasonable practicable" after commencement of business and must be kept up to date at least annually or where there is a significant change to the risk factors faced by the operators business.

3.4 Technology Risk Assessment (Paragraph 7)

The FATF Requirement

FATF Recommendation 15 requires obliged entities to carry out risk assessments prior to the launch of new products, business practices or the use of new or developing technologies. It also requires appropriate actions to manage or mitigate risks.

The 2019 Code

7 Technology risk assessment

(1) An operator must carry out an assessment (a "technology risk assessment") that estimates the risk of ML/FT posed by any technology to the operator's business.

(2) The technology risk assessment must be—
- (a) undertaken as soon as reasonably practicable after the operator commences business;
- (b) undertaken prior to the launch or implementation of new products, new business practices and delivery methods using new delivery systems;
- (c) undertaken prior to the use of new or developing technologies for both new and pre-existing products;
- (d) recorded in order to demonstrate its basis; and
- (e) regularly reviewed (details of any review must be recorded) and, if appropriate, amended so as to keep it up to date.

(3) The technology risk assessment must have regard to all relevant risk factors including—
- (a) technology used by the operator to comply with AML/CFT legislation;
- (b) the business risk assessment carried out under paragraph 6;
- (c) the products and services provided by the operator;
- (d) the manner in which the products and services are provided by the operator with consideration given to delivery methods, communication channels and payment mechanisms;
- (e) digital information and document storage;
- (f) electronic verification of documents; and
- (g) data and transaction screening systems.

GSC Guidance and Policy

What? The Code requires operators to formally undertake and document TRAs in order to estimate the risk of ML/FT/PF posed to the operator's business by technology.

Why? TRAs will assist operators in identifying, understanding and addressing the risks posed. This is particularly important for the gambling sector as it is noted for innovation and its track record as an early adopter.

When? Initially, a risk assessment must be undertaken as soon as reasonably practicable. A draft TRA should be prepared prior to launch (i.e. theory based) which is to be updated once the operator has customers (detailing the technology used with live statistics where possible).

Assessments must then be carried out prior to the launch of each new product, business practice, delivery method or delivery system. Such assessments must also be regularly reviewed and kept up-to-date.

Examples of matters that should trigger a TRA include new –

- Gambling licence categories;
- Payment methods or currencies;
- Back office systems;
- Customer messaging systems.

Who? The TRA process should be designed by AML/CFT experts such as the MLRO and AML/CFT Compliance Officer, and carried out with input from technical experts such as the manager responsible for IT.

How? A TRA must include consideration of the "relevant risk factors" as listed in the Code and explored in more detail below.

It should be noted that, unlike elsewhere in the Code, some of the listed risk factors for TRAs are likely to reduce ML/FT/PF risk.

- **A - Technology used for AML/CFT compliance**

  Any introduction or significant change to technologies used for AML/CFT compliance other than those considered under (F) Electronic verification of documents and (G) Data and transaction screening systems must also be risk-assessed.

  Examples of other technologies used for AML/CFT compliance include–

  - Systems used to monitor for large or unusual transactions;
  - Systems or databases used to verify customer identification and/or address information; and
  - Systems used to analyse customer gambling/playing behaviours (e.g. to identify chip dumping).

  Significant changes that would warrant a TRA include -

  - Switching off/on new system "rules"; and
  - A change in service provider.

- **B - The business risk assessment**

  As explained earlier in this guidance, the BRA sets the operator's risk appetite and provides the starting point for all risk-based AML/CFT processes and procedures.

- **C - Products and services**

  Please see 3.7 Risk Factors – Gambling Products and Services/Types.

- **D - The manner in which the products and services are provided**

  Please see 3.7.1 Risk factors: Delivery and transaction methods.

- **E - Digital information and document storage**

  The Code places record keeping requirements on operators. It is therefore essential that new and developing technologies used for digital information and document storage are risk assessed. For further detail on the record keeping requirements, please see Part 5: Record Keeping and Reporting.

- **F - Electronic verification of documents**

  Where physical documents are used for CDD purposes such as to establish customer

identity or source of wealth, there is a risk that the documents may be stolen, forged or tampered with. The GSC encourages, particularly where documents are not physically handled by the operator's staff, the use of electronic systems to verify documents (see 4.6 Verification of identity of customers (Paragraph 11).

❖ **G - Data and transaction screening systems**

There is a requirement for customers (and their beneficial owners) to be checked to see if they are, or they become, sanctioned or a politically exposed person. New and developing technology used for such checks must be risk-assessed. For further detail, please see 3.4 Technology risk assessment (Paragraph 7) and 4.11 Name screening systems.

Best Practice

- Consideration should also be given to non-AML/CFT matters such as the risk of hacking or data protection impact assessments. This may be included in the TRA provided that it does not pollute the AML/CFT risks
- In addition to screening the names of customers and beneficial owners, consideration should be given to screening transaction references and the names of any relevant third parties such as agents, affiliates or persons funding a customer's gambling activities
- Setting a particular date for each calendar year for a periodic TRA to take place
- Clear version controls

In addition to the mandatory risk factors detailed above, consideration should be given to whether the technology (which includes new products, new business practices and delivery methods using new delivery systems) –

- Relies on activity in high risk jurisdictions;
- Involves business partners that are high risk or whose ownership/credentials cannot be verified;
- Allows cash into the system without CDD measures compliant with the Code standard; or
- Is cited as high risk or included in typology reports by the FATF, an FSRB or competent authorities.

Key Messages

Technology Risk Assessment - Key Messages

- ✓ TRAs must be recorded.
- ✓ TRAs must estimate the ML/FT/PF risks in relation to the technology used throughout the operators business.
- ✓ TRAs must be conducted as soon as "reasonable practicable" after commencement of business.
- ✓ TRAs must then be carried out prior to the launch of each new product, business practice, delivery method or delivery system. Such assessments must also be regularly reviewed and kept up-to-date.

3.5 Customer Risk Assessment (Paragraph 8)

The FATF Requirement

FATF Recommendation 10 (Customer due diligence) states that CDD should be performed using a risk-based approach. The interpretive notes that accompany Recommendation 10 cite the following factors that should be taken into account during the risk assessment process –

- Customer risk factors such as geographic separation, arrangements with legal persons and the level of assets transacted;
- Country risk factors such as countries that do not have FATF compliance frameworks, are noted by credible sources as having significant levels of corruption or criminal activity or that are subject to sanctions; and
- Product and channel risks such as non-face-to-face business.

The 2019 Code

8 Customer risk assessment

(1) This paragraph applies to ongoing customer relationships and occasional transactions that exceed the occasional transaction threshold.
(2) An operator must carry out an assessment (a "customer risk assessment") that estimates the risk of ML/FT posed by a customer.
(3) A customer risk assessment must be—
    (a) undertaken as soon as reasonably practicable after entering into an ongoing customer relationship or carrying out an occasional transaction;
    (b) recorded in order to be able to demonstrate its basis; and
    (c) regularly reviewed (details of any review must be recorded) and, if appropriate, amended so as to keep the assessment up-to-date.
(4) The customer risk assessment must have regard to all relevant risk factors including—
    (a) the business risk assessment carried out under paragraph 6 (business risk assessment);
    (b) the nature, scale, complexity and location of the customer's activities;
    (c) the manner in which the products and services are provided to the customer;
    (d) the involvement of any third parties for elements of the customer due diligence process;
    (e) whether the operator and the customer met during an ongoing customer relationship or during its formation or in the course of an occasional transaction; and
    (f) the risk factors included in sub-paragraphs (5) and (7).
(5) Matters that pose a higher risk of ML/FT—
    (a) an ongoing customer relationship or occasional transaction with a customer that is resident or located in a jurisdiction in List A;
    (b) a customer that is the subject of a warning in relation to AML/CFT matters issued by a competent authority or equivalent authority in another jurisdiction.
(6) If sub-paragraph 5(a) or (b) applies, the operator's senior management must approve the establishment or continuation of the ongoing customer relationship or the carrying out of the occasional transaction.

(7) Matters that may pose a higher risk of ML/FT include—

(a) activity in a jurisdiction the operator deems to be higher risk of ML/FT;
(b) an ongoing customer relationship or occasional transaction with a customer that is resident or located in a jurisdiction in List B;
(c) activity in a jurisdiction in List A or B;
(d) a situation that by its nature presents an increased risk of ML/FT;
(e) an ongoing customer relationship or occasional transaction with a customer that is a PEP;
(f) a company that has nominee shareholders or shares in bearer form;
(g) the provision of high risk products;
(h) the provision of services to high-net-worth individuals;
(i) a legal arrangement;
(j) persons performing prominent functions for international organisations;
(k) customers that are sporting professionals betting on sports; and
(l) customers that use multiple sources to fund their gambling activities.

(8) Any customer identified as high risk must be subject to enhanced customer due diligence.

GSC Guidance and Policy

What? The Code requires operators to carry out and record risk assessments of customers.

Why? The risk assessment process exists to allow the (normally) finite monitoring resources of the operator to be focussed on the customer population most likely to attempt to launder money or fund terrorism. The risk assessment identifies higher risk customers and those customer must be subjected EDD (see 4.9 Enhanced customer due diligence (Paragraph 14)).

An accepted shortfall of this concept is that a small percentage of any ML/FT/PF may occur in the lower risk population and it could go unnoticed by all but the most sophisticated monitoring systems.

When? The Code specifies that the risk assessment process must be conducted as soon as reasonably practicable, after entering into an ongoing customer relationship or carrying out an occasional transaction that exceeds the threshold of EUR 3,000 (in a single or several linked transactions).

Who? The assessment process should be designed by AML/CFT experts such as the MLRO and/or AML/CFT Compliance Officer and carried out in practice by staff members with appropriate training.

The Code requires senior management (a defined term) approval for customers that are resident in a "List A" jurisdiction or that are the subject of an AML/CFT warning.

How? A CRA must include consideration of the mandatory risk factors (as detailed below). The Code also provides lists of matters that pose a higher risk (i.e. customer must be classed as high risk) and that *may* pose a higher risk (i.e. the operator determines whether they are high risk based on consideration of all relevant factors). After this initial CRA it must be regularly reviewed and updated. The GSC expects higher risk customers to be reviewed at least annually.

Terrestrial Operators

- Transactions are typically conducted face-face on a time-sensitive basis
- A simplified process such as a short form could be completed at the time with further consideration being given by back office staff members, such as the MLRO soon after

❖ **A - Business risk assessment**

As explained earlier in this guidance, the BRA sets the operator's risk appetite and provides the starting point for all risk-based AML/CFT/CPF processes and procedures.

❖ **B - Nature, scale and complexity of activities**

Operators are in the best position to identify the areas of their operations that present the greatest risks of ML/FT/PF and therefore those which should be the focus of their attention. By assessing the nature of gambling activities, the size of their operations, and any complex activities that may need additional scrutiny, this will help identify specific threats or vulnerabilities that exist in ML/FT/PF.

"Nature" of activities refers to the category/types of gambling, each of which has a unique set of characteristics and risks (see 3.6 Risk Factors – Gambling Customer Categories/Types).

"Scale" of activities refers to the volume and value of activities and the geographical spread.

When risk-assessing customers, particular attention should be given to the –

- Value of deposits (including aggregated values);
- Frequency of deposits;
- The value and frequency of withdrawals;
- The size and nature of bets; and
- Other relevant matters such as credit facilities

This guidance does not prescribe thresholds/trigger values over which customers must be treated as high risk. This is because operators, their business models and their customer bases can differ greatly so a one-size-fits-all approach is not appropriate.

"Complexity" of activities is a risk factor because overly complex models can be abused in order to disguise the source or destination of funds or criminal ownership.

Best Practice

- Aggregate values are considered on a daily/weekly/monthly/lifetime basis and not on annual values alone
- Focus is given to customers who are frequently "just under" any high risk thresholds
- Operators bear in mind that gambling is a recreational activity for retail customers and set thresholds/triggers based on consideration of average income, outgoings, etc. for their customer demographic
- For many gambling operators customers either will always be met or never met
- Consideration of this may be built into (and evidenced in) risk-assessment procedures rather than requiring documented consideration for each and every customer

❖ **C - The manner in which the products and services are provided**

This aspect refers to the delivery transaction methods accessed by the customers and covers a broad range of considerations; whether the customer and operator met face-to-face, what payment methods are used and the transactions types seen (see 3.7.1 Risk factors: Delivery and transaction methods).

❖ **D - The involvement of third parties**

Consideration must be given to the involvement of third parties in the CDD process. At a customer level, this means the use of agents or introducers.

Where CDD is not provided directly by the customer there is an increased risk that it may not be complete, accurate and up to date.

❖ **E - Whether the customer was met**

Where customers are not met by the operator there *may* be a higher ML/FT/PF risk because -

- The customer may not be who they claim to be; and
- Non face-to-face activity can be more appealing to criminals as it may reduce the likelihood of them being caught and dealt with by law enforcement.

The concept of meeting a customer need not be limited to face-to-face contact. Consideration should also be given to the use of real-time visual communication media via the internet such as full motion video conferencing.

❖ **F - The "must be" and "may be" high risk lists**

The Code provides only two things that dictate a customer must be categorised and treated as a high risk customer. For customers falling into either of these categories, senior management approval to conduct business with the customer must also be obtained and recorded –

- A customer that is resident (natural persons) or located (legal persons) in a "list A" jurisdiction; and

- A customer that is the subject of an AML/CFT warning issued by a competent authority (such as the GSC or its overseas equivalents).

"**List A**" refers to a very short list of jurisdictions published by the DHA on its website due to them having on-going and substantial risks of ML/FT/PF. The list is periodically updated based on the outcome of the FATF's plenary meetings, currently three per year.

The Code lists 12 things that may be high risk. The GSC expects operators to treat customers with these characteristics as high risk unless the customer's scale of activity is very small and this approach is permitted in line with their own risk appetite. This should be clearly documented in their BRA and CRA procedures. For further detail, see 3.7.2 Risk factors; Matters that may be high risk.

Key Messages

Customer Risk Assessment - Key Messages

- ✓ CRAs must be carried out and recorded to provide an audit trail and show how the rating was reached.
- ✓ CRAs must be carried out as soon as reasonably practicable after entering into an ongoing customer relationship or carrying out an occasional transaction that exceeds the threshold of EUR 3,000 (in a single or several linked transactions).
- ✓ CRA must give regard to; the BRA, nature, scale and complexity of activities, the manner in which the services are provided, the involvement of any third parties, whether the customer was met and whether the customer is resident in a high risk jurisdiction or subject to an AML/CFT warning.

3.6 Risk Factors – Gambling Customer Categories/Types

This section relates to the relevant (mandatory) risk factors for both 3.3 Business risk assessment (Paragraph 6) and 3.5 Customer risk assessment (Paragraph 8) (see factor B) – the "nature, scale and complexity" of activities.

GSC Guidance and Policy

"Standard retail" describes a customer who is a natural person and gambles as a recreational activity. The customer poses a low or medium risk (where other high risk factors are not present).

"VIP retail" describes a customer who is also a natural person and recreational customer but where the level of activity far exceeds that of an average customer. The customer poses a higher risk because –

- There is a risk that they would have undue influence over an operator due to their profitability;
- Wealthy VIP customers may also be politically exposed;
- They could be funded by proceeds of crime or be a problem gambler (although that is not an ML/FT/PF risk).

"Junket" describes a group of natural persons arranged by a junket agent. The group typically comprises wealthy foreign residents. Junkets present a higher risk due to the VIP retail risk factors above plus the following additional factors –

- There are typologies linking junket operations with organised crime;
- They can be used to facilitate cross-border movement of funds;
- Debts may be accumulated with the agent or between players that, in turn, could lead to extortion attempts.

"Professional gambler" describes a natural person who gambles by way of business. Please see below for the GSC's full definition. A professional gambler will play games of skills rather than games of chance. As they are highly skilled, they are expected to be more successful than a standard retail or VIP retail customer. They are also expected to spend considerable time gambling. The risk posed by a professional gambler would typically be lower than that of a VIP retail customer given that operator profits would generally be made through rake rather than losses against the house. There may be challenges in establishing SOF and SOW as this may derived from winnings elsewhere.

- **Professional gambler GSC policy definition:**
  - *Persistence in the market place,*
  - *A tendency towards success,*
  - *Possible personal acquaintance; and*
  - *An absence of casino play, play against the house.*

And more specifically players who –

  - *Act as a business looking to mitigate exposure (i.e. hedging);*

- *Act as an individual engaging in gambling activity as a means of earning a wage;*
- *Only participate in skill based activities such as sportsbook or poker and would not participate in casino games;*
- *Apply mathematical algorithms, strategy and statistics to place considered bets;*
- *Show a "winning" profile over long term activity;*
- *Place large amounts of bets with a large amount of bookmakers to engender an aggregate return;*
- *Place large bets in order to take advantage of discount incentives;*
- *Place bets logically with a focus on low over-rounding and probability of return.*

"Affiliate" describes a natural person who generates commission either by introducing customers or by acting as an informal MVTS arrangement that can be used by customers seeking to gamble but without ability to access a payment mechanism supported by the operator. Affiliates may also hold their own accounts for their personal gambling. Where an affiliate is providing only marketing or introductory services the risks are typically low-medium however where informal MVTS is present this would constitute high risk and consideration should be given to whether such a service would require a licensing by the relevant authority, for example the IOMFSA.

"Business to business" or "B2B" describes activity where the customer is a legal person (e.g. a company), legal arrangement (e.g. a trust) or foundation (a legal person that resembles a trust). B2B customers are typically only seen in online gambling and can cover a broad range of activities. B2B business is typically higher risk due to the volume and value of transactions. The introduction of complex ownership structures or reliance on third parties (such as introducers) would act to heighten the risk further.

3.7 Risk Factors – Gambling Products and Services/Types

This section relates to the relevant (mandatory) risk factors for both 3.3 Business risk assessment (Paragraph 6) and 3.4 Technology risk assessment (Paragraph 7) (see factor C).

GSC Guidance and Policy

"Against the house" is where customers bet against the operator. Risk levels will vary greatly depending on other factors such as the product and payment method.

"Peer to peer" is where customers bet against each other. Additional risks are present where there is also a skill element (see below).

"Peer to peer transfer" is a direct transfer of funds between customers without a third party intermediary i.e. banks. The nature of these transfer are at higher risk of ML/FT/PF due to the ease of movement and often the use of third parties can be used to obscure the source of ownership. Extra care should be taken when a customer has higher risk indicators e.g. jurisdiction, PEP, etc.

"Game of chance" describes betting on a random outcome. Examples include lotteries, roulette and loot boxes (in e-sports betting). These are generally viewed as lower risk except where the customer is able to bet on every possible outcome. Games of chance are not typically seen in organised or large-scale ML but can be used by customers spending proceeds of crime on a recreational basis.

"Game of skill" describes betting where the outcome is based on the mental or physical skill of the customers. Peer to peer skill games are higher risk than games of chance because customers can collude with each other where one customer deliberately loses in order to transfer value to another customer (e.g. chip-dumping in poker). The risks are further increased where customers select their opponents and play in a private environment (e.g. a private VIP poker room).

"Betting on the outcome of an event" typically describes sports-betting but can be applied to a huge range of activities such as political elections, TV game shows, e-sports and so on. Sporting events, particularly in lower leagues and less well regulated areas can be subject to corruption such as match-fixing, which has well established links to organised crime groups and features in Europol's Serious and Organised Crime Threat Assessment[2].

[2] https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

3.7.1 Risk Factors: Delivery and Transaction Methods

This section relates to the relevant (mandatory) risk factors for both 3.3 Business risk assessment (Paragraph 6) (see factor D), 3.4 Technology risk assessment (Paragraph 7) (see factor D) and 3.5 Customer risk assessment (Paragraph 8) (see factor C).

There are many and varied delivery methods and transaction types. Examples of higher risk methods and types include -

- **The customer and operator do not meet face-to-face**

  Establishing and verifying a customer's identity can be more difficult when the customer is not met face-to-face. The operator becomes reliant on the customer providing copies of documentation without being able to scrutinise them up close, feel them or compare to the customer standing in front of them, although other non-face-to-face meetings such as full motion video conferencing can greatly reduce the risk.

- **Transactions carried out on a time-sensitive basis**

  Where a staff member feels rushed they may be more likely to carry out cursory checks rather than to take their time and consider fully. An example of this is where a customer seeks to place a bet on a sporting event that is about to take place.

- **Transactions carried out at multiple premises**

  Multiple premises can be abused by customers seeking to structure their activity. This is where a customer (potentially a money mule) carries out multiple smaller transactions in an attempt to avoid triggering any reporting requirements or arousing suspicion.

  Effective transaction monitoring systems will collate transactions undertaken at each of the operator's premises so that the full extent of the activity can be observed.

  For further detail on how to do this in practice, see 4.10 Ongoing monitoring (Paragraph 15).

- **Multiple accounts**

  This presents another method to structure payments. Operators should take steps to identify multiple accounts held by the same customer by checking their databases for registrations with the same (or very similar) personal information and determine whether there is a valid reason for the holding of multiple accounts (some operators may offer accounts in difference currencies, for example).

  In addition to increasing the ML/FT risk, the Online Gambling (Registration and Accounts) Regulations 2008 state –

  "The Operator shall not encourage a Player to hold more than one account."

- **Multiple brands or sites**

  The multiple account risks apply equally where operators offer accounts with multiple URLs/brands. The Code requirements apply to operators meaning that transaction monitoring should be carried out at operator rather than site or brand level.

- **Cash or other anonymous payment method**

  The use of cash or methods such as crypto currency or prepaid cards that are not attached to a known account holder pose a higher ML/FT/PF risk as their ownership and the source/destination of funds is difficult to establish. (Note that cash is not permitted for online gambling customers). For further guidance on virtual currencies; see the AML/CFT Guidance page.

Virtual Currency & Virtual Goods

- *The IOMFSA is the AML/CFT supervisor for IOM virtual currency exchanges*
- *Additional guidance for virtual currencies (e.g. Bitcoin) and virtual goods (e.g. skins) gambling is published on AML/CFT Guidance page on the GSC website*
- *Although defined as "property", virtual currency should be treated and monitored as if it were money for AML/CFT purposes.*

❖ **Payment methods that are not well AML/CFT regulated**

Traditional payment methods such as bank transfers, debit and credit cards are usually well regulated meaning that the issuing entity should have carried out CDD on the customer. For non-traditional methods such as prepaid cards, payment service providers and virtual currency exchanges the standards of AML/CFT requirements, compliance and supervision vary greatly.

NRAs and MERs by the FATF or FATF-style regional bodies such as MONEYVAL provide valuable sources of information.

❖ **Multiple deposit sources**

Customers that use multiple mechanisms, such as different debit or credit cards to deposit should be considered as high risk as this can be a sign of card fraud (ML) or collating funds from third parties (FT). The risk is particularly high where funds are subsequently withdrawn with little gambling activity or where they request to withdraw to a different payment mechanism.

❖ **Different method used to deposit and withdraw**

This is particularly high risk where multiple deposit sources are used or where a customer is able to withdraw with little or no gambling activity. Operators should put in place "play-though" requirements to detect this.

❖ **Rapid, repeat transactions**

Such transactions can be used to structure payments in order to avoid CDD or reporting thresholds.

❖ **Transfer of value between customers**

Transfers between customers of money, credits, chips, etc. can be used as a way to make payments outside the regulated financial system especially where the customers are based in different jurisdictions (cross-border movements). Operators should only allow transfers between customers in very limited, well-monitored situations where EDD has been completed on both parties (as they should be deemed high risk).

Peer to Peer transfers without controls are at a higher risk of ML/FT/PF. Peer-to-peer gambling that allows one individual to play directly against another, such as poker, may be considered higher risk due to the associated risks of collusion and chip dumping. These types of transfers could offer criminals an opportunity to introduce criminal proceeds into the legitimate financial system and make it very difficult to follow the money.

Operators that provide Peer to Peer transfer functionality must ensure that they have effective risk mitigating controls in place to reduce the risks. Examples of risk mitigating controls are:

- Consider the risk to the business of Peer to Peer transfers though the BRA.
- Well established CDD/EDD procedures that are designed to identify the higher risks associated with Peer to Peer transfers.

- Setting lower limits for EDD.
- Clear and effective policies and procedures that are well communicated to staff.
- Enhanced transaction monitoring.

Play-through vs Responsible Gambling

- *A requirement to gamble prior to withdrawal reduces ML/FT/PF risk however this may conflict with responsible gambling*
- *Play-though rules should detect this unusual activity for further scrutiny however customers should not be forced to gamble to withdraw.*

3.7.2 Risk Factors: Matters That May Be High Risk

This section relates to 3.5 Customer risk assessment (Paragraph 8) (see factor F – The "must" and "may be" high risk lists)

❖ **A - Activity in a jurisdiction the operator deems to be a higher risk of ML/FT/PF**

In addition to the jurisdictions noted as higher risk in "List A" and "List B" published by the Department of Home Affairs https://www.gov.im/about-the-government/departments/home-affairs/chief-executives-office/anti-money-laundering-legislation-and-countering-the-financing-of-terrorism-amlcft/

Operators should consider whether there are any addition jurisdictions that it considers to be higher risk based on its own risk appetite and consideration of relevant factors such as –

- AML/CFT/CPF standards and regulation of gambling, banks, payment service providers, etc. in that jurisdiction;
- The prevalence of typologies or fraud emanating from that jurisdiction;
- The operator's own experience of business in that jurisdiction.

❖ **B - Customers resident or located in a "List B" jurisdiction**

The DHA publishes two lists. Being resident (natural persons) or located (customers that are legal person) in a "List A" jurisdiction makes a customer high risk automatically whereas being resident of located in a "List B" jurisdiction only *may* pose a higher risk.

❖ **C - Activity in a "List A" or "List B" jurisdiction**

This is a separate consideration to residency or location and should include consideration of the following, particularly where other risk factors are present –

- The source of funding (i.e. where funds come from);
- The destination of withdrawals;
- The original SOW (i.e. if the customers wealth originates from high risk jurisdictions);

- Where the customer is logging on or contacting the operator from (e.g. IP address and telephone number checks).

❖ **D - A situation that by its nature presents an increased risk of ML/FT/PF**

Like item (A) above, this requires an operator to consider whether there are any additional risk factors not covered by the Code that it deems to represent a higher risk based on knowledge and experience of business in the sector and analysis of internal and external disclosures.

❖ **E - A customer that is a PEP**

Please refer to 4.8 Politically exposed persons (Paragraph 13).

❖ **F - Nominee shareholders or shares in bearer form**

Customers that are legal persons (e.g. companies) with nominee shareholders or shares issues in bearer form pose additional risk as they may be used to conceal the true ownership.

❖ **G - The provision of high risk products**

Operators are required to consider the products and services that they offer as part of their BRA. Where it is determined that they offer high risk products this too should be a consideration in the CRA. This is particularly relevant where the operator offers a range of products with differing risk profiles.

❖ **H - High-net-worth individuals**

The risks associated with high net worth individuals (HNWIs) are similar to those of a PEP or person performing prominent functions for international organisations; that their wealth originates from criminal activities and that they are a person with celebrity or political connections making them a higher risk for bribery and corruption.

There is no FATF or other widely accepted definition for a HNWI however many financial institutions interpret this as being a person with liquid financial assets exceeding £1,000,000. As this information would not usually be known to gambling operators, the GSC would expect operators to treat as a HNWI –

- Their high roller or VIP customers;
- Customers whose SOW information indicates annual income exceeding £500,000
- Operators should consider implementing their own lower thresholds should they operate in markets where average income is far less than that in the IOM or UK.

❖ **I - Legal arrangements**

Customers acting by way of business would typically be natural persons (individuals) or legal persons (companies). Where a customer is, or is owned by, a legal arrangement (such as a trust) the ML/FT/PF risks are increased they can be abused for creating complex ownership structures to disguise true ownership.

❖ **J - Persons performing prominent functions for international organisations**

Please refer to 4.8 Politically exposed persons (Paragraph 13). The Code definition includes a person that is, or has been, a "senior member of management of, or a member of, the governing body of an international entity or organisation".

- **K - Sporting professionals betting on sports**

  "**Sporting professionals**" refers to professional players as well as persons involved in managing and operating sports such as team coaches, managers and owners.

  When sporting professionals bet on sport, there is a risk that they may be involved in match-fixing either as voluntary participants or due to coercion.

  Sports corruption was one of the 12 featured crimes in Europol's 2017 Serious and Organised Threat Assessment[3].

  Agents, particularly chains of agents, can be abused to disguise the underlying customer (potentially a corrupt sports professional) from the gambling operator. Lower league or less well regulated sports present the highest risks.

- **L - Customers that use multiple sources to fund their gambling**

  Customers that use multiple mechanisms, such as different debit of credit cards to deposit should be considered as high risk as this can be a sign of card fraud (ML) or collating funds from 3rd parties (FT). The risk is particularly high where funds are subsequently withdrawn with little gambling activity or where they request to withdraw to a different payment mechanism.

Responsible Gambling

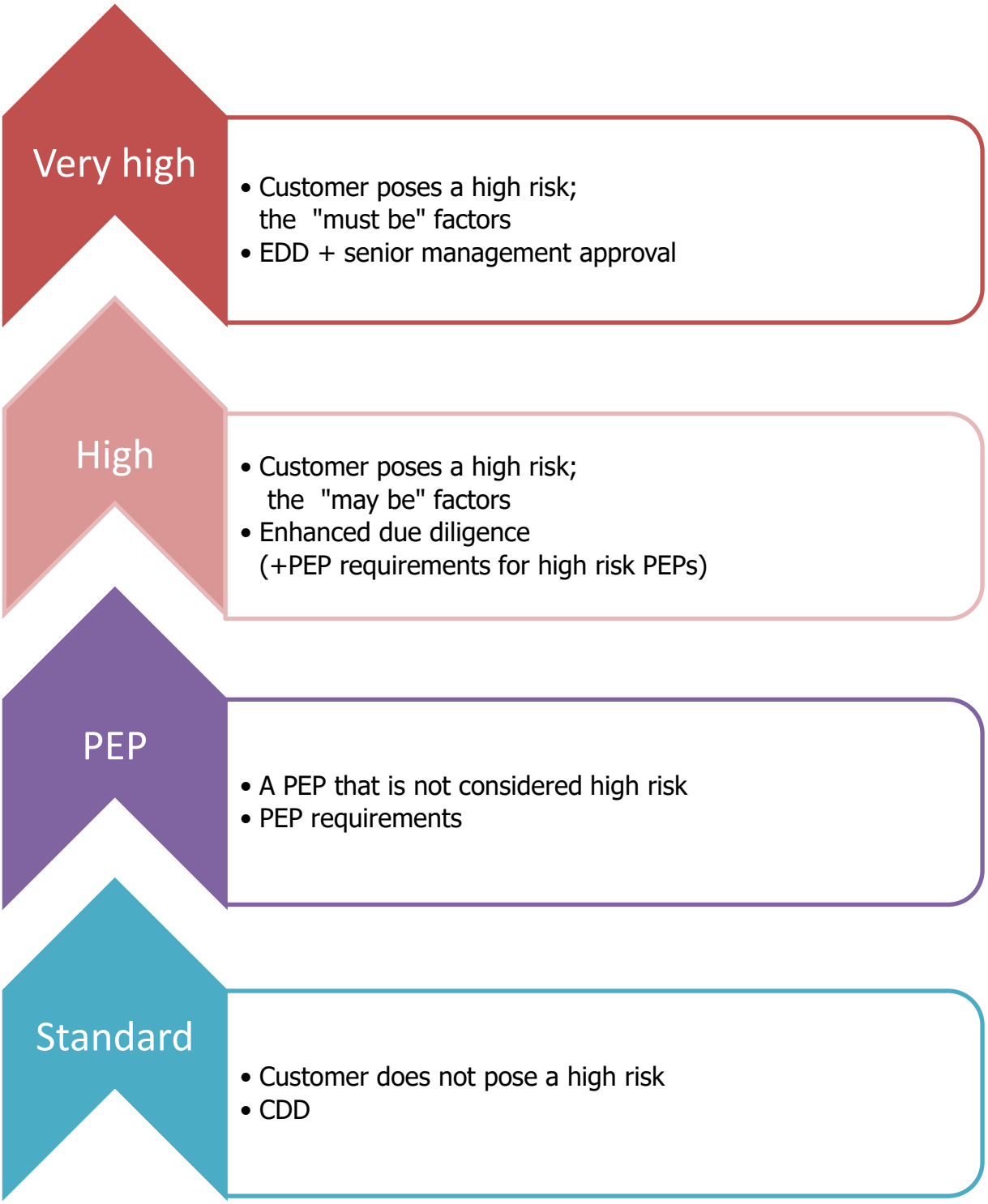
Whilst responsible gambling is not a Code requirement, consideration should be given to whether the use of multiple sources could also indicate that the customer may have a gambling problem.

3.7.3 Risk "Scores" and Customer Risk Summary

The Code requires a minimum of two customer risk categories; those that do and those that do not pose a higher ML/FT/PF risk.

As the Code requires additional measures for PEPs and for certain high risk customers and allows for simplified due diligence in certain low risk situations there are a possible 4 risk ratings. Operators may also consider a fifth category for "unacceptable risk"; a classification for customers that exceed the business risk appetite and whose business is not accepted or continued. Operators must be able to clearly separate out risk ratings in line with Code requirements and apply the correct standard for a particular risk rating, see example below.

[3] https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2


Very high
• Customer poses a high risk;
the "must be" factors
• EDD + senior management approval
High
• Customer poses a high risk;
the "may be" factors
• Enhanced due diligence
(+PEP requirements for high risk PEPs)
PEP
• A PEP that is not considered high risk
• PEP requirements
Standard
• Customer does not pose a high risk
• CDD

Key Messages

Risk Factors - Key Messages

- ✓ The following could be higher risk indicators for ML/FT/PF:
  - The customer and operator do not meet face-to-face
  - Transactions carried out on a time-sensitive basis
  - Transactions carried out at multiple premises
  - Multiple accounts
  - Multiple brands or sites
  - Cash or other anonymous payment method
  - Payment methods that are not well AML/CFT regulated
  - Multiple deposit sources
  - Different method used to deposit and withdraw
  - Rapid, repeat transactions
  - Transfer of value between customers
- ✓ Matters that may be high risk:
  - Activity in a jurisdiction the operator deems to be a higher risk of ML/FT/PF
  - Customers resident or located in a "List B" jurisdiction
  - Activity in a "List A" or "List B" jurisdiction
  - A situation that by its nature presents an increased risk of ML/FT/PF
  - A customer that is PEP
  - Nominee shareholders or shares in bearer form
  - The provision of high risk products
  - High-net-worth individuals
  - Legal arrangements
  - Persons performing prominent functions for international organisations
  - Sporting professionals betting on sports
  - Customers that use multiple sources to fund their gambling
- ✓ The Code requires a minimum of two customer risk categories; those that do and those that do not pose a higher ML/FT/PF risk
- ✓ Operators must be able to identify customers that have been assessed as posing a higher risk of ML/FT/PF and demonstrate that the necessary CDD, EDD or other additional requirements have been met.

Part 4: Customer Due Diligence (Paragraph 9 – 15)

The Code requirements are designed to achieve the following by using a risk-based approach:

- Deter criminals from laundering money or financing terrorism;
- Detect any suspicious activity;
- Assist the authorities in investigating and apprehending criminals; and
- Seize criminal or terrorist property.

The requirement for identity to be provided and verified therefore has this dual purpose – deterrence and detection.

A criminal is less likely to use a framework that obliges him/her to provide information that could positively identify them and link them with crime; the requirement to disguise identity and acquire a compatible financial set-up is an additional cost, which makes crime more expensive.

4.1 CDD Terminology

An understanding of the following terms is essential for compliance with the Code requirements:

"Customer due diligence" (CDD) is an umbrella term used to describe the various measures required to be carried out including, for standard risk customers, identification, verification of identity, SOF and ongoing monitoring.

"Enhanced due diligence" (EDD) is the term used to describe measures that are required to be carried out for higher risk customers in addition to the CDD requirements required for standard risk customers.

"PEP requirements" is the term used to describe measures (which vary slightly to EDD measures) that must be carried out for politically exposed persons in addition to the CDD requirements for standard risk customers.

"Identification" is the collection of information required to establish a person's identity (customer or any other subject you may be dealing with). The information required will vary depending on the legal status of the person.

"Verification of identity" is the process of confirming that someone is who they say they are.

"Evidence of identity" is documentary evidence that corroborates and supports the validity of the information provided. Again, the documentation required will vary depending on the legal status of the person.

"SOF" refers to the origin of the money being used in a particular transaction and or a series of transactions and describes a customer's immediate SOF (i.e. the deposit method).

"SOW" is distinct from SOF and refers to the origin of the customer's entire body of wealth.

"Acting by way of business" describes a customer that is a legal person or arrangement or a natural person that is a professional gambler or an agent. Additional CDD requirements apply.

"Legal person" includes any body corporate or unincorporated capable of establishing a business relationship with a financial institution or of owning property (i.e. a company).

"Legal arrangement" includes express trusts and other arrangements with similar legal effect.

Two tables summarising the Code requirements for standard risk, PEPs and higher risk (EDD) are provided at -

- 4.2 Summary of requirements (all customers); and
- 4.3 Summary of requirements (customers that act by way of business or are legal persons/ arrangements/foundations)

As set out in paragraph 9 of the Code, the CDD requirements apply to ongoing customer relationships and occasional transactions that exceed the EUR 3,000 threshold.

4.2 Summary of Requirements (all customers)

	Monitor to see if exceeds threshold	Identify (incl beneficial owners)**	Source of funds	Verify identity	Ongoing monitoring	Senior management approval	Source of wealth	Enhanced ongoing monitoring	Additional identification*	Additional verification*	Research*	Additional monitoring*
	15(1) / 15(2)(b)	10(3)(a)	10(3)(b)	11	12 & 15	8(6) / 13(3)	13(4) / 14(2)(c)	13(5)	14(2)(a)	14(2)(b)	14(2)(d)	14(2)(d)
Occasional transaction under threshold	x											
Occasional transaction over threshold		x	x	x	x							
Ongoing customer relationship under threshold	x	x	x		x							
Ongoing customer relationship over threshold		x	x	x	x							
Customer is PEP		x	x		x	x	x	x				
Customer is high risk (or unusual activity)		x	x		x		x	x	x	x	x	x
Customer is very high risk		x	x		x	x	x	x	x	x	x	x

*Requirements that must be considered **(the GSC expects to see documented consideration in order to demonstrate compliance).**

** The Code mandates verification of identity when the transaction threshold is met however it is considered best practice to partially verify at first deposit or, where this is not feasible, consider conducting full verification prior to reaching the threshold.

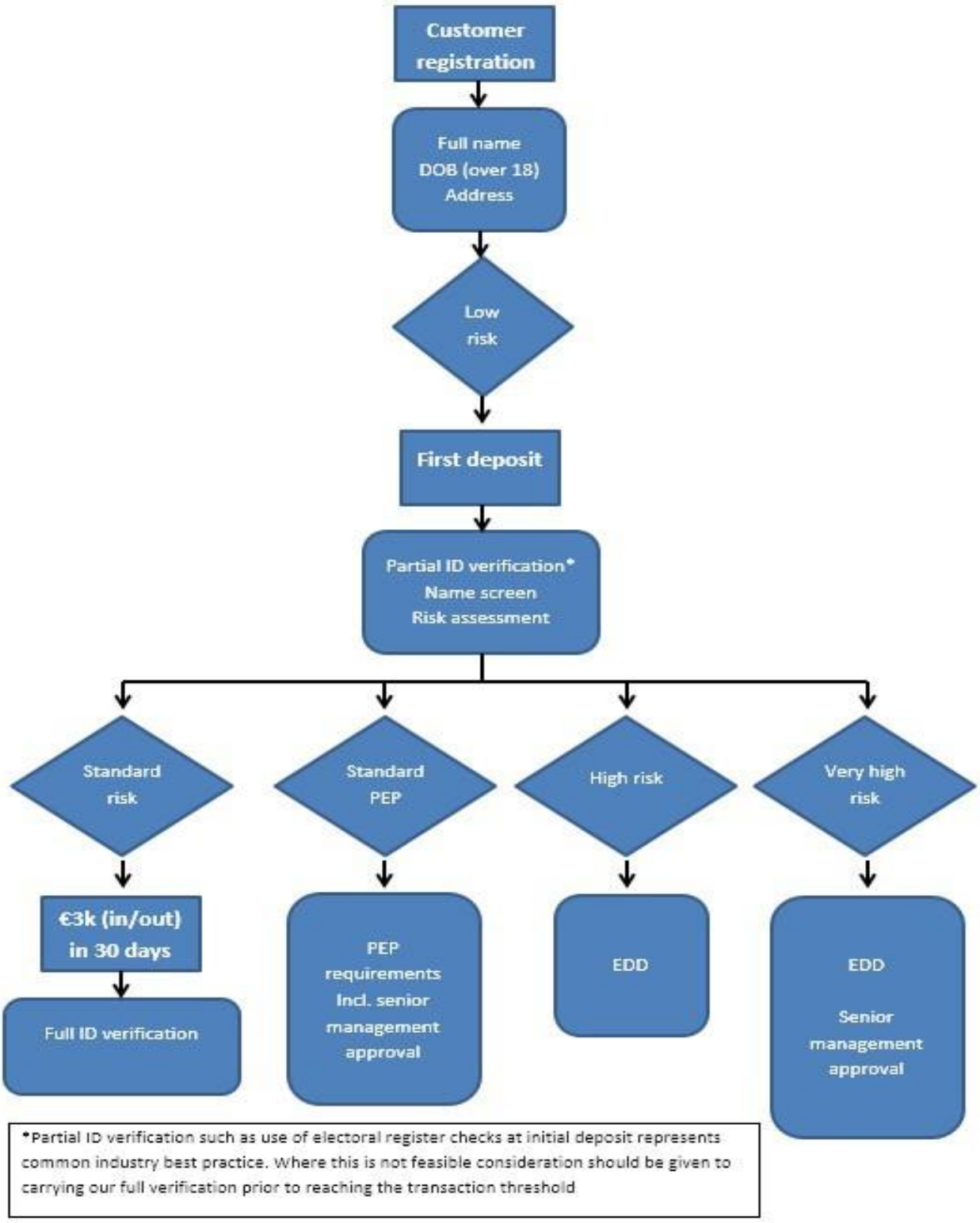
4.3 Summary of Requirements (customers that act by way of business or are legal persons/ arrangements/foundations)

The following requirements apply in addition to those that apply to all customers at 4.2 Summary of Requirements (all customers)

	ID&V beneficial owner(s)	Nature & purpose	Verify persons authority to act	ID&V person acting	Binding obligations	Ownership & control structure	ID trustees, controlling parties, known beneficiaries or instructing person	ID council members, equivalent, known beneficiaries, founder, other dedicator
	10(3)(c)(i)	10(3)(c)(ii)	10(4)(a)(i)	10(4)(a)(ii)	10(4)(a)(iii)	10(4)(a)(iv)	10(4)(b)	10(4)(c)
Customer acting by way of business (regardless of legal status)	x	x						
Customer that is a legal person (e.g. a company)	x	x	x	x	x	x		
Customer that is a legal arrangement (e.g. a trust)	x	x	x	x	x	x	x	
Customer that is a foundation	x							x

4.4 CDD Flow Chart

The chart below represents the process for obtaining the minimum required CDD for a standard retail customer from account opening (an ongoing customer relationship).



4.5 Occasional Transactions and New Customer Relationships (Paragraph 10)

The FATF Requirement

FATF Recommendation 10 states that businesses must identify the customer and verify a customer's identity using reliable, independent source documents, data or information.

Verification of identity should be conducted as soon as reasonably practicable but need not occur immediately if to do so would interrupt the normal course of business.

Where a delay occurs between identification and verification, the ML/FT/PF risks must be effectively managed.

FATF Recommendation 10 also states that when business relationships are formed, then an effort must be undertaken to identify and verify the beneficial owners of customers which are businesses, including developing an understanding of the ownership and control structure of the business. Furthermore, the purpose and intended nature of the business relationship must be understood for the purposes of ongoing monitoring.

The 2019 Code

10 Occasional transactions and new customer relationships

(1) An operator must in relation to each new ongoing customer relationship or transaction which exceeds the occasional transaction threshold, establish, record, maintain and operate appropriate procedures and controls in accordance with sub-paragraphs (3) and (4).

(2) Those procedures and controls must be undertaken—

(a) before an ongoing customer relationship is entered into or during the formation of that relationship; or

(b) before or as soon as reasonably practicable after an occasional transaction that exceeds the occasional transaction threshold is conducted.

(3) The procedures and controls referred to in sub-paragraph (1) are—

(a) identifying the customer and any known beneficial owner of the customer;

(b) the taking of reasonable measures to establish the source of funds;

(c) the taking of reasonable measures to establish whether the customer is acting by way of business and, if so—

(i) the verification of the identity of the customer and any known beneficial owner of the customer using reliable, independent source documents, data or information; and

(ii) the obtaining of information on the nature and intended purpose of the ongoing customer relationship.

(4) Without limiting sub-paragraph (3), an operator must—

(a) in the case of a customer that is a legal person or legal arrangement—

(i) verify that any person purporting to act on behalf of the customer is authorised to do so;

(ii) identify that person and verify the identity of that person using reliable, independent source documents, data or information;

(iii) obtain information concerning the person by whom and the method

by which, binding obligations may be imposed on the customer; and

(iv) obtain information to understand the ownership and control structure of the customer;

(b) in the case of a legal arrangement, identify—

(i) the trustees or any other controlling party;

(ii) any known beneficiaries; and

(iii) the settlor or other person by whom the legal arrangement is made or on whose instructions the legal arrangement is made or on whose instructions the legal arrangement is formed; and

(c) in the case of a foundation, identify—

(i) the council members (or equivalent);

(ii) any known beneficiaries; and

(iii) the founder and any other dedicator.

(5) Where the requirements of this paragraph are not met, the procedures and controls must provide that—

(a) the ongoing customer relationship or transaction must proceed no further;

(b) the operator must terminate any ongoing customer relationship; and

(c) the operator must consider making an internal disclosure.

GSC Guidance and Policy

What? This paragraph of the Code sets out the CDD requirements that apply to each customer establishing a new customer relationship or where an occasional transaction exceeds the EUR 3,000 threshold. It includes specific requirements that are applicable for online gambling operators (as such activity is not permitted to be carried out by terrestrial operators) regarding customers that are that are acting by way of business (which can include natural persons) and for legal persons and arrangements.

Two tables summarising the Code requirements are provided at -

- 4.2 Summary of requirements (all customers); and
- 4.3 Summary of requirements (customers that act by way of business or are legal persons/ arrangements/foundations).

A flow chat summarising the process for standard "retail" customers is provided at 4.4 CDD Flow chart.

Why? To establish the customer's identity and that of any beneficial owner or controller. This information is used to distinguish between different customers and can be used later to verify the customer and owner's identity.

When? The Code requires that this information (and verification, where applicable) is obtained prior to establishing an ongoing customer relationship (i.e. an account) or carrying out an occasional transaction over the EUR 3,000 threshold. Where this is not completed, the operator must not continue with opening the account or carrying out the transaction* and must consider making an internal disclosure (if they are suspicious).

*When a qualifying transaction is requested no withdrawals or deposits should be allowed until such time as satisfactory evidence is produced. Further gaming activity should only be permitted to continue for a period of 7 days, provided that the activity is monitored. This should allow the customer a reasonable amount of time to provide the necessary documentation. If the evidence is not produced within 7 days, the account should be locked.

Please note that paragraph 12 requires checks regarding the CDD of existing customers. For further detail, please see 4.7 Ongoing Customer Relationships (Paragraph 12). The GSC does not consider that these requirements apply to free-play modes (because no online gambling is occurring when they are played) but they are triggered if a free-play customer switches to a real-money play mode.

The awarding of bonuses or incentives to a customer's account does not make any free-play preceding the award of the bonus online gambling unless the bonus or incentive can be withdrawn as money (or money's worth such as crypto currency).

Who? Identification information should be supplied to the operator by the customer. Methods to verify the information will vary and can be based on documents provided by the customer, checks undertaken by staff or services provided by third parties. Please see 4.6 Verification of identity of customers (Paragraph 11) for further detail.

How? Typically, a customer is identified by completing a registration form (in person or online) or by a staff member recording information supplied by the customer verbally or by using identification documents. Information regarding the nature and purpose of a relationship or ownership and control are a little more complex - Please see 4.6 Verification of identity of customers (Paragraph 11) for further detail.

The information required to identify a customer depends on their legal status - see below.

Natural persons

As a minimum the following identification information should be obtained for natural persons (those marked * are explained in more detail below)

Full name
Date of birth
Residential address*
Full name, date of birth and residential address of any known beneficial owner*

And reasonable measures* to establish -

The source of funds*
If the customer is acting by way of business*

Best Practice

Consideration should also be given to establishing a customer's nationality and place of birth of the customer as this will be helpful for risk assessment and PEP/sanctions etc. screening (in order to discount false positives)

And, where acting by way of business –

Verification of the customer's identity
Identification and verification of identity of any known beneficial owner
Obtain information on the nature and purpose* of the business relationship

"**Residential address**" means a physical address where the customer resides. PO Boxes should not usually be accepted. The exception to this is where this is the norm for that country or location. Extra risk should be assumed if a 'care of' address is provided and these should only be accepted in compelling circumstances. The GSC would expect to see additional measures to mitigate the risk.

"**Known beneficial owner**" means a person or persons that the operators knows is the owner or controller of a customer and includes where the customer is acting on behalf of another person. The GSC expects operators to make enquiries to ascertain if a customer is acting on behalf of another person where their gambling activity or behaviour indicates that may be the case. For example, where a customer attempts to deposit using a third party's bank card or appears to be taking instructions from another person.

"**Reasonable measures**" means taking appropriate steps, which are commensurate with the ML/FT/PF risks.

"Source of funds" describes a customer's immediate source of funds (i.e. the deposit method).

Terrestrial Operators

Should consider carrying out CDD prior to when an occasional transaction exceeds the EUR 3,000 in 30 days threshold in line with their BRA and appetite.

Where customers gamble with significant sums of cash, the customer should be asked the source of the cash; did they obtain from another person in cash, withdraw from their bank, etc.?

"By way of business" describes gambling activities that business related rather than a recreational activity. Reasonable measures to establish this activity include making enquiries with the customer to ascertain whether the activity is being conducted by way of business where it appears that is the case - if the activity has the characteristics of business activity or the customer refers to themselves as a professional, agent, affiliate, etc.

"Nature and purpose of the business relationship" provides useful information for both risk assessment and transaction monitoring purpose and should include high level information on the anticipated value and volume of transactions.

Please see 4.9 Enhanced customer due diligence (Paragraph 14) for additional information that should be considered for higher risk customers.

Legal persons, arrangements and foundations

The requirements for customers that are not natural persons are more complex and can be represented as a series of steps-

Step 1: Identification information regarding the entity/arrangement –

Full name
Date of incorporation/establishment
Registered address (where applicable)

Step 2: Obtain the information to understand the ownership and control structure though company documents, structure charts, etc. (the documents used to verify identity should be referred to).

Step 3: Establish the following-

For legal persons…	For legal arrangements…	For foundations…
Ultimate owner or controller of 20% or more of the shares or voting rights	Trustees or any other controlling party	Council members (or equivalent)
Persons with ultimate effective control or influence over management (i.e. directors, powers of attorney, signatories)	Known beneficiaries*	Known beneficiaries*
	Settlor	Founder
	Any other person on whose instructions it was made or formed (in the case of a blind or dummy trust)	Any other dedicator*

Operators should also obtain information regarding classes of beneficiaries to enable them to have the capacity to establish the identity of a beneficiary in future and appropriately risk assess the relationship

A dedicator is any other person(s) with a sufficient interest, including a person who in the view of the High Court, can reasonably claim to speak on behalf of an object or purpose of the foundation and a person who the High Court determines to be a person with a sufficient interest under section 51(3) of the Foundations Act 2011 (or equivalent in non-Isle of Man established foundations).

Step 4: Identify (full name, date of birth, address) and verify the identity of -

The persons established in step 3
Any person purporting to act on behalf of the customer; any representative or agent who will correspond or make transactions for the customer.

Step 5: Complete the following steps

Verify that the person(s) purporting to act on behalf of the customer are authorised to do so (by verifying this with persons established in step 3).
Obtain information on the binding obligations of the persons identified at step 3 as set out in formal documents such as Memorandums and Articles of Associations, Power of Attorney, a signatory list plus a board resolution.
Take reasonable measures to establish the source of funds of the customer.

Key Messages

Occasional Transactions and New Customer Relationships - Key Messages

- ✓ The Code requirements are designed to achieve the following by using a risk-based approach:
  - Deter criminals from ML/FT/PF;
  - Detect any suspicious activity;
  - Assist the authorities in investigating and apprehending criminals; and
  - Seize criminal or terrorist property.
- ✓ The requirement for identity to be provided and verified therefore has this dual purpose – deterrence and detection.
- ✓ Understanding CDD terminology is essential for compliance with the Code.

4.6 Verification of Identity of Customers (Paragraph 11)

The FATF Requirement

FATF Recommendation 10 recommends that CDD includes requirements to verify a customer's identity using reliable, independent source documents, data or information.

Verification of identity should be conducted as soon as reasonably practicable but need not occur immediately if to do so would interrupt the normal course of business.

Where a delay occurs between identification and verification, the ML/FT/PF risks must be effectively managed.

The 2019 Code

11 Verification of identity of customers

(1) This paragraph applies—

(a) in respect of occasional transactions, on the first occasion on which an operator identifies that a customer has, or will, exceed the occasional transaction threshold; or

(b) when a customer has reached the qualifying transaction threshold.

(2) An operator must establish, record, maintain and operate appropriate procedures and controls which require verification of the identity of the customer and any known beneficial owner of the customer using reliable, independent source documents, data or information before carrying out any further occasional transactions or making a qualifying transaction.

(3) Where the requirements of this paragraph are not met, the procedure must provide that—

(a) the ongoing customer relationship or transaction must proceed no further;

(b) the operator must consider terminating any ongoing customer relationship; and

(c) the operator must consider making an internal disclosure.

GSC Guidance and Policy

What? Verification of identity is the term used to describe the steps that are taken to verify the identification information provided (e.g. name, date of birth, address).

Why? To establish that such a person truly exists and, using risk-based procedures, that the customer is truly the person they claim to be.

When? The Code requires identity to be fully verified -

- Prior to carrying out an occasional transaction that exceeds the occasional transaction threshold (EUR 3,000 in a single or several linked transactions);
- Prior to carrying out a transaction during an ongoing customer relationship that exceeds the threshold (EUR 3,000 in 30 days);
- Prior to establishing a relationship with customers that act by way of business;
- For higher risk customers (EDD also applies).

Best Practice

- Common industry best practice is for partial verification to be carried out at first deposit.
- Operators should consider their BRA and risk appetite to determine whether information should be verified sooner than the Code requires it
- Extra care should be taken when reviewing identity documents that are less familiar to staff members (e.g. foreign identity documents)

Who? The Code requirement is for the operator to verify using "reliable, independent source documents, data or information". This means that verification can be carried out by asking the customer to produce evidence or by the operator using information sources and electronic systems, subject to the guidance below. It is noted that the FATF currently takes a technology neutral stance.

How? The below identification information must be verified as a minimum with consideration given to verifying more information for higher risk customers (see 4.9 Enhanced customer due diligence (Paragraph 14).

Natural persons:

- Full name;
- Date of birth; and
- Residential address.

Legal persons:

- Name;
- Date of incorporation/establishment
- Registered address (where applicable); plus the
- Owners' and controllers' names, dates of birth and residential addresses.

Terrestrial Operators

Although some customers may be known to staff members the GSC does not consider being "known" to be sufficient evidence of verification.

Steps taken such as the use of electoral registers or ID documents should be recorded

Verification of identity is often a cumulative process with more than one source of information being used. The extent of checks undertaken should vary depending on the risks. Where obtaining physical documents, additional steps should be taken to ensure that they are valid documents and, that the customer is the true owner of the documents.

❖ **Natural persons - traditional methods (documents)**

Each of these traditional methods are considered to be "full verification" and meet the requirement to verify identity when a customer reaches the threshold.

Traditionally, verification of identity is carried out by having the customer evidence of their identity by producing or providing copies of physical documentation. This approach requires the customer to take the required action and is vulnerable to fraudulent or stolen documents, which are mitigated by checks to verify the evidence. Some customers may also struggle to produce acceptable proof of address documentation.

The following documents are considered "full verification" -

For name and date of birth (plus address when included in the document) –

- Passport;
- National identity card;
- Driving licence (although care should be given regarding international licences where checks may not be thorough);
- Proof of age card (where combined with additional checks).

For address –

- Recent (within 6 months) bank, building society, mortgage or credit card statement;
- Recent (within 6 months) rates, council tax or utility bill (other than for a mobile device except where the bill includes internet services to the residential address);
- Known lawyer's confirmation of property purchase or legal document recognising the title to the property;
- Letter from a person director or manager of an IOM employer, college or university (noting that customer consent must be sought before contacting the author to confirm validity);
- Physical verification of address made by sending letter requiring action from the customer to confirm receipt.

For all documents, the operator should check -

- That they appear valid (e.g. the correct layout and style);
- That they do not appear to have been tampered with and have not expired;
- The algorithm / "MRZ" on passports.

Consideration should also be given to requesting that documents are certified (and check the certifications) or a request a "selfie" or video chat to compare the individual's appearance with the image on the document.

❖ **Natural persons - non-traditional methods**

Of these non-traditional methods, only digital ID is considered "full verification" and meets the requirement to verify identity when a customer reaches the threshold. The other methods are suitable for use prior to reaching the threshold or as an additional check to be used with traditional methods or digital ID.

Non-traditional methods can be beneficial (e.g. potential to reduce costs, increase efficiencies and reduce human error) however they carry risks. Operators need to understand the architecture and governance of such methods in order to establish independence and reliability. A TRA will be required – please see 3.4 Technology risk assessment (Paragraph 7). Where possible a cumulative approach should be taken,

ideally combining both traditional and non-traditional methods, and multiple information sources.

Non-traditional methods alone can be used to verify address but should not be used to verify name and date of birth, except in the case of digital IDs that are established in line with national or internationally acceptable assurance frameworks.[4]

Examples of non-traditional methods –

- Digital IDs including biometric and distributed ledger technology (establishing official identity)[5];
- Use of electronic data sources that access information from electoral registers, passport issuing offices, driving licence issuing authorities, company registers, electoral rolls and other commercial databases;
- Social media (useful as additional information source but should never be used in isolation);
- Public domain information sources as news media or company registers;
- Facial / age recognition software;
- Third party CDD/EDD service providers (noting that such services are not usually regulated);
- Third party "identity wallet" providers that act as CDD introducer (noting that such services are not usually regulated). It should be noted that it is not acceptable for a third party to obtain and hold ID documents without the operator having access.

Best Practice

Operators must be mindful that providing information to third parties for verification may have GDPR implications

❖ **Legal persons, arrangements and foundations**

Customers that are legal persons, arrangements and foundations are acting by way of business and therefore pose an intrinsically higher ML/FT/PF risk. As such, customers must be required to produce documentary evidence of identity and address (where applicable) with consideration given to verifying the evidence though non-traditional methods such as company registers.

The identity of the owners and controllers of the entity or arrangements may be verified by traditional or non-traditional methods, in accordance with the risk posed.

Acceptable documents are –

- Certificate of Incorporation and/or Articles of Association (or equivalent, i.e. foundation charter);
- Certificate of Incorporation and/or Articles of Association (or equivalent, i.e. foundation charter);
- Trust Deed (or relevant extracts of Trust Deed);
- Recent (within 6 months) bank statement or utilities bill (address only);
- Latest annual return filed;
- Audited financial statements sourced from an independent public registry;
- Prepared accounts signed by a reporting accountant.

[4] Such as ISO or EIC standards, the US NIST framework or the EU's e-IDAS regulation
[5] Based on characteristics that establish a person's uniqueness in the population and is recognised by the state of residence for official purposes

Key Messages

Verification of Identity of Customers - Key Messages

- ✓ Verification of identity is the term used to describe the steps that are taken to verify the identification information provided to prove that the customer is truly the person they claim to be.
- ✓ The Code requires identity to be fully verified:-
  - Prior to carrying out an occasional transaction that exceeds the occasional transaction threshold (EUR 3,000 in a single or several linked transactions);
  - Prior to carrying out a transaction during an ongoing customer relationship that exceeds the threshold (EUR 3,000 in 30 days);
  - Prior to establishing a relationship with customers that act by way of business;
  - For higher risk customers (EDD also applies).
- ✓ Operators must verify using "reliable, independent source documents, data or information.
- ✓ Verification of identity is often a cumulative process with more than one source of information being used.
- ✓ The extent of checks undertaken should vary depending on the risks.

4.7 Ongoing Customer Relationships (Paragraph 12)

The FATF Requirement

FATF Recommendation 10 applies CDD requirements to both new and existing customers and requires businesses to conduct CDD on existing customers at appropriate times.

The 2019 Code

12 Ongoing customer relationships

(1) This paragraph applies in respect of ongoing customer relationships.

(2) An operator must, in relation to each ongoing customer relationship, establish, record, maintain and operate the procedures and controls specified in sub-paragraphs (4), (5) and (6).

(4) The procedures and controls must be undertaken during an ongoing customer relationship as soon as reasonably practicable and periodically thereafter.

(5) The procedures and controls referred to in sub-paragraph (2) are—

(a) an examination of the background and purpose of the ongoing customer relationship; and

(b) if satisfactory verification of the customer's and any known beneficial owner of the customer's identity has not already been obtained or produced, requiring such verification to be obtained or produced in accordance with paragraphs 10(3) (customers acting by way of business) and 11 (verification of identity of customers).

(6) An operator must record any examination, steps, measures or determination made or taken under this paragraph.

(7) Where the requirements of this paragraph are not met within a reasonable timeframe, the procedure must provide that—

(a) the ongoing customer relationship or transaction must proceed no further;

(b) the operator must consider terminating any ongoing customer relationship; and

(c) the operator must consider making an internal disclosure.

GSC Guidance and Policy

What? This paragraph requires operators to have and operate procedures to examine the background and purpose of the relationship and ensures that, satisfactory verification of identity is held; from the outset of the relationship and periodically thereafter.

If an operator is unable to obtain satisfactory information and verification within a reasonable timeframe, any transactions should proceed no further and consideration should be given to terminating the relationship, and where applicable, filing an internal disclosure.

Why? This is to ensure that existing relationships are in accordance with the requirements of the current Code and that the verification remains satisfactory. Where the nature and purpose of the relationship or verification of identity cannot be established, particularly where other unusual or risky factors or behaviours are noted, there may be cause to suspect ML/FT/PF.

When? For new relationships, the checks must be carried out as soon as reasonably practical and periodically thereafter. The frequency of periodical checks should be determined by the operator in accordance with the AML/CFT/CPF risk.

Who? How? The Code does not specify that these actions require the operator to take action. Checks may be carried out behind the scenes by staff members if they meet the requirements.

Key Messages

Ongoing Customer Relationships - Key Messages

- ✓ Operators must operate procedures to examine the background and purpose of the relationship and ensures that, satisfactory verification of identity is held; from the outset of the relationship and periodically thereafter.
- ✓ If an operator is unable to obtain satisfactory information and verification within a reasonable timeframe, any transactions should proceed no further and consideration should be given to terminating the relationship, and where applicable, filing an internal disclosure.
- ✓ For new relationships, the checks must be carried out as soon as reasonably practical and periodically thereafter. The frequency of periodical checks should be determined by the operator in accordance with the AML/CFT/CPF risk

4.8 Politically Exposed Persons (Paragraph 13)

The FATF Requirement

FATF Recommendation 12 states that PEPs should be subject to additional due diligence requirements including establishing their SOW, obtaining senior management approval to do business with PEPs and enhanced ongoing monitoring.

Such requirements are to apply to all foreign PEPs and higher risk domestic PEPs.

The 2019 Code

13 Politically exposed persons

(1) This paragraph applies to ongoing customer relationships and customers that have exceeded the occasional transaction threshold.

(2) An operator must establish, record, maintain and operate appropriate procedures and controls for the purpose of determining whether any of the following is, or subsequently becomes, a PEP—

(a) any customer;

(b) any natural person having the power to direct the activities of a customer; and

(c) any known beneficial owner of a customer.

(3) An operator must establish, record, maintain and operate appropriate procedures and controls for requiring the approval of its senior management before—

(a) any ongoing customer relationship is established with;

(b) any occasional transactions is carried out with; or

(c) any ongoing customer relationship is continued with,

a domestic PEP who has been identified as posing a higher risk of ML/FT or any foreign PEP.

(4) An operator must take reasonable measures to establish the source of wealth of—

(a) a domestic PEP who has been identified as posing a higher risk of ML/FT; and

(b) any foreign PEP.

(5) An operator must perform ongoing and effective enhanced monitoring of any ongoing customer relationship with—

(a) a domestic PEP who has been identified as posing a higher risk of ML/FT; and

(b) any foreign PEP.

(6) To avoid doubt, this paragraph does not affect the requirement for the operator to comply with the requirements of paragraph 14 (enhanced customer due diligence) where a PEP has been identified as posing a higher risk of ML/FT.

(7) Where the requirements of this paragraph are not met within a reasonable timeframe, the procedures and controls must require that—

(a) the ongoing customer relationship or occasional transaction must proceed no further;

(b) the operator must consider terminating any ongoing customer relationship; and

(c) the operator must consider making an internal disclosure.

(8) In this paragraph—

"domestic PEP" means a PEP who is or has been entrusted with prominent public functions in the Island and any family members or close associates of the PEP, regardless of the location of that PEP, those family members or close associates; and

"foreign PEP" means a PEP who is or has been entrusted with prominent public functions outside of the Island and any family members or close associates of the PEP, regardless of the location of that PEP, those family members or close associates.

3 Interpretation

"**politically exposed person**" or "**PEP**" means any of the following—

(a) a natural person who is or has been entrusted with prominent public functions ("P"), including—

(i) a head of state, head of government, minister or deputy or assistant minister;

(ii) a senior government official;

(iii) a member of parliament;

(iv) a senior politician;

(v) an important political party official;

(vi) a senior judicial official;

(vii) a member of a court of auditors or the board of a central bank;

(viii) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;

(ix) a high-ranking officer in an armed force;

(x) a senior member of an administrative, management or supervisory body of a state-owned enterprise; or

(xi) a senior member of management of, or a member of, the governing body of an international entity or organisation;

(b) any of the following family members of P, including—

(i) a spouse;

(ii) a partner considered by national law as equivalent to a spouse;

(iii) other known close personal relationships not covered by sub-paragraphs (i) or (ii) such as a partner, boyfriend or girlfriend;

(iv) a child;

(v) a spouse or partner of a child;

(vi) a brother or sister (including a half-brother or half-sister);

(vii) a spouse or partner of a brother or sister;

(viii) a parent;

(ix) a parent-in-law;

(x) a grandparent; or

(xi) a grandchild;

(c) any natural person known to be a close associate of P, including—

(i) a joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with P;

(ii) the sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of P;

(iii) a beneficiary of a legal arrangement of which P is a beneficial owner or beneficiary; or

(iv) a person in a position to conduct substantial financial transactions on behalf of P

GSC Guidance and Policy

What? The Code requires operators to put appropriate procedures and controls in place to determine whether a customer is, or becomes (therefore a requirement to do ongoing checks) a PEP. For foreign PEPs and higher risk domestic PEPs (based on the location of the role rather than residency) additional due diligence measures must be applied. The categorisation of PEPs also applies to close family members and associates.

Why? The measures aim to address risks posed by PEPs. The increased risk stems from the possibility of the PEP misusing their position and influence for personal gain through bribery or corruption. Family members and close associates of PEPs also pose a higher risk as PEPs may use family members and/or close associates to hide any misappropriated funds or assets gained through abuses of power, bribery or corruption. You can find further information Anti-Bribery and Corruption here: https://abc.gov.im/.

When? Checks must take place at customer take-on (either at registration or initial deposit) or where the occasional transaction threshold is reached and on an ongoing basis via continuous or periodic re-checking.

Who? The Code requires appropriate procedures and controls for identifying PEPs. The GSC does not consider asking a customer to declare whether they are or are not a PEP to be sufficient. Instead, the operator must take steps to establish the information, which should include the use of open source information or third party screening providers.

Please see 4.11 Name screening systems for guidance on selecting and using third party providers.

Terrestrial Operators

Likely to have low volumes of customers that exceed the EUR 3,000 threshold and require to be PEP checked.

Operators may use open source checks (e.g. Google searches) to when a customer exceeds the threshold and periodically (at least annually) thereafter to establish if they are, or become, a PEP.

How?

The Code PEP requirements cover two distinct stages; the identification of PEPs and the treatment of PEPs.

- **Identifying PEPs**
  - **PEP definition**

    Paragraph 3 of the Code (page 8) contains a list of posts and roles, which confer PEP status. People who either undertake such roles or are closely associated through business or family must also be treated as a PEP. The affected family members are also listed in the definition. Note that the Code requires "appropriate" measures therefore the GSC expects only reasonable attempts to be made to identify a customer that is a PEP due to family or business ties.

  - **Foreign vs domestic PEPs**

    The PEP requirements apply to all foreign PEPs and to domestic PEPs that pose a higher ML/FT/PF risk.

    The designation of "foreign" or "domestic" PEP is based on where the role of position is held rather than where the customer resides.

  - **Once a PEP, always a PEP?**

    The Code states that a PEP is a natural person that is or has been entrusted with a prominent public function.

    Guidance on Recommendation 12 issued by the FATF in 2013 states that the language is consistent with a possible open-ended approach i.e. "once a PEP, always a PEP". It goes on to suggest that the treatment of an individual who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. Consideration should be given to the risks posed (see below Risk Assessment section for further detail).

  - **Methods of identifying**

    Operators should determine the method used to identify PEPs based on the size, nature and risks of their business. Methods include -

    - Checking customer and beneficial owners' names against Government issued PEP lists;
    - Checking names against databases provided by third parties (see 4.11 Name screening systems for further detail on selecting a provider);
    - Consideration of other information that may indicate that a customer is a PEP e.g. source of wealth, contact details or open source checks carried out as part of EDD.

- **Treatment of PEPs**
  - **Risk assessment**

    An effective risk assessment is required because -

    - The PEP requirements apply to all foreign PEPs and high risk domestic PEPs; and
    - The extent of the measures carried out should be risk-based.

    Consideration should be given to the following factors -

    - The level of influence that the individual holds;
    - The scale of their public profile;
    - The level of seniority within their organisation or Government;
    - Authority over or access to state funds and assets, policies and operations;
    - Control over regulatory approvals, awarding of licences and concessions.
  - **Additional due diligence requirements**

    The additional due diligence measures that apply to PEPs are similar to but separate to EDD measures that must be carried out for high risk customers.

    Consideration of PEP status is required as part of a CRA as it is a factor that indicates a customer may be high risk (please see 3.7.2 Risk Factors: Matters that may be High Risk). Therefore, a PEP customer is likely to also be a high risk customer. In that case, both the PEP measures and EDD measures must be applied.

Requirement	PEP	EDD (for high risk)
Reasonable measures to establish source of wealth	Yes	Yes
Ongoing and effective enhanced monitoring	Yes	Yes
Senior management approval	Yes	Only for customers resident in a "List A" jurisdiction or that are the subject of an AML/CFT warning
Consider additional ID info	No	Yes
Consider additional verification of ID	No	Yes

For further detail on how to fulfil the requirements please see 4.9 Enhanced customer due diligence (Paragraph 14).

Key Messages

Politically Exposed Persons - Key Messages

- ✓ PEPs should be subject to additional due diligence requirements including establishing their SOW, obtaining senior management approval to do business with PEPs and enhanced ongoing monitoring.
- ✓ PEP requirements apply to all foreign PEPs and higher risk Domestic PEPs.
- ✓ Checks must take place at customer take-on (either at registration or initial deposit) or where the occasional transaction threshold is reached and on an ongoing basis via continuous or periodic re-checking.
- ✓ Operators must put appropriate procedures and controls in place to determine whether a customer is, or becomes (therefore a requirement to do ongoing checks) a PEP. For foreign PEPs and higher risk domestic PEPs (based on the location of the role rather than residency) additional due diligence measures must be applied. The categorisation of PEP also applies to close family members and associates.
- ✓ The increased risk stems from the possibility of the PEP misusing their position and influence for personal gain through bribery or corruption. Family members and close associates of PEPs also pose a higher risk as PEPs may use family members and/or close associates to hide any misappropriated funds or assets gained through abuses of power, bribery or corruption.
- ✓ An effective risk assessment is required as PEP requirements apply to all foreign PEPs and high risk domestic PEPs.
- ✓ The extent of the measures carried out should be risk-based.

4.9 Enhanced Customer Due Diligence (Paragraph 14)

The FATF Requirement

FATF Recommendation 1 and the related Interpretive Note require due diligence measures to be carried out using a risk-based approach. The Interpretive Note to Recommendation 10 (Customer Due Diligence) goes on to state that businesses should be required to carry out enhanced measures for higher risk customers and provides examples of such measures.

The 2019 Code

14 Enhanced customer due diligence

(1) An operator must establish, record, maintain and operate appropriate procedures and controls in relation to undertaking enhanced customer due diligence.

(2) Enhanced due diligence includes—

(a) considering whether additional identification information needs to be obtained and, if so, obtaining such additional information;

(b) considering whether additional aspects of the identity of the customer and any known beneficial owner need to be verified by reliable independent source documents, data or information, and, where it is considered necessary, the taking of reasonable measures to obtain such additional verification;

(c) the taking of reasonable measures to establish the source of wealth of a customer;

(d) the undertaking of further research, where considered necessary, in order to understand the background of a customer and the customer's business; and

(e) considering what additional ongoing monitoring should be carried out in accordance with paragraph 15 (ongoing monitoring) and carrying it out.

(3) An operator must conduct enhanced customer due diligence—

(a) where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment;

(b) in the event of any unusual activity; and

(c) in the event of any suspicious activity, unless the operator reasonably believes conducting enhanced customer due diligence will tip-off the customer.

(4) Where the requirements of this paragraph are not met within a reasonable timeframe, the procedures and controls must provide that—

(a) the ongoing customer relationship or occasional transaction must proceed no further;

(b) the operator must consider terminating any ongoing customer relationship; and

(c) the operator must consider making an internal disclosure.

GSC Guidance and Policy

What? EDD is the umbrella term used to describe measures that must be carried out in addition to "standard" CDD for higher risk customers, in the event of unusual activity or in the event of suspicious activity except where the operator reasonably believes this may tip-off the customer.

Why? The FATF Recommendations require due diligence to be risk-based. This includes conducting enhanced measures in higher risk scenarios. The aim of this is to focus AML/CFT/CPF resource on the customers that pose the highest risks rather than a one-size-fits-all approach.

When? The Code requires EDD to be carried out within a reasonable timeframe* of the customer being assessed as high risk, in the event of any usual activity or in the event of any suspicious activity. Where this does not occur the transaction must proceed no further and consideration must be given to terminating the relationship and making an internal disclosure to the MLRO (if suspicious of ML/FT/PF) (see 5.7 Reporting procedures, Internal disclosures and External disclosures (Paragraph 22, 23, 24).

**No further withdrawals or deposits should be allowed until satisfactory EDD is carried out. Further gaming activity should only be permitted to continue for a period of 7 days for high risk or in the event of any unusual activity provided that the activity is monitored. This should allow the customer a reasonable amount of time to complete the EDD process, including, where necessary, the customer providing additional information or verification. If satisfactory EDD is not completed within 7 days or where the activity is suspicious, the account should be locked*.

Who? The Code requires senior management approval for very high risk customers - those that are resident in a "List A" jurisdiction or that are the subject of an AML/CFT warning. For other high risk customers EDD may be carried out by staff members and may require the customer to provide additional information or verification. Operators should consider, in line with their own risk appetite, whether additional checks (e.g. 4 eyes checks) should be carried out on EDD. Operators may commission third parties to undertake elements of the EDD process but must carefully review the information provided to ensure that they are satisfied. The operator remains responsible for compliance with the Code.

Best Practice

Operators must be mindful that providing information to third party providers may have GDPR implications.

How? EDD comprises 5 elements in addition to standard CDD.

4 of those 5 elements require "**consideration**" by the operator. Ideally, each high risk customer should be treated on a case-by-case basis; risk factors reviewed, understood, and appropriate measures taken to address the risk posed by the customer. Consideration may also be demonstrated through detailed and effective operational procedures that advise staff what measures to carry out in various circumstances.

- **1 - Additional identification information (consider if)**

  Obtaining additional identification information is particularly useful where risks relate to the possibility of stolen or fake identity. It can also assist in confirming or discounting potential PEP, sanctions or negative press matches or when conducting open source research.

Examples of additional information include:

Natural Person	Legal Person
• Middle names • Aliases • Former names • Nationality(ies) • Gender • Official person identification number • Occupation • Name of employer • Previous address	• Trading name • Principle place of business • Mailing address (if different from registered address) • Whether listed and, if so, where • Name of regulator (if any)

- **2 - Additional verification (consider if)**

  Consideration should also be given to carrying out additional measures to verify the customer's identification information as part of standard CDD and to verifying additional information provided as part of the EDD.

  Examples of additional verification methods include:

Natural Person	Legal Person
• Obtaining additional ID documents such as driver's licence, student card or bus pass • A telephone or video call with the customer • Request a selfie of the customer holding their ID or outside their home address (which can then be verified using google maps, etc.) • Verify information supplied using internet searches and open source databases (e.g. Facebook, LinkedIn)	• A telephone or video call with the directors • Verify information supplied using internet searches and open source databases (e.g. Facebook, LinkedIn, Google) • If possible, verify information using companies and beneficial ownership registers

- **3 - Source of wealth (reasonable measures)**

  SOW is distinct from SOF and describes the origins of a person's financial standing or total net worth (i.e. the activities that generated a person's funds and property). What constitutes "reasonable measures to establish" will vary depending on the risks

associated with the customer and the value of their transactions.

The Code does not require operators to contact a customer to establish their SOW. In some cases, it may be appropriate for checks to be carried out behind the scenes by using (and recording) information available in the public domain. Useful information can often be found using corporate social netwoking sites such as LinkedIn.

When determining what is "reasonable" an operator should consider –

- The factors that resulted in the customer being deemed high risk;
- The value of the customer's transactions; and
- The period over which the the transactions occurred - if over a short period of time consider what the value would be if it were to continue at this level for a year.

When reviewing SOW information the operator should consider -

- How reliable or independent the source of the information is;
- How plausible the information is; and
- How this compares to the customer's activity.

A diagram showing a graduated approach to SOW checks is provided below.

Source of Wealth & Responsible Gambling

- *For the vast majority of customers gambling is enjoyed as a recreational activity*
- *SOW checks should be considered from both an AML/CFT/CPF and a responsible gambling point of view*
- *Gambling of significant portions of income, frequent use of overdrafts and use of payday loans should prompt interaction with the customer*

- **4 - Background research (consider if)**

For high risk customers, particularly those with large or unusual transactions or where there are concerns over the SOW, the operator should make efforts to establish whether the customer has been accused or convicted of a proceeds generating crime (e.g. theft, fraud).

This can be achieved using open source information, name screening for negative press or by commissioning third party reports.

Staff members tasked with carrying out open source checks should be trained in how to conduct effective internet searches, made aware of the particular websites or search engines that are available for their customer base and, where applicable, access to translation services.

In addition to carrying out checks on the customer, checks should also be considered for their person(s) or entity(ies) from which their funding derives.

- **5 - Additional ongoing monitoring (consider how)**

Paragraph 15 of the Code requires all ongoing monitoring to be risk-based, see 4.10 Ongoing monitoring (Paragraph 15). This paragraph covers the ongoing monitoring of both a customers' CDD/EDD and their transactions.

Operators should concentrate their ongoing monitoring efforts on high risk customer by conducting (and recording) more frequent or more extensive checks on them. Staff

members tasked with carrying out the monitoring should be trained and understand the relevant risk factors.

Depending on the risk factors that resulted in the customer being deemed high risk the operator may consider monitoring additional areas, such as -

- Seeking rationale and evidence for any changes in the source or destination of funds;
- Monitoring the IP address or devices used to log into the customer's account;
- Periodic or ongoing open source checks for negative press.

A graduated approach to SOW checks:

Where a customer is deemed higher risk (i.e. due to country of residence) and transacts only minimal amounts (i.e. £10s per month) it would be acceptable for the operator to determine that there would be little value in carrying out checks or contacting the customer to establish the SOW. In such cases this decision must be documented and the activity monitored in case it increases to a level where checks should be carried out.

Where a high risk customer carries out low-moderate value transactions (i.e. £100s per month) it would be acceptable for the operator to conduct SOW checks using open source/public domain information provided that it seems reliable, plausible and in line with the customer's activity.

Where satisfactory public domain information is not available or the customer transacts moderate amounts the operator should contact the customer to enquire about their SOW. Vague descriptions should not be accepted. For example, "salary" is not sufficient and more detail such as employer name, role and annual salary should be obtained. Again the operator should consider how plausible this information is and how it compares to the customer's activity.

Where a high risk customer's SOW information is not satisfactory or where their activity is significantly higher than an average customer, the SOW information should be verified, where possible, using both open source information and supporting evidence (e.g. bank statements, pay slips). The operator should consider having a senior manager, MLRO or AML/CFT Compliance Officer review the SOW. If not satisfied the transaction or relationship must proceed no further. Consideration should be given to filing a SAR.

Key Messages

Enhanced Customer Due Diligence - Key Messages

- ✓ EDD is the umbrella term used to describe measures that must be carried out in addition to "standard" CDD for higher risk customers, in the event of unusual activity or in the event of suspicious activity except where the operator reasonably believes this may tip-off the customer.
- ✓ The Code requires EDD to be carried out within a reasonable timeframe and transactions frozen until satisfactory EDD is carried out. Further gaming activity should only be permitted to continue for a period of 7 days for high risk or in the event of any unusual activity provided that the activity is monitored.
- ✓ The Code requires senior management approval for very high risk customers - those that are resident in a "List A" jurisdiction or that are the subject of an AML/CFT warning.
- ✓ EDD comprises of 5 elements in addition to standard CDD:
    - Additional identification information (consider if)
    - Additional verification (consider if)
    - SOW (reasonable measures)
    - Background research (consider if)
    - Additional ongoing monitoring (consider how)

4.10 Ongoing Monitoring (Paragraph 15)

The FATF Requirement

FATF Recommendation 10 includes a requirement for businesses to conduct ongoing due diligence including scrutiny of transactions to ensure consistency with their knowledge of the customer. This requirement should be met using a risk-based approach.

The 2019 Code

15 Ongoing monitoring

(1) An operator must take reasonable measures to identify a customer involved in an occasional transaction that exceeds the occasional transaction threshold.

(2) An operator must perform ongoing and effective monitoring, including carrying out—

(a) a review of information and documents held for the purpose of customer due diligence to ensure that they are up-to-date, accurate and appropriate, in particular where that transaction or relationship poses a higher risk of ML/FT;

(b) appropriate scrutiny of transactions and other activities to ensure that they are consistent with—

(i) the operator's knowledge of the customer, the customer's business and risk profile and source of funds for the transaction;

(ii) the business risk assessment carried out under paragraph 6 (business risk assessment);

(iii) any relevant technology risk assessment carried out under paragraph 7 (technology risk assessment); and

(iv) the customer risk assessment carried out under paragraph 8 (customer risk assessment);

(c) monitoring whether the customer or any known beneficial owner is listed on the sanctions list.

(3) Where an operator identifies any unusual activity in the course of an ongoing customer relationship or occasional transaction, the operator must, within a reasonable timeframe—

(a) perform appropriate scrutiny of the activity;

(b) conduct enhanced customer due diligence; and

(c) consider whether to make an internal disclosure.

(4) Where an operator identifies any suspicious activity in the course of an ongoing customer relationship or occasional transaction, an internal disclosure must be made in accordance with paragraph 23 (internal disclosures).

(5) The extent and frequency of any monitoring under this paragraph must be determined—

(a) on the basis of materiality and risk of ML/FT;

(b) in accordance with the risk assessments carried out under Part 3 (Risk-based Approach); and

(c) having particular regard to whether a customer poses a higher risk of ML/FT.

(6) An operator must record any examination, steps, measures or determination made or taken under this paragraph.

GSC Guidance and Policy

What? Ongoing monitoring describes the ongoing or periodic customer checks that aim to ensure ongoing compliance with the Code requirements, to detect changes in customer risk factors or unusual activity. It comprises three parts -

- Reviews of CDD/EDD to check that the information and documentation held is accurate, up-to-date and appropriate;
- Scrutinising of transactions (both financial and gambling) to ensure that they are consistent with the CDD/EDD; and
- Monitoring whether the customer or any beneficial owner is listed on the sanctions list (see Sanctions and Proliferation for more detail).

Why? The primary focus of ongoing monitoring is to identify unusual activity, which requires further scrutiny and EDD to be conducted.

"unusual activity" means any activity including the receipt of information during the course of an ongoing customer relationship, occasional transaction or attempted transaction where—

(a) the transaction has no apparent economic or lawful purpose, including a transaction which is—

(i) complex;

(ii) both large and unusual; or

(iii) of an unusual pattern;

(b) the operator becomes aware of anything that causes the operator to doubt the identity of a person it is obliged to identify;

(c) the operator becomes aware of anything that causes the operator to doubt the good faith of a customer or known beneficial owner of a customer

The requirement for accurate, up-to-date and appropriate CDD/EDD can -

- Assist with risk assessment considerations - CRA, BRA and NRA;
- Establish what would appear normal or expected for a customer or category of customer;
- Deter criminals from using the regulated gambling sector;
- Be used by the authorities to track and locate criminals.

When? The Code requires ongoing monitoring to be risk-based. The frequency and veracity of checks should be increased for higher risk customers.

❖ CDD/EDD Reviews

CDD information may change due to circumstances (e.g. marriage, name change, change of address) but could also be due to a slipup by a criminal (supply of incorrect details that differ from false identity supplied for example). Such changes should be re-verified in line with the requirements set out in 4.6 Verification of identity of customers (Paragraph 11).

Where ID documents are provided to verify a customer's identity there is no GSC expectation that they are requested again each time the customer transacts over the EUR 3,000 threshold if the CDD information has not changed and that documents have not expired.

The GSC expects operators to review the CDD/EDD held for high risk customers at least annually to ensure that the information remains sufficient - this includes information on the SOF and SOW. Reviews should also be conducted for any customer at a "trigger

event" including where transaction monitoring identifies unusual activity or where there is a material change to in customer risk factors.

- **Transaction monitoring**

  The Code does not stipulate the timing or frequency of transaction monitoring, only that it must be risk-based. As the monitoring aims to identify unusual activity (see above definition) which includes large transactions patterns of activity it is prudent for monitoring to include reviews of transactions over a certain threshold or during a reporting period. For example, an operator could establish daily, weekly and monthly transaction reports and scrutinise those where customers exceed a certain volume or value of deposits. Lower thresholds should be adopted for high risk customers.

Who? Operators should consider, in line with their risk-based approach, having monitoring checked by managers, the MLRO or AML/CFT Compliance Officer, particularly in relation to very high risk customers or unusual activity.

Unusual activity requires further scrutiny of transactions, which may include asking the customer for their rationale for carrying out the activity or further information or evidence of the SOF or SOW.

Responsible Gambling

- *For the vast majority of customers gambling is enjoyed as a recreational activity.*
- *Financial and gambling transactions should be considered from both an AML/CFT and a responsible gambling point of view.*
- *Significant changes in activity (e.g. chasing losses, taking greater risks, multiple deposit methods) should prompt an interaction with the customer.*

How? Ongoing monitoring can be carried out with the assistance of technological solutions. Remember that such systems must be risk-assessed (see 3.4 Technology risk assessment (Paragraph 7)).

Regardless of whether monitoring is carried out manually or using technology all monitoring efforts, including investigation work and customer interactions, must be recorded. For example, where a system is used to flag transactions over a certain value notes should be recorded to demonstrate who reviewed the "alert", when, what action they took and why.

Reports or thresholds for alerts should be set up and reviewed by those with a good understanding of the operator's BRA, relevant typologies and red flags.

Terrestrial Operators

- The Code requires operators to take reasonable measures to identify customers that exceed the EUR 3,000 (in a single or several linked transactions) limit.
- After the threshold is met the customer must be subject to ongoing monitoring.
- Staff members should pay attention to customers that place larger than average bets and should record information so that it may be shared with colleagues including those at different branches.
- Until such time as the customer's identity is known, a 'nom de plume' system may be used.
- Subject to GDPR requirements, sources such as security camera footage and handwriting comparisons (on betting slips) can assist.

Key Messages

Ongoing Monitoring - Key Messages

- ✓ The primary focus of ongoing monitoring is to identify unusual activity, which requires further scrutiny and EDD to be conducted.
- ✓ The Code requires ongoing monitoring to be risk-based. The frequency and veracity of checks should be increased for higher risk customers.
- ✓ CDD information may change due to circumstances (e.g. marriage, name change, change of address) but could also be due to a slipup by a criminal (supply of incorrect details that differ from false identity supplied for example). Such changes should be re-verified.
- ✓ The GSC expects operators to review of the CDD/EDD held for high risk customers at least annually to ensure that the information remains sufficient.
- ✓ Transaction monitoring should be risk-based.
- ✓ Unusual activity requires further scrutiny of transactions.
- ✓ All transaction monitoring efforts should be recorded.
- ✓ Reports or thresholds for alerts should be set up and reviewed by those with a good understanding of the operator's BRA, relevant typologies and red flags.

4.11 Name Screening Systems

IT systems can provide highly effective method for screening names (customer, beneficial owner, SOF, etc.) to detect PEPs, sanctioned persons or persons that are the subject of negative public domain information (e.g. charged with a proceeds generating crime).

Operators should carefully consider which providers they contract with, how the systems are set up or customers and how alerts are handled, including from a GDPR perspective. Operators should have a good understanding of the system and its parameters rather than placing total faith in the system provider.

Considerations should include -

- Whether the system provides functionality for a manual check (i.e. you type in a name to search) or automated (i.e. you upload a list of names or it runs against your database);
- Whether the system provides a one-off check, periodic or real time monitoring;
- Where the system pulls information from (e.g. public databases, internet searches, manual research);
- What PEP definition is used in the system and how this matches up to the Code;
- Which countries are covered (e.g. does it include the US OFAC sanctions list?);
- How your data is used (e.g. does it go to their servers, are there data protection issues?);
- Whether the system provides audit trail functionality (i.e. recording the outcome of investigations, discounting of false positives, etc.);
- Whether there is functionality to screen against name and other data (i.e. date of birth) in order to reduce false positives;
- Whether the screening includes negative press screening (e.g. public domain information about criminals, etc.);
- Whether there is the ability to customise settings (e.g. types of negative press you care about, how close a name match must be to alert, etc.);
- Whether you need functionality to check foreign language characters on registration details (e.g. Chinese, Cyrillic, etc.)?

Reminder: In order to meet the Code PEP requirements and in order to prevent a breach of TOCFRA, PEP and sanctions checks should be carried out at customer take-on (for ongoing customer relationships), at occasional transaction threshold and during a customer relationship, either periodically or perpetually. All AML/CFT/CPF systems and procedures must be risk-based and may vary depending on the size and nature of the operator.

Part 5: Record Keeping and Reporting

This section primarily focused on the Code requirements regarding record keeping however, some reference is also made to General Data Protection Regulations 2018 (GDPR).

5.1 Record Keeping (Paragraph 16)

The FATF Requirement

FATF Recommendation 11 deals specifically with record keeping and reporting requirements. The elements that affect operators are -

- Businesses should be required by law to retain records on their customers for at least 5 years;
- All CDD records including evidence captured to verify identify must be retained;
- Records must be kept that allow the customer's activity and individual transactions to be reconstructed;
- The types and amounts of currently used in the transactions must be recorded; and

Records of the results of analysis performs on evidence must be retained, including the analysis performed on variances in the volumes or patterns of transactions.

The 2019 Code

16 Record keeping

An operator must keep—

(a) a copy of the documents obtained or produced under Part 3 (Risk-based Approach) and Part 4 (Customer Due Diligence) (including identification information, account files, business correspondence records and the results of any analysis undertaken) or information that enables a copy of such documents to be obtained;

(b) a record of all transactions carried out in the course of gambling business in the regulated sector, including identification information, account files, business correspondence records and the result of any analysis undertaken; and

(c) all such other records as are sufficient to permit reconstruction of individual transactions and compliance with this Code.

GSC Guidance and Policy

What? This paragraph of the Code details the types of records that must be kept regarding AML/CFT/CPF in accordance with the retention periods mandated in Paragraph 17 – see 5.2. Record retention (Paragraph 17).

The following records must be kept by or available to the operator –

- CDD documents (photo ID, proof of address, SOW evidence, etc.);
- Account files (records and notes about the customer and their activities);
- Business correspondence (emails, notes of phone calls, etc.);
- Transactions records (further detail is provided below);
- Any analysis undertaken on CDD or transactions

and, importantly -

- Other records to demonstrate compliance with the Code – this includes all AML/CFT/CPF activities such as risk assessments, procedures, investigation of unusual or suspicious transactions, staff vetting and training.

Why? Records are required to be kept because –

- Competent authorities may wish to obtain them to assist with investigations or information exchanges with their counterparts;
- For use in transaction monitoring and risk assessment;
- To demonstrate that the operator is compliance with the Code.

When? Record keeping requirements apply from when an operator is licenced (in respect of procedures, BRA, etc.) and throughout all customer relationships. This includes records that relate to attempted transactions and customers that attempt to open an account but are refused.

Who? All staff members should be made aware of the requirement to record information. The GSC expects all policies and procedures for record keeping to be approved by the operator's Data Protection Officer to ensure compliance with GDPR as well as the Code.

How? The Code does not mandate how records should be kept with the exception of registers required for internal disclosures, external disclosures and ML/FT enquiries (see 5.2. Record retention (Paragraph 17). However, operators should be mindful that AML/CFT/CPF records are confidential documents and must be kept secure when not being processed. Access to more sensitive matters such as those detailed in the registers should be restricted to only those that require it.

Records should be kept in a format that makes it possible to locate, retrieve and understand them.

Care should be taken if record keeping is outsourced. The operator must always be confident it can retrieve the records within a satisfactory timescale, that the records are being held securely against internal and external misuse and that a contingency exists to safeguard the records in the event the third party ceases to operate or a dispute arises.

Transactions that must be recorded and retained include:

- Deposits made by customers acting by way of business to player wallets/accounts held by operators;
- Withdrawals made by operators to bank cards, bank accounts and other externally held instruments;

as well as-

- Gaming/betting activity;
- Business payments, reconciliations, etc. made to operators by customers acting by way of business;
- The commitment by customers of deposits to wagering (e.g. bets, stakes on games, the purchase of tickets in a lottery, etc.) even if they are reversed or cancelled before the outcome is known;
- The crediting of winnings from games, bets, etc. to customer wallets/accounts held by operators;
- Redeemed bonuses credited to customers by operators; and
- Player-to-player transfers using internal transfer mechanisms supplied to players by

operators.

Gaming/betting records should include game times, stakes, wins, losses odds/types of games and full transactional history and can be utilised—

- To detect unusual activity for AML/CFT/CPF purposes;
- For responsible gambling and fairness/complaints.

Transaction data must be complete to the extent it allows for the identification of the source of a payment as well as the payment's recipient. The GSC also requires that the type of currency be noted in the transaction data or where the currency type is homogenous, that the currency used in the records can be identified.

Transaction data must be complete to the extent it allows competent authorities to construct an audit trail for suspected ML/FT/PF.

Key Messages

Record Keeping - Key Messages

- ✓ Operators are required by the Code to keep or make available to the operator the following:
  - CDD documents (photo ID, proof of address, SOW evidence, etc.);
  - Account files (records and notes about the customer and their activities);
  - Business correspondence (emails, notes of phone calls, etc.);
  - Transactions records (further detail is provided below);
  - Any analysis undertaken on CDD or transactions; and
  - Other records to demonstrate compliance with the Code.
- ✓ Record keeping requirements apply from when an operator is licensed (in respect of procedures, BRA, etc.) and throughout all customer relationships.
- ✓ All staff members should be made aware of the requirement to record information.
- ✓ Records should be kept in a format that makes it possible to locate, retrieve and understand them.

5.2. Record Retention (Paragraph 17)

The FATF Requirement

FATF Recommendation 11 requires records on customers to be retained for at least 5 years after the last transaction or the termination of the relationship.

The Code 2019

17 Record retention

(1) An operator must keep the records required by this Code for at least the period specified in sub-paragraph (3) or (4).

(2) To avoid doubt the obligation in sub-paragraph (1) continues to apply after a person ceases to be an operator.

(3) In the case of records required to be kept under paragraph 16(b), the records must be kept for a period of 5 years from the date of completion of the transaction.

(4) In the case of records to which sub-paragraph (3) does not apply, the records must be kept for a period of 5 years beginning on the date which—

(a) all activities in relation to an occasional transaction were completed; or

(b) in respect of other activities—

(i) the ongoing customer relationship was formally ended; or

(ii) if the ongoing customer relationship was not formally ended, when all activities relating to the relationship were completed.

(5) Without limiting sub-paragraph (1), if—

(a) an external disclosure has been made to the Financial Intelligence Unit under paragraphs 22(f) and paragraph 24 (external disclosures);

(b) the operator knows of or believes that a matter is under investigation by a competent authority; or

(c) the operator becomes aware that a request for information or an enquiry is underway by a competent authority,

the operator must maintain all relevant records for as long as required by the competent authority.

GSC Guidance and Policy

What? This paragraph of the Code details the length of time that the records described in Paragraph 16 (see 5.1 Record keeping (Paragraph 16)) must be kept for.

Why? It is essential that records are kept for a suitable period of time as this allows for records to be retrieved to assist with investigations (either ML/FT/PF or regulatory) after the activity has occurred.

The DPO should also consider any other relevant legislation and the companies own retention and destruction procedures.

When? Record keeping requirements apply from when an operator is licensed (in respect of procedures, BRA, etc.) and throughout all customer relationships. This includes records that relate to attempted transactions and customers that attempt to open an account but are refused.

Who? All staff members should be made aware of the requirement to record information The GSC expects all policies and procedures for record keeping to be approved by the operator's DPO to ensure compliance with GDPR as well as the Code.

How? The DPO should advise staff members on processes to follow (recording date of records, data weeding, destruction, deletion, etc.) when disposing of records.

Records relating to investigations and enquiries

The standard 5 year retention requirement does not apply where a disclosure has been made to the FIU or there is an investigation, enquiry or information request under way with a competent authority (e.g. the GSC or FIU). Instead, the records must be kept as long as required by the authority.

In such cases, the operator should contact the relevant authority and seek guidance on what records must be kept and for how long.

Former operators

The Code states that the record retention requirements continue to apply after a licence ceases.

It is the GSC's view therefore that the data must be preserved notwithstanding no licensee exists and there may be no remuneration for server upkeep, administration and so forth.

As persons with the greatest influence over the operations of the licensee, the GSC considers that it falls to the directors of the company to ensure that AML/CFT/CPF data is retained for the requisite timescales irrespective of the licensing status of the licensee.

The GSC recommends that licensees consider what steps will be taken for record retention in the event of de-licensing in the IOM and that the directors of the licensee take steps to store records and advise the FIU and GSC of the mechanism for their retrieval.

Please see 5.3 Format and retrieval of records (Paragraph 18) for guidance on utilising a third party to store records.

Key Messages

Record Retention - Key Messages

- ✓ It is essential that records are kept for a suitable period of time as this allows for records to be retrieved to assist with investigations (either ML/FT/PF or regulatory) after the activity has occurred.
- ✓ The standard 5 year retention requirement does not apply where a disclosure has been made to the FIU or there is an investigation, enquiry or information request under way with a competent authority.
- ✓ Record retention requirements continue to apply after a licence ceases.

5.3 Format and Retrieval of Records (Paragraph 18)

The FATF Requirement

FATF Recommendation 11 states that businesses should be able to comply swiftly with requests from competent authorities who require their data.

The Code 2019

18 Format and retrieval of records

(1) To avoid doubt the obligations of this paragraph continue to apply after a person ceases to be an operator. In the case of any records that are required to be established and maintained by this Code—

(a) if the records are in the form of hard copies kept on the Island, the operator must ensure that they are capable of retrieval without undue delay;

(b) if the records are in the form of hard copies kept outside the Island, the operator must ensure that the copies can be sent to the Island and made available within 7 days; and

(c) if the records are not in the form of hard copies (such as copies kept on a computer system), the operator must ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

(2) An operator may rely on the records of a third party in respect of the details of transactions, if satisfied that the third party will—

(a) produce copies of the records on request; and

(b) notify the operator if the third party is no longer able to produce copies of the records on request.

GSC Guidance and Policy

What? This paragraph sets out the requirement for how quickly an operator must be able to retrieve AML/CFT/CPF records (as described in 5.1 Record keeping (Paragraph 16)). It also includes requirements for records kept by third parties. It clarifies that all requirements continue to apply to former operators (in accordance with the timeframes detailed in 5.2. Record retention (Paragraph 17).

Why? It is important that operators are able to quickly access records for both their own processes (e.g. investigation of unusual activity) and to satisfy requests for information from a competent authority (e.g. the GSC or FIU). An operator's AML/CFT/CPF records could play a key part in a criminal investigation and, as a regulated sector, it is expected that operators swiftly comply with such requests.

When? Where records are held electronically or in hard copy on-Island, the records must be retrievable without "undue delay". For hard copies off-Island, the requirement is seven days.

Who? It should be noted that these requirements apply to all operators (current and former) including land-based operators that may have a large amount of paper records.

The GSC expects all policies and procedures for record keeping, including retrieval, to be approved by the operator's DPO to ensure compliance with GDPR as well as the Code. Consideration should also be given to how non-routine requests are dealt with; who is responsible for checking the legal basis of requests and how? How will this impact on the timeliness of the response?

Operators should take care to ensure that records are filed in such a way that they can be easily identified as this will help speed the retrieval process.

The GSC considers it reasonable for the time period to start either from the time request was sent to the operator or the time it was received by the operator if the request was sent outside of the operator's normal business hours.

- **Who can ask for our AML/CFT/CPF records?**

  The most common source of information requests will be the GSC. The GSC has provisions under the gambling acts and the Gambling (AML/CFT) Act for compelling the production of information. Typically, the GSC will request information as part of its routine ongoing supervision of the entity however there may be occasions where the GSC is cooperating with domestic and foreign competent authorities in accordance with its own information sharing powers. The GSC will not be offended if an operator asks us to explain why we are requesting information, for what purpose or under what legislation.

  Please see 5.5 Registers of money laundering and financing of terrorism enquiries (Paragraph 20) for how to handle enquiries from other agencies.

- **What does "without undue delay" mean?**

  Hard copy documents held off-Island must be retrievable within 7 days so it is reasonable to assume that hard copies held on-Island or electronic records should be retrievable in a shorter than 7 day period.

  The GSC expects operators to be able to respond within 3 days to requests that do not require extensive system searches or very large volumes of records.

- **What if I'm unable to meet the deadlines?**

  In some cases, authorities may request a significant amount of records making it difficult or possible to comply within the without undue delay/seven day timeframe. In such cases, the operators should advise the requester of any issues at the earliest possible opportunity. Consideration could also be given to supply any more urgent/essential items prior to the rest or agreeing with the requester that hard copy documents could be scanned and provided electronically.

- **How can former operators comply?**

  The requirement to retain records (see 5.2. Record retention (Paragraph 17)) and the requirement to be able to retrieve those records within the without undue delay/seven day timeframe also applies to former operators.

  When arrangements are made to store the records of a former operator this must also include consideration of who will be able to retrieve the documents and how.

  The GSC will ask for a named contact to be provided. The GSC does not assume responsibility for holding the records that belong to former operators.

  Where competent authorities have sought copies or originals on an intelligence or evidential basis, enquiries should be made with those agencies at the end of the retention period to establish their view on further retention.

- **What 3rd parties can hold transaction data and what controls must be in place?**

  The second part of this paragraph relates only to operators that have some transaction records held by a third party. All transaction data would usually be held by the operator rather than, or as well as, by a third party however there may be instances where a payment service provider holds some information that the operator does not.

  The Code requires that the operator be satisfied that the third party will be able to produce records on request (and this should be within the without undue delay/seven day timeframe) and that they will notify the operator should that change.

5.4 Registers of Disclosures (Paragraph 19)

The FATF Requirement

N/A – there is no specific FATF requirement for registers

The Code 2019

19 Registers of disclosures

(1) An operator must establish and maintain separate registers of—

(a) all internal disclosures;

(b) all external disclosures; and

(c) any other disclosures to the Financial Intelligence Unit.

(2) The registers must include details of—

(a) the date on which the disclosure is made;

(b) the person who made the disclosure;

(c) for internal disclosures, whether it is made to the MLRO or deputy MLRO;

(d) for external disclosures, the reference number supplied by the Financial Intelligence Unit; and

(e) information sufficient to identify any relevant papers or records.

(3) The registers of disclosures required by sub-paragraph (1) may be contained in a single document if the details required to be included in those registers can be presented separately for each type of disclosure on request by a competent authority.

GSC Guidance and Policy

What? This paragraph sets out the requirements to maintain registers of disclosures made to the MLRO (or Deputy) and disclosures made to the FIU.

Why? Keeping records of disclosures evidences compliance with the suspicious activity reporting requirements of the AML Code, POCA and ATCA. Registers will also provide the MLRO and AML/CFT Compliance Officer with useful information for trend analysis.

When? Registers should be kept up to date at all times. Entries should be added to the register as soon as a disclosure is made/received with further detail added as the matter progresses.

Who? The GSC expects access to registers to be restricted to small number of staff who require access due to their role in the reporting process. The MLRO should be responsible for ensuring that the register is properly maintained. Access should be restricted due to the sensitive nature of the information.

How? The requirement for three separate registers can be met by either using entirely separate documents, separate tabs or including ability to filter records depending of the type of disclosure.

The three categories that must be filter-able are:

- Internal disclosure - any type of internal disclosure made to the MLRO (or deputy);
- External disclosure - ML/FT/PF disclosures made to the FIU; and
- Any other disclosure made to the FIU - this means sanctions reporting or reports of any

intelligence under Section 24 of the FIU Act.

The minimum data to be recorded is listed as date report made, who by/to, any FIU reference and information (e.g. file path or internal reference) used to find the related records.

The GSC recommends that further information is included to assist with trend analysis -

- Action taken regarding any internal disclosures;
- Time elapsed between the internal disclosure being made and decision taken; and
- Brief reason for suspicion (Re. external disclosures) or rationale for report (other disclosures). Ideally, this would be from a standardised list in order to facilitate easy analysis.

Key Messages

Retrieval of Records and Registers of Disclosures - Key Messages

- ✓ Keeping records of disclosures evidences compliance with the suspicious activity reporting requirements of the AML Code, POCA and ATCA.
- ✓ Registers will also provide the MLRO and AML/CFT Compliance Officer with useful information for trend analysis.
- ✓ Registers should be kept up to date at all times
- ✓ The requirement for three separate registers can be met by either using entirely separate documents, separate tabs or including ability to filter records depending of the type of disclosure.

5.5 Registers of Money Laundering and Financing of Terrorism Enquiries (Paragraph 20)

The FATF Requirement

N/A – there is no specific FATF requirement for registers.

The Code 2019

20 Register of money laundering and financing of terrorism enquiries

(1) An operator must establish and maintain a register of all ML/FT enquiries received by it from competent authorities.

(2) The register must be kept separate from other records and include—

(a) the date of the enquiry;

(b) the nature of the enquiry;

(c) the name and agency of the enquiring officer;

(d) the powers being exercised; and

(e) details of the accounts or transactions involved.

GSC Guidance and Policy

What? This paragraph sets out the requirements to maintain registers of ML/FT/PF enquiries made to the operator. The GSC would not expect routine sports betting integrity enquiries to be treated as AML/CFT/CPF enquiries.

Why? Operators may hold valuable information and records that could assist authorities in their investigations. Keeping records of enquiries evidences that the operator cooperates with competent authorities. By properly recording the source of the enquiry and the legal powers being exercised it also demonstrates that the operator considered whether the requester has the proper authority to request and that they are able to respond without breaching any data protection or confidentiality rules. Further, this log will provide the MLRO with useful information for trend/risk analysis and could prompt further scrutiny of the customer/activity in question.

When? Registers should be kept up to date at all times. Entries should be added to the register as soon as a request is received with further detail added as the matter progresses.

Who? Competent authorities (the requester) is a defined term in the Code and means Island's authorities concerned with AML/CFT/CPF including the GSC, IOMFSA, DHA, Constabulary, FIU, Attorney General's Chambers (AGC), Customs and Excise and Income Tax.

The requirement to maintain the register applies to the operator however, the GSC would expect the MLRO to "own" the register with access provided to the AML/CFT Compliance Officer.

Access should be restricted due to the sensitive nature of the information.

How?

- **Timeframes for responding**

  It is important that operators respond to requests in a timely manner as the enquiry could be time-critical. There may also be a legal requirement to respond within a certain timeframe.

  If further information is required from the requester such as the legal basis for their enquiry then this should be sought as soon as possible. Equally if the response will take some time to complete the requester should be advised at the earliest opportunity.

❖ **Checking the requester's credentials and legal basis for enquiry**

Authorities, particularly those that are not IOM authorities may lack the necessary authority to request data or the operator may lack the disclosure provisions to enable them to respond despite their willingness to cooperate.

It is reasonable for an operator to seek clarification from the requester on their role and the legislation under which the information is sought. If operators are uncertain they could seek legal advice but this could cause delay. Alternatively, they could ask that the requester submit their request via the Island's central intelligence hub, the FIU.

If the operator does not hold the requested information, it would be helpful to advise the requester of this rather than waste time and effort seeking the information through the proper channels only to later find that the information does not exist.

Tipping off

An operator must not disclose to the subject of the request (i.e. the customer) that an enquiry has been made. The only exception to this would be where the requestor has provided explicit consent to the operator to do so.

Further to tipping off provisions there may be additional restrictions on sharing the data. The request should be read very carefully before being discussed with any colleagues or group entities.

❖ **Should an enquiry prompt a suspicious activity report?**

An ML/FT/PF enquiry made to an operator should prompt a review of the customer or activity in question to determine whether there may be any unusual or suspicious activity or whether the risk assessment or customer due diligence should be refreshed.

Reports should not be made to the FIU because of an ML/FT/PF enquiry on an automatic or 'covering' basis. Disclosures to the FIU must be considered on the merits of the operator's review of the customer or activity.

Key Messages

Registers of ML/FT Enquiries - Key Messages

- ✓ Operators may hold valuable information and records that could assist authorities in their investigations. Keeping records of enquiries evidences that the operator cooperates with competent authorities.
- ✓ Registers should be kept up to date at all times.
- ✓ Competent authorities (the requester) is a defined term in the Code and means Island's authorities concerned with AML/CFT/CPF including the GSC, FSA, DHA, Constabulary, FIU, AGC, Customs and Excise and Income Tax.
- ✓ It is important that operators respond to requests in a timely manner as the enquiry could be time-critical.
- ✓ It is reasonable for an operator to seek clarification from the requester on their role and the legislation under which the information is sought.
- ✓ An operator must not disclose to the subject of the request (i.e. the customer) that an enquiry has been made.
- ✓ An ML/FT/PF enquiry made to an operator should prompt a review of the customer or activity in question to determine whether there may be any unusual or suspicious activity or whether the risk assessment or CDD should be refreshed.

5.6 Money Laundering Reporting Officer (Paragraph 21)

The FATF Requirement

N/A – there is no specific FATF requirement to appoint an MLRO.

The Code 2019

21 Money Laundering Reporting Officer

(1) An operator must appoint a Money Laundering Reporting Officer ("**MLRO**") to exercise the functions conferred by paragraphs 22 (reporting procedures) and 24 (external disclosures).

(2) An MLRO must—

(a) be sufficiently senior in the organisation of the operator or have sufficient expertise and authority;

(b) have a right of direct access to the officers of the operator; and

(c) have sufficient time and resources to properly discharge the responsibilities of the position.

(3) An operator may appoint a Deputy Money Laundering Reporting Officer ("Deputy MLRO") in order to exercise the functions specified in paragraphs 22 (reporting procedures) and 24 (external disclosures) in the MLRO's absence.

GSC Guidance and Policy

What? This paragraph sets out the requirement for all operators to appoint an MLRO and their duties and responsibilities. This Code role of MLRO has the same meaning as "nominated officer" in POCA and ATCA.

It should be noted that the role of MLRO is separate to the role of AML/CFT Compliance Officer however in some cases both roles may be performed by the same individual.

The MLRO is responsible for the SAR reporting process and handling of SARs whereas the AML/CFT Compliance Officer is responsible for ensuring that all Code requirements are complied with, tested and reported on to senior management.

The Code allows a Deputy to be appointed and the GSC encourages all operators to do so to ensure that there is adequate cover to promptly deal with SARs when the MLRO is unavailable.

Why? A SAR reporting framework is one of the key components of AML/CFT/CPF. The role can be a complex one requiring sound technical understanding of the Code reporting requirements and of key parts of POCA and ATCA, including the different types of disclosures and "consent".

It is essential that the person performing the reporting role is a competent, professional and ethical person (a person that would not view business profits as more important than proper handling of suspicious activity).

When? All operators must have an MLRO appointed even if not currently trading.

Who? A change of MLRO must be notified to the GSC as entry controls apply. An MLRO does not need to hold a professional AML/CFT qualification but does need to meet the requirements described below.

How?

❖ **MLRO role holder**

The Code provides three requirements for MLRO role holders –

1 - Seniority, expertise and authority

The Code states that the MLRO must have sufficient seniority and authority. The GSC expects an MLRO to be a managerial post that carries influence but a director need not hold it.

The GSC will expect an MLRO to be able to demonstrate expertise and competency and be able to describe in detail -

- Applicable suspicious activity reporting requirements;
- Gambling typologies and risk factors;
- The business model and customer base;
- All aspects of AML/CFT/CPF processes in the organisation;
- Broad patterns or trends, including:
  - the approximate ratio of high risk to low risk players;
  - the approximate volume of internal and external disclosures;
  - the conversion rate of internal SARs to external SARs;
  - the reasons for any apparent under- or over-reporting by staff;
  - the risk factors that are proving useful in the risk-rating process.

It is strongly recommended by the GSC that MLROs be in possession of clear job descriptions and that those job descriptions mandate all of the reporting requirements specified in this guidance.

2 - Direct access to officers of the operator

The MLRO must be able to liaise directly with the board and senior management of the operator. It is imperative that the advice of the MLRO is taken on board regarding the handling of suspected proceeds of crime.

The GSC would also expect the MLRO to provide regular reports to the board regarding AML/CFT/CPF trends and typologies so that the business can feed this into its risk-based policies, procedures and staff training.

3 - Sufficient time and resource

The MLRO must have sufficient time and resource to properly discharge their responsibilities (see 5.7 Reporting procedures, Internal disclosures and External disclosures (Paragraph 22, 23, 24)) for details of the MLRO's responsibilities).

"Resource" includes access to the appropriate systems and records (including the Themis FIU reporting system) and to staff to assist with systems and product expertise as may be required.

An MLRO should be able to demonstrate that they have sufficient time and resource through-

- Staying abreast of AML/CFT/CPF trends and typologies;

- No backlogs or delays in handling suspicious activity reports or enquiries;
- Making good quality and timely external disclosures;
- Regular reports on SARs (trends, volumes) to the board; and
- Participation in AML/CFT/CPF consultations and events such as the AML Forum.

Group/Head Office MLROs

- *Some operators may have group/head office MLROs that carry out the role across a number of jurisdictions;*
- *This approach is permissible however the MLRO must be able to demonstrate understanding of IOM requirements and that they have sufficient time and resource to carry out the role effectively.*

❖ **Deputy MLRO**

The Code states that the operator may appoint a deputy but it does not require one to be appointed. Except for very small or new operators, the GSC would expect a deputy to be appointed and advised to the GSC so that any entry controls may be satisfied.

Operators should put in place measures to deal with short or longer-term absence of the MLRO and deputy (where appointed) so that the suspicious activity reporting function may continue uninterrupted.

❖ **Conflicts of interest**

The MLRO should be independent from the enterprise functions of the company (i.e. those roles and departments charged with generating money, managing player accounts (particularly VIP accounts), managing finance, marketing to players and so forth). When suspicion needs to be investigated, it is vital that the MLRO does not have a conflict of interests.

For this reason, care should be taken to ensure that (wherever possible) the MLRO does not hold a joint role that has a responsibility to AML/CFT/CPF and an enterprise function. If the MLRO reports to a senior figure (such as a director) then it should not be to a person with responsibility to profit rather than compliance.

It is understood that this may not be possible for smaller operations however best efforts should be made.

❖ **Large AML/CFT/CPF teams with multiple Themis reporters**

For larger operators the MLRO may be supported by a team of staff members each with the ability to submit disclosures to the FIU using the Themis reporting system. As the Code requires the MLRO or DMLRO to assess internal disclosures and make external disclosures, the work of the reporting team must be closely supervised by the MLRO or their Deputy and they remain responsible for the reporting function.

Note: all Themis users will be able to see details of all external disclosures so this will need to be carefully managed, particularly where there may be sensitivities such as a Themis user being connected to the subject of a report.

Key Messages

Money Laundering Reporting Officer - Key Messages

- ✓ The role of MLRO is separate to the role of AML/CFT Compliance Officer however in some cases both roles may be performed by the same individual.
- ✓ The Code allows a Deputy to be appointed and the GSC encourages all operators to do so.
- ✓ The three Code requirements for MLRO role holders are:
  - Seniority, expertise and authority;
  - Direct access to officers of the operator;
  - Sufficient time and resource.
- ✓ The MLRO should be independent from the enterprise functions of the company.

5.7 Reporting Procedures, Internal Disclosures and External Disclosures (Paragraph 22, 23, 24)

The FATF Requirement

FATF Recommendation 20 states that businesses should be required to promptly report suspicions to the FIU.

The 2019 Code

22 Reporting procedures

An operator must establish, record, maintain and operate reporting procedures and controls that—

(a) enable its officers, all other persons involved in its management, and all appropriate employees and workers to know to whom they should report any suspicious activity;

(b) ensure that there is a clear reporting chain to the MLRO;

(c) require an internal disclosure to be made to the MLRO if any information or other matters that come to the attention of the person handling that business are, in that person's opinion, suspicious activity;

(d) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the operator;

(e) require the MLRO to consider internal disclosures in the light of all other relevant information available to the MLRO for the purpose of determining whether the activity is, in the MLRO's opinion, suspicious activity;

(f) enable the information to be provided as soon as is practicable to the Financial Intelligence Unit if the MLRO knows or suspects, or has reasonable grounds to suspect, that the activity is ML/FT; and

(g) ensure the registers as required by paragraphs 19 (registers of disclosures) and 20 (register of money laundering and financing of terrorism enquiries) are maintained and completed in accordance with those paragraphs.

23 Internal disclosures

Where an operator identifies any suspicious activity in the course of an ongoing customer relationship or in relation to an occasional transaction, the operator must—

(a) conduct enhanced customer due diligence in accordance with paragraph 14 (enhanced customer due diligence) unless the operator reasonably believes conducting enhanced customer due diligence will tip-off the customer; and

(b) make an internal disclosure.

24 External disclosures

(1) Where an internal disclosure has been made, the MLRO must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/FT.

(2) The MLRO must make an external disclosure in accordance with the reporting procedures and controls established under paragraph 24 (external disclosures) as soon as practicable to the Financial Intelligence Unit if the MLRO—

(a) knows or suspects; or

(b) has reasonable grounds for knowing or suspecting,

that the activity is related to ML/FT.

(3) If the MLRO is of the view that there are not reasonable grounds for knowing or suspecting that the activity is related to ML/FT, but the MLRO believes that it would assist the Financial Intelligence Unit in the exercise of any of its functions, the MLRO may make a disclosure to the Financial Intelligence Unit under section 24 of the Financial Intelligence Unit Act 2016.

(4) A disclosure under subparagraph (3) does not breach—

(a) any obligation of confidence owed by the MLRO; or

(b) any other restriction on the disclosure of information (however imposed).

GSC Guidance and Policy

What? These paragraphs of the Code set out the requirements for procedures and controls for the reporting of suspicions both internally (to the MLRO) and externally (to the FIU). It also provides protections from data confidentiality where the reports are made in accordance with the Code.

Procedures and controls - must be established by all operators ready for go-live;

Training and awareness - must be done for all new staff, at least annually and in the event of any changes to procedures and controls; and

Report suspicions - as soon as practicable.

Who? Procedures and controls should be established and approved by both the MLRO and the AML/CFT Compliance Officer.

The requirement for training and awareness applies to all officers and appropriate employees and workers (this includes contractors and those employed via service companies). Very few staff (e.g. those with very limited IT development roles) would not be considered as appropriate for AML/CFT/CPF training.

Non-AML/CFT reports to the MLRO

Some operators may establish procedures that require reports other than ML/FT/PF suspicions to be sent to the MLRO such as-

- *T&C breaches*
- *Bonus abuse*
- *Professional gambling*

This is acceptable provided that they are not incorrectly counted in statistics or create backlogs or delays in dealing with ML/FT/PF reports.

How?

- **Procedures**

  The Code provides clear detail on what must be included in reporting procedures -

  - Advise all staff how to report suspicions. This should be done for new starters and as part of their periodic training (see 6.3 Staff training (Paragraph 27));
  - Establish a clear reporting chain to MLRO (see below);
  - Require staff to report suspicions to MLRO (see below);

- Provide the MLRO with access and systems needed to investigate;
- Require MLRO to consider and report if suspicious or reasonable grounds to suspect (see below);
- Enable to reports to be made as soon as practicable (see below);
- Ensure the registers are updated (see 5.4 Registers of disclosures (Paragraph 19))

❖ **Clear reporting chain**

Reporting lines should be as short as possible with the minimum number of people between the person with suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

All disclosure reports must reach the MLRO without any undue delay. Under no circumstances should reports of suspected ML/FT/PF be filtered out by supervisors or managers such that they do not reach the MLRO.

Staff members should be made to feel comfortable in raising suspicions without fear of criticism or judgement from their superiors.

❖ **EDD & internal disclosures**

The Code requires that, where there is a ML/FT/PF suspicion, EDD be conducted. The reason for this is that the extra information (SOW, verification of identity, asking for rationale regarding a certain transaction, etc.) may support the suspicion or remove it and provide useful information for the authorities.

The conducting of EDD should not cause a delay to making the report to the MLRO. If there is grounds for suspicion without the EDD being completed, a disclosure should be made and then later updated when the EDD is completed.

If the staff member reasonably believes that conducting EDD would tip off the customer then this requirement may be waived. This should be noted and included in the report made to the MLRO who can provide guidance on how best to proceed.

All suspicions reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the details of the customer, relevant transactions and explanation of the reason for suspicion.

❖ **MLRO investigations & reporting "as soon as practicable"**

The Code does not specify an absolute time limit before a disclosure is made. The timing of a disclosure is a subjective decision made by the MLRO or other person making the report (see 5.6 Money Laundering Reporting Officer (Paragraph 21) for guidance on multiple Themis users).

Where a matter is complex, significant amounts of work may be required before a full report can be submitted. Where offending appears serious, TF or organised crime related, an initial disclosure outlining the concerns and subjects should be made with notes to explain that work is ongoing to further enhance the report. Inclusion of an estimated timescale for completing the work would be helpful.

The GSC offers the following guidance on what it considers to be, or to not be, 'as soon as practicable' -

As soon as practicable:

- Further information is being gathered to assist the FIU to identify a person or the whereabouts of the criminal property;
- The circumstances of suspicion are being investigated to determine whether they constitute grounds for a disclosure;
- The operator has received specific directions from the FIU which must be processed before the disclosure is submitted;
- Holidays and non-work days prevent the disclosure from being made;
- Ongoing discussions with the FIU are determining the format of the disclosure;
- Ongoing discussions with the FIU are determining whether a disclosure is justified;
- The organisation is experiencing a disaster and systems are temporarily unavailable to the MLRO and deputies;
- The MLRO and deputies are unavailable under extraordinary and unexpected circumstances;
- A large number of cases where suspicious transactions may need to be processed has unexpectedly occurred and the operator's systems are gearing up to handle them (the GSC would expect a dialogue between the operator and the FIU in this instance);
- Legal advice is being sought on the correct procedure for complying with the AML/CFT/CPF requirements;
- The FIU are unavailable to receive the disclosure.

NOT as soon as practicable:

- MLRO unavailable and no deputy appointed;
- No MLRO or deputy available (for example, both persons on annual leave);
- Confusion exists over the reporting requirements;
- An investigation into whether a report should be made has stalled;
- Workload is preventing reports from being made quickly enough and the operator is chronically understaffed;
- All reports must be done manually and there is insufficient resource;
- Internal sign-off by management is blocking reporting (note that operators should ensure that MLROs are able to report directly to the FIU without interference from management);
- The MLRO has multiple duties and other work is preventing access to the MLRO workload;
- Preferred channel (say internet or electronic submission) not available and preference to not report manually until preferred channel becomes available again.

Dual Reporting

Where activity relates to activity or customers outside of the Island, there may also be a requirement to report to their local FIU. This is known as dual reporting.

The designated reporting platform for reporting to the FIU is 'Themis'. The platform can be accessed at the following link: https://disclosures.gov.im.

All operators must have at least one staff member (the MLRO) registered on Themis in the name of the operator at all times. This is to avoid delay in reporting due to the need to set up an account. Further, Themis is used by the FIU as a messaging system and repository for guidance and other useful information.

THEMIS is the single point of contact for Operators in relation to:-

- Reporting under the Proceeds of Crime or Terrorism Legislation;
- Reporting under Section 24 of the FIU Act;
- Reporting Sanction Breaches.

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

❖ **What to do (or not to do!) after making a disclosure**

The MLRO should acknowledge receipt of an internal disclosure and, at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries i.e. tipping off the customer or any other third party.

Where funds are suspected to be the proceeds of crime (i.e. an authorised disclosure should be made) the operator commits a criminal offence if funds are converted, transferred, etc. without the necessary approvals (known as "consent") from the FIU (or an ATCA offence where funds are suspected to be intended for terrorist use).

Please see the Legislation section of this document for further details on POCA and ATCA.

❖ **Knowledge, suspicion, reasonable grounds**

The threshold that must be made in order to make an external disclosure re ML/FT/PF is that there must be "knowledge", "suspicion" or "reasonable grounds" to suspect ML/FT/PF.

First, the MLRO must be aware of what the ML/FT/PF offences are under Manx law. There is no requirement to identify the underlying proceeds generating offence(s) that may have occurred. Please see "POCA & ATCA" for further detail regarding the ML/FT offences.

Then the MLRO must determine, whether there is -

- **"Knowledge"**

  Knowledge of money laundering means that actual knowledge of money laundering is possessed.

- **"Suspicion"**

  Suspicion is a subjective test that a person applies. It is defined in case law as something more than a fanciful possibility and where facts exist – it is more than just a vague feeling of unease. The law does not require the suspicion to be 'clear', 'firmly grounded on targeted or specific facts' or 'based on reasonable grounds.' However, it is important that concerns be justified by the

existence of facts even if those facts do not prove that ML/FT/PF is occurring. Typically, suspicion will arise when something unusual is noticed and when a subsequent investigation continues to produce unusual or contradictory facts.

MLROs should carefully document their evidence when considering whether to make a disclosure. In this way, if such a disclosure is not made, it is easy for the MLRO to evidence the logic behind the decision.

- **"Reasonable grounds to know or suspect"**

  Reasonable grounds for knowledge or suspicion of ML are facts, which, if presented to a reasonable person, would suggest that ML could be occurring.

  Therefore, an MLRO should ask themselves both "am I suspicious" and "would a reasonable person be suspicious".

Where this threshold test is not met but the MLRO still feels that they may have some intelligence that could be of use to the FIU, the MLRO can still make a report under section 24 of the FIU Act, which is also protected from data confidentiality rules. The Themis reporting system presents the MLRO with the option to select whether the report is under POCA, ATCA, the FIU Act or sanctions.

Key Messages

Reporting Procedures, Internal and External Disclosures - Key Messages

- ✓ Procedures and controls should be established and approved by both the MLRO and the AML/CFT Compliance Officer.
- ✓ Reporting procedures must include:
  - Procedures;
  - Clear reporting chain;
  - EDD & internal disclosures;
  - MLRO investigations & reporting "as soon as practicable".
- ✓ The MLRO must be aware of what the ML/FT/PF offences are under Manx law.
- ✓ The threshold that must be made in order to make an external disclosure re ML/FT/PF is that there must be "knowledge", "suspicion" or "reasonable grounds" to suspect ML/FT/PF.

5.8 ML/TF/PF/S.24 Matters to Report to FIU

Activity Type	Reportable to the FIU?	
Money laundering	✓	Yes - must report to FIU under POCA
Terrorist financing	✓	Yes - must report to FIU under ATCA
Breaches of EU/UN/UK financial sanctions	✓	Yes - must report to FIU under Sanction breach-not OFAC
Proliferation of WMD	✓	Yes - must report to FIU under TOCFRA
Breaches of other types of financial sanction e.g. OFAC	✗	No requirement to report under TOCFRA but can report under S.24 FIU Act
Fraud or other financial crime	✗	No - Economic Crime Unit (local victims or suspected criminals) or UK's Action Fraud
Non-financial crimes e.g. property theft, drugs	✗	No - please report to local police
Something that is not ML/FT/PF suspicious but might assist the FIU with - ❖ Info about financial crime ❖ Prevention and detection of crime ❖ Cooperation with law enforcement ❖ Reducing crime	✓	Non mandatory reports made under S.24 FIU Act

It is important to remember that there is no de-minimis or threshold for reporting. ML/FT/PF/sanction of any value must be reported.

Part 6: Staffing, Training and Monitoring Compliance

6.1 Monitoring and Testing Compliance (Paragraph 25)

The FATF Requirement

FATF Recommendation 18 requires businesses to implement AML/CFT programmes. The Interpretative notes state that this should include an independent audit function to test the system and the appointment of a compliance officer at a managerial level.

The Code 2019

25 Monitoring and testing compliance

(1) An operator must establish, record, maintain and operate appropriate procedures and controls for monitoring and testing compliance with the AML/CFT legislation, so as to ensure that—

(a) the operator has robust and documented arrangements for managing the risks identified by the business risk assessment conducted in accordance with paragraph 6 (business risk assessment);

(b) the operational performance of those arrangements is suitably monitored; and

(c) prompt action is taken to remedy any deficiencies in arrangements.

(2) A report to the senior management of the operator must be submitted, at least annually, describing—

(a) the operator's AML/CFT environment including any developments in relation to AML/CFT legislation;

(b) progress on internal developments in relation to the operator's policies, procedures and controls for AML/CFT;

(c) any activities relating to compliance with this Code that have been undertaken by the operator during the period covered by the report; and

(d) the results of any testing undertaken in sub-paragraph (1).

(3) An operator must ensure there is a suitable person (the **"AML/CFT Compliance Officer**") to exercise the functions specified in this paragraph.

(4) To be effective in the exercise of their functions the suitable person (the **"AML/CFT Compliance Officer")** must—

(a) be sufficiently senior in the organisation of the operator or have sufficient experience or authority;

(b) have a right of direct access to the officers of the operator; and

(c) have sufficient time and resources to properly discharge the responsibilities of the position.

GSC Guidance and Policy

What? This paragraph requires operators to appoint a suitable person to be the AML/CFT Compliance Officer and lists their responsibilities; implementation of risk-based AML/CFT/CPF procedures in line with AML/CFT Code, monitor performance, address issues and report to the board of the operator.

Why? The role of the AML/CFT Compliance Officer is different to the role of the MLRO. The MLRO is responsible for suspicious activity reporting whereas the AML/CFT Compliance Officer is responsible for all AML/CFT/CPF procedures and controls.

When? All operators must have an AML/CFT Compliance Officer appointed even if not currently trading.

Who? Changes to the AML/CFT Compliance Officer must be notified to the GSC as entry controls apply. An AML/CFT Compliance Officer does not need to hold a professional AML/CFT/CPF qualification but does need to meet the requirements described below.

How? Appointment of the AML/CFT Officer; like the MLRO role, the Code mandates three requirements for the AML/CFT Compliance Officer -

- **Appointment of the AML/CFT Officer**

1 - Seniority, expertise and authority

The Code states that the AML/CFT Compliance Officer must have sufficient seniority and authority. The GSC expects an AML/CFT Compliance Officer to be a managerial post that carries influence but a director need not hold it.

The GSC will expect an AML/CFT Compliance Officer to be able to demonstrate expertise and competency and be able to describe in detail -

- Applicable AML/CFT/CPF requirements;
- Gambling typologies and risk factors;
- The business model and customer base;
- The findings of the BRA;
- The operator's AML/CFT/CPF policies, procedures and systems;
- The programmes to test those policies, procedures and systems;
- Any shortcomings, including GSC report findings, of those policies procedures and systems;
- Plans to remediate any shortcomings.

2 - Direct access to officers of the operator

The AML/CFT Compliance Officer must be able to liaise directly with the board and senior management of the operator. It is imperative that the advice of the AML/CFT Compliance Officer is taken on board regarding AML/CFT/CPF policies, procedures and systems.

The GSC would also expect the MLRO to provide regular reports to the board regarding AML/CFT/CPF trends and typologies so that the business can feed this into its risk-based policies, procedures and staff training.

3 - Sufficient time and resource

The AML/CFT Compliance Officer must have sufficient time and resource to properly discharge their responsibilities for implementing and testing AML/CFT/CPF procedures and controls and reporting to the board.

"Resource" includes access to the appropriate systems and records and to staff in order to assess how well procedures and controls are working.

An AML/CFT Compliance Officer should be able to demonstrate that they have sufficient time and resource through

- Staying abreast of AML/CFT/CPF trends and typologies;
- Demonstrating up-to-date and detailed understanding of AML/CFT/CPF requirements and the operator's own procedures and controls, including any short comings and plans for remediation;
- Regular (at least annually) AML/CFT reports to the board;
- Participation in AML/CFT/CPF consultations and events such as the AML Forum.

Unlike with the MLRO role, the Code does not refer to a Deputy role holder.

The GSC does not expect or require a Deputy to be formally appointed but does expect the operator to arrange cover in the event of the AML/CFT Compliance Officer being out of office. This includes having someone in the organisation able to deal with regulatory queries, compliance visits, remediation plans, etc.

❖ **Conflicts of interest**

The AML/CFT Compliance Officer should be independent from the enterprise functions of the company (i.e. those roles and departments charged with generating money, managing player accounts (particularly VIP accounts), managing finance, marketing to players and so forth). When decisions need to be made around risk appetite and AML/CFT/CPF procedures and controls, it is vital that the AML/CFT Compliance Officer does not have a conflict of interest.

For this reason, care should be taken to ensure that (wherever possible) the AML/CFT Compliance Officer does not hold a joint role that has a responsibility to AML/CFT/CPF and an enterprise function. If the AML/CFT Compliance Officer reports to a senior figure (such as a director) then it should not be to a person with responsibility to profit rather than compliance.

It is understood that this may not be possible for smaller operators however best efforts should be made.

❖ **AML/CFT/CPF procedures and testing**

The AML/CFT Compliance Officer is responsible for ensuring that the operator has procedures and controls to monitor the AML/CFT/CPF function; to test that the AML/CFT/CPF procedures and controls are compliant with the law and are effective.

Please see 2.1 Procedures and controls (Paragraph 4) for detail on how to establish, record, maintain and operate procedures and controls in line with the operator's risk appetite.

The testing of AML/CFT/CPF procedures and controls must be suitably monitored and comprises two components - technical compliance and effectiveness.

Technical Compliance

This element of testing checks that procedures, policy and training are in line with current AML/CFT/CPF requirements (i.e. the Code, POCA, ATCA) and the operator's BRA.

The GSC expects this to be done at least annually and soon after any changes to the AML/CFT/CPF requirements.

Effectiveness

This element of testing checks how closely the procedures, policy and training are followed and how well they work in practice. It should include

- Spot checks to ensure that staff members know where to find procedures and other reference materials and that they understand their contents; and
- Sample checking of AML/CFT/CPF work including CRAs, due diligence, SOW and ongoing monitoring.

The GSC expects operators to put in place a programme of checks, which could include testing of different aspects throughout the year rather than doing all in one big check at least annually. For example, a drive on risk assessment one month followed by source of wealth the next.

❖ **AML/CFT reporting to the board**

The Code requires the AML/CFT Compliance Officer to report to the board at least annually. Again, rather than one big annual report, they may report on difference aspects on a more frequent basis. It could be that Operators have AML/CFT as a standing agenda item at all board meetings which includes reports from the MLRO and/or AML/CFT Compliance Officer.

❖ **Group/Head Office AML/CFT Compliance Officers**

As the role holder has a large responsibility and requires in-depth understanding of all of the Island's AML/CFT/CPF requirements, the GSC would discourage the same individual holding this role across multiple jurisdictions.

Independent Audit Function

Operators should consider commissioning periodic audit reports by an independent third party expert.

Such reports can be helpful to provide an unbiased view and "fresh pair of eyes". They can be particularly helpful where it is not possible for the AML/CFT Compliance Officer to be completely conflict free or where extra attention is required to fully understand and remediate shortcomings.

Key Messages

Monitoring and Testing Compliance - Key Messages

- ✓ AML/CFT Compliance Officer is responsible for all AML/CFT procedures and controls.
- ✓ All operators must have an AML/CFT Compliance Officer appointed even if not currently trading.
- ✓ Changes to the AML/CFT Compliance Officer must be notified to the GSC as entry controls apply.
- ✓ An AML/CFT Compliance Officer does not need to hold a professional AML/CFT qualification but does need:
  - To be sufficiently senior in the organisation of the operator or have sufficient experience or authority;
  - Direct access to officers of the operator;
  - Sufficient time and resource to properly discharge their responsibilities.
- ✓ The AML/CFT Compliance Officer should be independent from the enterprise functions of the company.
- ✓ The AML/CFT Compliance Officer is responsible for ensuring that the operator has procedures and controls to monitor the AML/CFT/CPF function; to test that the AML/CFT/CPF procedures and controls are compliant with the law and are effective.
- ✓ The Code requires the AML/CFT Compliance Officer to report to the board at least annually.

6.2 New Staff Appointments (Paragraph 26)

The FATF Requirement

The Interpretive note to Recommendation 18 states that AML/CFT policies procedures and controls should include screening procedures to ensure high standards when hiring employees.

The Code 2019

26 New staff appointments

An operator must establish, record, maintain and operate procedures and controls to enable the operator to satisfy itself of the integrity of new officers and of all new appropriate employees and workers

GSC Guidance and Policy

What? The paragraph requires operators to conduct integrity checks on new officers, appropriate employees and workers.

Why? Effective staff vetting controls help to protect an operator from the financial and reputational harms that could result from staff misconduct. Misconduct could range from not following AML/CFT/CPF procedures (whether due to collusion with criminal elements or disregard for the rules) to financial theft or theft of company or customer data.

When? Ideally, all parts of the vetting checks should be completed prior to the staff member commencing work. In some cases, such as delays in obtaining criminal background checks, this may not be possible. In such cases the GSC recommends that the staff member be provided a conditional appointment, restrictions put on their access levels and supervised closely until the checks are finalised.

Who? The requirement for vetting applies to all officers and appropriate employees and workers (this includes contractors and those employed via service companies). The GSC considers appropriate employees and workers to be those who have access to customers, customer information, company records, systems, hardware and software. Very few staff (e.g. those with very limited IT development roles) would not be considered as appropriate for vetting.

The GSC makes no distinction between different types of director (non-executive directors for example) and expects due diligence to be performed and documented for anybody to whom is assigned a directorship.

How? As with all AML/CFT/CPF procedures, those for integrity controls must have regard to the size and risks of the operator. The extent of checks carried out should vary based on the role of the person, their level of influence and access and not focus merely on senior management roles.

In order to meet these requirements operators must, where possible-

- Obtain and confirm references;
- Confirm employment history and the qualifications advised;
- Request details of any regulatory action taken against the individual (or the absence of such action); and
- Request details of any criminal convictions (or the absence of such convictions) and verify where possible.

Operators must document the steps taken to satisfy these requirements including the information and confirmations obtained. Operators must also document where it has not been possible to obtain such information including the reasons why this is the case.

Operators may wish to make ongoing character checks a part of employment contracts.

Key Messages

New Staff Appointments - Key Messages

- ✓ Effective staff vetting controls help to protect an operator from the financial and reputational harms that could result from staff misconduct.
- ✓ Ideally, all parts of the vetting checks should be completed prior to the staff member commencing work.
- ✓ The requirement for vetting applies to all officers and appropriate employees and workers (this includes contractors and those employed via service companies).
- ✓ Integrity controls must have regard to the size and risks of the operator.
- ✓ Operators must document the steps taken to satisfy these requirements including the information and confirmations obtained.
- ✓ Operators must also document where it has not been possible to obtain such information including the reasons why this is the case.

6.3 Staff training (Paragraph 27)

The FATF Requirement

The Interpretive note to Recommendation 18 states that AML/CFT policies, procedures and controls should include an ongoing employee-training programme.

The Code 2019

27 Staff training

(1) An operator must provide or arrange education and training, including refresher training, at least annually, for—

(a) all officers;

(b) any other persons involved in its senior management; and

(c) appropriate employees and workers.

(2) The training referred to in sub-paragraph (1) must make those persons aware of—

(a) the provisions of the AML/CFT legislation;

(b) any personal obligations in relation to the AML/CFT legislation;

(c) the reporting procedures and controls established under paragraph 22 (reporting procedures);

(d) the operator's policies and procedures and controls for AML/CFT as required by paragraph 4 (procedures and controls);

(e) the recognition and handling of unusual activity and suspicious activity;

(f) their personal liability for failure to report information or suspicions in accordance with internal procedures and controls, including the offence of tipping off; and

(g) new developments, including information on current techniques, methods and trends in ML/FT.

(3) Where there have been significant changes to AML/CFT legislation or the operator's policies and procedures, the operator must provide appropriate education and training to those persons included in sub-paragraph (1) within a reasonable timeframe.

(4) The operator must maintain records which demonstrate compliance with sub-paragraph (1).

GSC Guidance and Policy

What? This paragraph details when AML/CFT training must be delivered and, importantly, what exactly must be included in the training.

Why? AML/CFT training is a legal requirement and essential for managing financial crime risk. Employees particularly those that are customer facing or deal with financial transactions are at the forefront of identifying unusual or suspicious activity.

If an AML/CFT/CPF breach occurs and the staff member involved can demonstrate there has been a lack of training then the GSC will view the failure as an organisational one and will investigate the root cause.

For this reason, special care should be taken to ensure that staff training could be evidenced.

When? There are three times when training should be delivered; for new starters, refresher training (at least annually) and in the event of changes to the AML/CFT/CPF requirements or the operators own AML/CFT/CPF processes and procedures.

Who? The requirement for training and awareness applies to all officers and appropriate employees and workers (this includes contractors and those employed via service companies). The GSC considers appropriate employees and workers to be those who have access to customers, customer information, company records, systems, hardware and software. Very few staff (e.g. those with very limited IT development roles) would not be considered as appropriate for AML/CFT/CPF training.

The GSC makes no distinction between different types of director (non-executive directors for example) and training for anybody to whom is assigned a directorship.

The GSC would expect the AML/CFT Compliance Officer to be involved in creating, delivering or supervising AML/CFT/CPF training to ensure that it meets the Code requirements, is in line with the business' risks and is effective. The MLRO should contribute in the area of suspicious activity reporting.

How? Whilst the Code is clear on what has to be included in the training and when it must be delivered, it does not stipulate how the training is delivered.

The GSC sees merit, particularly for smaller businesses, to contract third party AML/CFT/CPF experts to deliver aspects of the training. A third party, however, will not usually be suitable to provide training on the operator's own processes and procedures.

General AML/CFT/CPF (could be delivered by a third party)	**Operator Specific AML/CFT/CPF** (should be in-house)
• AML/CFT/CPF legislation • Personal obligations in law • POCA/ATCA/FIU reporting • Personal liability in law • General trends and typologies	• Operator's AML/CFT/CPF procedures and controls • Operator's reporting procedure • Personal liability in staff contract • Trends and typologies identified by MLRO or AML/CFT Compliance Officer

Key Messages

Staff Training - Key Messages

- ✓ AML/CFT/CPF training is a legal requirement and essential for managing financial crime risk.
- ✓ There are three times when training should be delivered; for new starters, refresher training (at least annually) and in the event of changes to the AML/CFT/CPF requirements or the operators own AML/CFT/CPF processes and procedures.
- ✓ The requirement for training and awareness applies to all officers and appropriate employees and workers (this includes contractors and those employed via service companies).
- ✓ The GSC would expect the AML/CFT Compliance Officer to be involved in creating, delivering or supervising AML/CFT/CPF training to ensure that it meets the Code requirements, is in line with the businesses risks and is effective.
- ✓ The MLRO should contribute in the area of suspicious activity reporting.

Part 7: Miscellaneous

7.1 Fictitious, Anonymous and Numbered Accounts (Paragraph 28)

The FATF Requirement

FATF Recommendation 10 states that businesses should be prevented from keeping anonymous accounts or accounts in obviously fictitious names.

The Code 2019

28 Fictitious, anonymous and numbered accounts

(1) An operator must not set up or maintain an anonymous account, a numbered account or an account in a name that it knows, or has reasonable grounds to suspect, is fictitious for any new or existing customer.

(2) To avoid doubt sub-paragraph (1) does not apply to occasional transactions that have not been identified as exceeding the occasional transaction threshold.

GSC Guidance and Policy

What? This paragraph prohibits operators from setting up accounts that are anonymous, in fictitious names or numbered.

Why? Accounts must only be established for a named individual or entity so that due diligence measures may be applied including verification of identity and checks to establish whether the customer is a PEP or sanctioned.

When? This paragraph applies at account registration or where the occasional transaction threshold is reached.

It does not apply in respect of occasional transactions under the threshold. For these transactions, fictitious names may be used in nom de plume systems until the customer's true name is established.

Who? This applies to all types of customer including those acting by way of business or on behalf of another person.

How? Operators should put in place measures to both prevent and detect anonymous, potentially fictitious or numbered accounts.

- **"Anonymous"**

  Accounts where information is insufficient to allow positive identification of a person including accounts with no names or partial name.

- **"Fictitious"**

  Accounts in made-up names, nicknames, etc. Test accounts should be clearly identifiable as such and be discounted from reports on real customer accounts.

  Operators allow customers to use player names however, they must always be accompanied with the customer's full name.

- **"Numbered"**

  Multi-digit number known only to the customer and select employees such as a VIP manager. This is prohibited because it adds a layer of secrecy. All employees must be able to easily establish who a customer really is.

  Operators may assign unique customer references to customer however they must always be accompanied with the customer's full name.

Prevention methods include restricting numbers and symbols on name fields on registration pages.

Detection methods include a review of recent registrations to identify any names that appear to be incomplete or fictitious. Where such names are identified, the customer should be asked to confirm their full name with supporting evidence or verification.

Key Messages

Fictitious, Anonymous and Numbered Accounts - Key Messages

- ✓ Accounts must only be established for a named individual or entity so that due diligence measures may be applied including verification of identity and checks to establish whether the customer is a PEP or sanctioned.
- ✓ Operators should put in place measures to both prevent and detect anonymous, potentially fictitious or numbered accounts

7.2 Payment of Online Gambling Winnings (Paragraph. 29)

The FATF Requirement

N/a – there is no FATF Recommendation regarding the payment of online gambling winnings.

The Code 2019

29 Payment of online gambling winnings

Any winnings from online gambling due to a customer may be paid only—

(a) to a card account or other financial facility from which a deposit has previously been made by the customer and which the operator is satisfied stills belongs exclusively to the customer; or

(b) to a card account or other financial facility that the operator is satisfied will result in the customer exclusively receiving the withdrawal,

in accordance with the Online Gambling (Registration and Accounts) (Amendment) Regulations 2014

GSC Guidance and Policy

What? This paragraph details restrictions on the payment of online gambling winnings.

Why? The restrictions help to ensure that funds are not sent from gambling accounts to third parties as this poses an ML/FT/PF risk.

When? The Code specifies these restrictions in respect of winnings however the GSC expects the requirements to be complied with in respect of all account withdrawals regardless of win/loss.

Who? This applies to all types of online gambling account holders.

How? Wherever a customer requests funds to be withdrawn to a different financial facility than that used to deposit, steps should be taken by the operator to determine whether that facility belongs to the customer. This could be done by having the customer send a photo of their bank cards, bank statement or screen grab of an e-wallet.

Financial facility means a bank card, bank account, prepaid card, e-wallet, etc.

It can be perfectly normal for customers to change financial facilities from time to time. Usually this will be due to a bank card expiring. However, Operators should be aware of the "multiple card" typology. This is where a customer attempts to deposit from multiple cards (whether in their own name or someone else's) before withdrawing either to one card or to another facility such as an e-wallet.

Consideration should be given to whether the activity may be unusual or suspicious -

- Has the customer used a larger than normal number of financial facilities?
- Has the customer frequently changed or updated their details?
- Has the request definitely come from the customer or could their account have been hacked?
- Have funds been played through or simply deposited and then withdrawn to another facility?

Responsible Gambling

The use of multiple financial facilities could be a sign that the customer has a gambling problem. Staff should be alert to this and interact with the customer accordingly.

Key Messages

Payment of Online Gambling Winnings - Key Messages

- ✓ The Code details restrictions in respect of online gambling winnings however the GSC expects the requirements to be complied with in respect of all account withdrawals regardless of win/loss.
- ✓ Wherever a customer requests funds to be withdrawn to a different financial facility than that used to deposit, steps should be taken by the operator to determine whether that facility belongs to the customer.
- ✓ Consideration should be given to whether the activity may be unusual or suspicious.

7.3 Transfer of a Block of Business (Paragraph 30)

The FATF Requirement

FATF Recommendation 1 states that simplified due diligence measures may be applied in certain situations where there is a low ML/FT/PF risk.

Recommendation 17 permits reliance on third parties to carry out CDD if certain conditions are met including that responsibility for the CDD remains with the business relying on the third party.

The Code 2019

30 Transfer of a block of business

(1) This paragraph applies where the operator ("the **purchaser**") acquires a customer or group of customers from another entity (the "**vendor**").

(2) The acquired customer or group of customers constitutes a new ongoing customer relationship for the purchaser and customer due diligence in respect of that new ongoing customer relationship may be provided to the purchaser by the vendor, if each of the conditions in sub-paragraph (3) are met.

(3) The conditions referred to in sub-paragraph (2) are that—

(a) the vendor is, or was—

(i) the holder of an online gambling licence issued under section 4 of the Online Gambling Regulation Act 2001; or

(ii) a gambling business—

(A) regulated under the law of a jurisdiction in List C; and

(B) subject to AML/CFT legislation and has procedures and controls that are at least equivalent to the Code; and

(b) the purchaser—

(i) has identified the customer and any known beneficial owner and has no reason to doubt those identities;

(ii) undertakes a risk assessment of the customer and has not identified the customer as posing a higher risk of ML/FT;

(iii) knows the nature and intended purpose of the ongoing customer relationship;

(iv) has taken reasonable measures to establish the source of funds;

(v) has not identified any suspicious activity; and

(vi) has put in place appropriate measures to remedy, in a timely manner, any deficiencies in the customer due diligence of the acquired customer or group of customers.

(4) Where a customer has been identified by the vendor or purchaser as posing a higher risk of ML/FT the purchaser must undertake its own enhanced customer due diligence in respect of that customer in accordance with paragraph 14 (enhanced customer due diligence).

GSC Guidance and Policy

What? This paragraph is a new addition to the 2019 Code and provides operators with the ability to take CDD from another entity when taking on a block of business, if certain conditions are met.

Why? This part of the Code aims to simplify the process of taking on a block of business by removing the need for the operator to obtain CDD direct from the customers.

When? This applies where an operator acquires a block of business i.e. a customer database from another online gambling entity.

Who? Any operator can use this concession if the vendor (the entity supplying the block of business to the operator) either holds or has held an OGRA licence or equivalent in a List C jurisdiction that applies AML/CFT/CPF measures to online gambling in line with the Code.

How?

- **Does the vendor meet the eligibility criteria?**

For IOM entities, the operator must check that the entity has or previously held an OGRA licence. Current operators may be found on the GSC's website. Details of former operators can be provided on request.

For non-IOM entities, the operator must check-

- **That the entity is based in a List C country.**

Please see DHA's website

- **That the entity is regulated.**

The operator should ask the vendor to provide details of their licence type and regulator. The operator should then verify this information.

- **That the entity is subject to AML/CFT/CPF legislation in line with the Code.**

This aspect will require some research. Useful information sources include the MONEYVAL, FATF and regulators' websites.

- **Information required**

The following information is required. It may be provided by the vendor however, it is the operator's responsibility to check that information is present and correct.

- **Identification of the customers and any known beneficial owner.**

This includes full names, addresses and dates of birth plus verification/evidence for those over the threshold. The operator must check to ensure there are no anonymous, fictitious or numbered accounts.

- **Customer risk assessment of all customers.**

Operator's CRA processes will vary. For this reason, any risk score and assessment carried out by the vendor should be used for information only with the operator updating the risk assessment under its own methodologies at the earliest possible opportunity.

- **Source of funds.**

The operator should be provided with detail of the customer's SOF for activity that occurred prior to the transfer of business.

❖ **Treatment of high risk customers in the acquired block of business**

For customers identified as higher risk either by the vendor or the operator, EDD is required and the operator must carry this out. Information provided by the vendor such as source of wealth may be included in the operator's EDD.

❖ **Remediation of shortcomings**

The operator must make plans to remediate any shortcomings in CDD/EDD in a timely manner. It is understood that such remediation could be significant and complex. The GSC therefore expects operators to advise of any significant acquisitions of customers and of plans to remediate shortcomings so that timeframes may be agreed and monitored.

It would be beneficial for operators to add a "flag" to customers that have been acquired as a block of business so that they can easily be identified and reported on for regulatory and remediation purposes.

❖ **Treatment of suspicious activity**

If the operator identifies any suspicious activity the concession may not be used meaning that the operator must carry out CDD on all acquired customers itself without any reliance on the vendor.

Operators should ensure that the vendor does not include in the block of business any customers that have conducted suspicious activity.

Key Messages

Transfer of a Block of Business - Key Messages

- ✓ This part of the Code aims to simplify the process of taking on a block of business by removing the need for the operator to obtain CDD direct from the customers.
- ✓ This applies where an operator acquires a block of business i.e. a customer database from another online gambling entity.
- ✓ Any operator can use this concession if the vendor (the entity supplying the block of business to the operator) either holds or has held an OGRA licence or equivalent in a List C jurisdiction that applies AML/CFT measures to online gambling in line with the Code.
- ✓ For a vendor to meet the eligibility criteria it must check:
  - That the entity is based in a List C country;
  - That the entity is regulated;
  - That the entity is subject to AML/CFT legislation in line with the Code.
- ✓ The following information is required:
  - Identification of the customers and any known beneficial owner;
  - CRA of all customers;
  - SOF.

7.4 Foreign Branches and Majority Owned Subsidiaries (Paragraph 31)

The FATF Requirement

FATF Recommendation 18 states that businesses should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements, implementing the FATF Recommendations through the groups' AML/ CFT programmes.

The Code 2019

31 Foreign branches and majority-owned subsidiaries

(1) An operator must ensure that any branch or majority-owned subsidiary in a jurisdiction outside the Island takes measures consistent with this Code and guidance issued by the Commission relating to AML/CFT, to the extent permitted by the laws of that jurisdiction.

(2) If the host country does not permit the proper implementation of measures consistent with this Code and guidance issued by the Commission for AML/CFT, the operator must—

(a) apply appropriate additional measures to manage the ML/FT risks; and

(b) inform the Commission within a reasonable timeframe.

(3) To avoid doubt, the requirements of this paragraph apply only in respect of foreign branches and majority-owned subsidiaries undertaking activities that are, or if carried on in the Island would be regulated under—

(a) the Online Gambling Regulation Act 2001*;*

(b) the Casino Act 1986; or

(c) the Gaming, Betting and Lotteries Act 1988.

GSC Guidance and Policy

What? This paragraph requires operators to apply IOM-standard AML/CFT/CPF procedures and controls to their foreign branches and subsidiaries.

Why? The FATF Recommendations aim to create a level playing field of requirements around the globe. In particular, they aim to prevent global businesses from having an arm of their business with poor AML/CFT/CPF controls that acts as the gateway for illicit funds into their structure.

Who? This requirement applies any operator (online, casino or bookmaker) that has foreign branches or majority-owned subsidiaries. For clarity, this does not mean that IOM requirements must be pushed up the structure, to head office or across to sister companies.

The GSC does not expect these requirements to apply to many operators due to the nature of their structures and would be pleased to field enquiries from any operators that may be unsure whether the requirements apply to their structure.

How? The GSC expects the operator's AML/CFT Compliance Officer to advise the board on how to implement the IOM standards.

In some jurisdictions, there may be legislation that conflicts with the IOM AML/CFT/CPF laws making it impossible to comply. In such instances, the operator must take steps to address the resulting AML/CFT/CPF risk and liaise with the GSC within a reasonable timeframe.

Part 8: Offences and Revocations

8.1 Offences (Paragraph 32)

The FATF Requirement

FATF Recommendation 35 states that countries should ensure there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, where there is a failure to comply with AML/CFT requirements. Sanctions should be applicable not only to businesses, but also to their directors and senior management.

The Code 2019

32 Offences

(1) Any person who contravenes this Code is guilty of an offence and liable—

(a) on summary conviction to custody for a term not exceeding 12 months or to a fine not exceeding level 5 on the standard scale, or to both; or

(b) on conviction on information to custody not exceeding 2 years or to a fine, or to both.

(2) In determining whether a person has complied with any of the requirements of any part of this Code a court may take account of any relevant supervisory or regulatory guidance given by the Commission which applies to that person.

(3) In proceedings against a person for an offence under this paragraph, it is a defence for the person to show that it took all reasonable measures to avoid committing the offence.

(4) If an offence under this paragraph is committed by a body corporate and it is proved that the offence—

(a) was committed with the consent or connivance of an officer of the body; or

(b) was attributable to neglect of the part of an officer of the body,

the officer, as well as the body, is guilty of the offence and liable to the penalty provided for it.

GSC Guidance and Policy

What? This paragraph sets out the criminal offence of failing to comply with the Code and the related penalties. It also states that supervisory and regulatory guidance will be taken into consideration when determining whether a person has complied and that taking all reasonable measure to comply is a defense.

Offences in the primary law for ML, FT, sanctions and proliferation are detailed later in this guidance.

Why? Criminal prosecution of Code breaches is one of a range of possible actions that could be taken in relation to AML/CFT/CPF failings. The available criminal and civil (regulatory) actions together constitute a "range of effective, proportionate and dissuasive sanctions" as required by the FATF.

When? Criminal prosecution will be pursued in circumstances where the public interest requires a prosecution.

Who? Code breaches are committed by the operator as an entity. Offences are also committed

by officers of the entity if the offence was committed with their consent or connivance or because of neglect on their part.

Officer is a defined term and includes directors and secretaries. The term does not include MLROs or AML/CFT Compliance Officers although they may be held accountable (as a senior manager) under the Gambling (AML/CFT) Act which could result in the Commission determining them as a "not fit and proper" person to hold such a role.

How? Guidance on the Gambling (AML/CFT) Act including GSC's AML/CFT enforcement policy can be found on the AML/CFT Guidance page of the GSC's website.

- **Standard scale of fines**

  Details of the minimum and maximum fines can be found at www.legislation.gov.im

  At the time of writing this guidance, a level 5 fine can be up to £10,000.

Part 9: Links & Further Information

9.1 Legislation

Please see www.legislation.gov.im for more information on current IOM Legislation.

POCA is the primary law regarding ML.

ATCA is the primary law for FT.

9.2 Sanctions and Proliferation

More information about sanctions and proliferation financing can be found on the Isle of Man Customs and Excise website. The GSC recommends that all regulated entities sign up to the IOM Customs and Excise News RSS feed. IOM Customs and Excise have a number of notices and documents which may be of use to regulated entities, these include:

Financial Sanctions - Guidance

Financial Sanctions Relating to Terrorism - Guidance

Financial Sanctions Relating to Proliferation - Guidance

Trade-Based Money Laundering Guidance