GIBRALTAR FINANCIAL SERVICES COMMISSION

Systems of control to prevent the financial system from being used for money laundering, terrorist financing or proliferation financing activities

The GFSC is working to update the Guidance Note and whilst every reasonable effect is made to ensure that the information provided on the GFSC's website is accurate, no guarantee for the accuracy of the information is made. Therefore, where there is a discrepancy between the contents of the Guidance Note and the requirements set in the Act or the Directive, the entity is to refer to and comply with the requirements set in the Directive.

The GFSC does not give any express or implied warranty as to the accuracy of the information contained in this document. The GFSC does not accept any liability for error or omission.

December 2022

www.gfsc.gi

Contents

CHAPTER I

1 Introduction

These Guidance Notes (the Notes) represent a major step forward in the approach taken by the regulator in setting out the requirements in respect of systems of controls that firms need to have in place in order to prevent the misuse of the financial services sector for criminal activity.

These Notes reflect the revised 40 FATF recommendations as well as the provisions of the Money Laundering Directive (MLD)[1] as they affect the regulated financial sector for which the GFSC has responsibilities. These notes also give effects to implementing measures published by the EU since

[1]http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

the Directive was published e.g. on Politically Exposed Persons, Reduced Due Diligence Measures and information accompanying fund transfers.

1.1 About these Notes

The Risk-based approach is prevalent throughout the Notes. By definition, it is impossible to reconcile a risk-based approach with prescriptive requirements. A prescriptive approach may be favoured by some firms, as this gives clarity in relation to the regulator's expectations, but this goes against the concept of applying a risk-based approach. Notwithstanding this, these Notes have introduced the concept of a Requirement and an expectation. These are highlighted throughout the Notes and can be defined as:

Rx *Requirement. An action or process that must be applied. Compliance with each of these requirements must be documented by the firm. The firm's compliance with the requirement will be measured by the GFSC, both in terms of its adequacy to the firm's own situation and as to how the practice matches the requirement.*

! *Expectation. A process that a firm must apply in order to give effect to a requirement. The GFSC will need to see how the firm's senior management has applied this to meeting the requirements of the Notes.*

In both Requirements and Expectations, there are no detailed processes which a firm could cross-check against their own procedures. This is the limit of the level of detail that the Notes will prescribe unless there is an international obligation that must be met when certain criteria are met.

Risk-based must be read "as it applies to the firm" or there would be no risk-based elements to the Notes. Each firm will have a different view of the risks that it faces and what processes are already in place, in the firm itself or within the group that addresses those risks.

Because not all regulated firms are large enough to have developed a risk management role, these Notes outline, in the appendices, a suitable risk framework which they could adopt for these purposes. Firms are not obliged to adopt this methodology but in the absence of a better approach, this methodology should provide the essential elements to ensure compliance with the same.

Overarching the requirements are six Statements of Principle. How a firm is required to meet these Statements of Principles is then explained in the chapters that follow.

The context in which compliance with the Notes is mandated must be clearly understood.

1.2 Applicable Legislation

The following is a list of legislation, which is applicable to the Notes:

- Drug Trafficking Offences Act (part V of which was repealed);
- Proceeds of Crime Act 2015 (POCA);
- Terrorism Act 2018;
- The Terrorism (United Nations Measures)(Overseas Territories) Order 2001;
- The Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002;
- Sanctions Act 2019; and
- Orders made under the Export Control Act 2005.

Applicable UN Security Council Resolutions:

- The EU implements all UN Security Council Resolutions. For more information on this, please refer to Appendix 3 of these Notes under section titled “Countries and Territories on which sanctions apply”.

CHAPTER II

2 Legal Basis for the Notes

These Notes are "supervisory or regulatory" guidance for the purposes of Section 33(2) of the Proceeds of Crime Act 2015 and have been issued:

a) Under the Proceeds of Crime Act 2015, as read with Section 23(g) of the Interpretation and General Clauses Act;
b) under the powers conferred upon the Commission appointed under Section 37 of the Financial Services Act 2019 in pursuit of the functions outlined in Section 22 of that Act;
c) by the Gibraltar Financial Services Commission;

2.1 Scope and application

The coverage of the Crime (Money Laundering and Proceeds) Act (since repealed and replaced by the Proceeds of Crime Act 2015) was extended with the transposition of the MLD to include non-financial sectors. The HM Government of Gibraltar has produced its own Guidance Notes for business sectors which accept large cash payments for goods. These Guidance Notes only, therefore, cover the following financial services providers:

- Banks and Building Societies whether or not operating in or from Gibraltar as a branch or locally incorporated institution;
- Electronic Money Institutions;
- Insurance Managers;
- Life insurance distribution;
- Audit firms;
- Investment services;
- Regulated Markets and Stock Exchanges;
- Trust and Company Services Providers;
- Pension related activities e.g. personal pension schemes, advisory services, etc.;
- Mortgage Credit Intermediaries;
- Life insurance Companies;
- Currency exchangers/bureau de change;
- Firms providing payment services;
- Any collective investment scheme (recognised or authorised) or any authorised restricted activity caught by the Financial Services (Collective Investment Schemes) Act 2011;
- Statutory Auditors and Audit Firms;
- Insolvency Practitioners;
- DLT Providers;
- Accountants;
- Tax Advisors; and
- Other VASP activities that include:
    - undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of DLT or a similar means of recording a digital representation of an asset.

- persons that, by way of business, exchange, or arrange or make arrangements with a view to the exchange of– (a) virtual assets for money; (b) money for virtual assets; or (c) one virtual asset for another.

Reference to "Firms" throughout the Guidance Note refers to all the entities listed above.

2.2 Implementation

These Notes came into effect on 15 December 2007. The requirements and expectations laid out in these notes apply to all business relationships and occasional transactions commenced or entered into after this date.

2.3 Is compliance compulsory?

Section 33(2) of the POCA provides, inter alia, as follows:

"(2) In deciding whether a person has committed an offence under sub-section(1), the courts must consider whether he followed any relevant guidance which was at the time issued by a supervisory authority or any other appropriate body."

The Notes are drawn up by the GFSC in light of the above provisions.

Therefore, the notes are intended to interpret the requirements of the POCA in a practical manner. They intend to illustrate good industry practice. The key question, however, is whether a relevant financial business is obliged to comply with the provisions of the Notes.

The word "must" in section 33(2) of the POCA imports an obligation on the Courts to "consider" the Notes in determining whether a person has complied with the POCA.

It is the view of the GFSC that the provisions and the structure of the POCA must be taken as a whole. Part III creates an obligation on relevant financial businesses to establish and maintain certain standards and procedures to combat money laundering, terrorist financing and proliferation financing – the Act is not, however, prescriptive on how these requirements should be fulfilled. It is suggested that it was clearly intended that this would be left to industry practice as embodied in the Notes and that a judge, in determining whether a breach had been committed, would be obliged to consider such guidance issued by the regulatory authorities.

By way of summary:

a) the Notes are written in such a way that compliance with its terms is obligatory;
b) if there is non-compliance with the Notes, a judge must take into account such noncompliance when determining whether a person is in breach of the provisions of section the POCA;
c) the end result of the combination of (a) and (b) immediately above is that a judge, save in an exceptional case, must hold that a person who does not comply with the terms of the Notes is in breach of the provisions of the POCA.

It follows that, if a person does not adhere to the provisions of the Notes, such person would be applying the standards of practice falling below best market practice and would not be held to have taken all reasonable steps and exercised all due diligence.

2.4 What action can be taken against firms that do not comply?

As well as the criminal sanctions for failure to comply with the POCA, TO and the UN Orders, the GFSC will consider the "fit and proper" status of its officers, for the purposes of assessing its compliance with the regulatory and supervisory Acts under which it exercises its powers.

Firms are also required to implement systems of control under the legislation in which they are authorised. As a result, the Authority that issued this authorization may take regulatory action against a firm whose systems of control do not meet the requirements of these Notes.

These powers range from the imposition of penalty fees in certain circumstances, the imposition of conditions or directions and ultimately, the revocation of the firm's authorization.

CHAPTER III

3 National Risk Assessment (NRA)

In April 2016, HM Government of Gibraltar published its first National Risk Assessment. The risks posed have since been reviewed and updated NRAss have been published in September 2018[2] and August 2020[3]. The NRA takes into account, and is reflective of, the EU Supranational Risk Assessment.

A NRA is defined as "An Analysis of Theoretical Threats, Vulnerabilities and Risks in a Money Laundering and Terrorist Financing Context" – as per the Financial Action Task Force best practice guidelines to all member countries/associated countries and territories.

The process is led by both the Minister for Justice and the Minister for Financial Services, as both portfolios have a vested interest in the Assessment and the mitigation of the outcomes.

Both public and private sector input was sought from the commencement, in order to identify as broad a range of threats and vulnerabilities as possible, both from an enforcement angle as well as a customer facing and transactional perspective. A series of workshops and presentations were held in which all sectors were represented.

HM Government of Gibraltar appointed a project coordinator to design and oversee the implementation of the methodology. On 7 July 2016, the Minister with responsibility for financial services appointed the Attorney General as National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing.

[2] http://www.fsc.gi/uploads/2018%20NRA.pdf
[3] https://www.fsc.gi/uploads/National%20Risk%20Assessment%202020.pdf

CHAPTER IV

4 Statements of Principle

The Notes adopt a new approach to the requirements that each firm must put in place in order to mitigate the risks that it is exposed to.

The following principles outline these requirements and are explained in more detail in the following chapters.

SP1 The senior management of a firm is responsible for ensuring that the systems of control operated in the firm appropriately address the requirements of both the legislation and these guidance Notes.

SP2 Firms must adopt a risk-based approach to these statements of principle and their requirements.

SP3 All firms must know their customer to such an extent as is appropriate for the risk profile of that customer.

SP4 Effective measures must be in place that require firms to have both internal and external reporting requirements whenever money laundering, terrorist financing or proliferation financing is known or suspected.

SP5 The firm will establish and maintain effective training regimes for all of its officers and employees.

SP6 Firms must be able to provide documentary evidence of their compliance with the legislation and these Notes.

CHAPTER V

SP1 **The senior management of a firm is responsible for ensuring that the systems of control operated in the firm appropriately address the requirements of both the legislation and these Guidance Notes.**

5 Senior Management's Responsibilities and the Role of the MLRO

Section 26 of the POCA imposes a requirement on every relevant financial business under legislation to maintain policies and procedures to prevent money laundering. Section 34 supplements this requirement by apportioning the responsibility amongst directors, managers, company secretary or other officers, members or partners if such failings can be attributable to the neglect of such persons. For the purposes of these Notes such persons are known collectively as "senior management"

These Notes carry these requirements forward throughout and the GFSC will be ensuring that firm's senior management are held accountable for any failings in the systems of control required to be implemented by the legislation or these Notes.

5.1 Accountability for systems of control to prevent and report money laundering, the financing of terrorism, or proliferation financing

R2 Senior management of firms must ensure that the following processes have been adopted:

a. The allocation to a director or senior manager overall responsibility for the establishment and maintenance of effective AML,CFT and CPF systems of control in compliance with the Proceeds of Crime Act; and the appointment of a person with adequate seniority and experience as Money Laundering Reporting Officer (MLRO);
b. That appropriate training on money laundering is identified, designed, delivered and maintained to ensure that employees are aware of, and understand;
    1. their legal and regulatory responsibilities and obligations;
    2. their role in handling criminal property and terrorist financing;
    3. the management of the money laundering, terrorist financing and proliferation financing risk;
    4. how to recognise money laundering, terrorist financing and proliferation financing transactions or activities; and
    5. the firm's processes for making internal suspicious transaction reports.
c. That regular and timely information is made available to senior management relevant to the management of the firm's money laundering, terrorist financing and proliferation financing risks;
d. That the firm's risk management policies and methodology are appropriately documented including the firm's application of those policies and methodologies; and
e. That appropriate measures to ensure that money laundering, terrorist financing and proliferation financing risks are taken into account in the day-to-day operation of the firm, including in relation to:
    1. the development of new products;
    2. the taking-on of new customers; and
    3. changes in the firm's business profile.

f. Senior management of the firm must ensure that the MLRO has sufficient resources available to him, including appropriate staff and technology. This should include arrangements to apply in his temporary absence; and

g. Employee screening.

Many firms outsource some of their systems and controls and/or processing outside of Gibraltar. It is important that outsourcing does not result in reduced standards or requirements being applied.

Firms cannot contract out of their regulatory responsibilities, and therefore remain responsible for systems of control in relation to the activities outsourced.

In all instances of outsourcing, the delegating firm bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the provider of the outsourced services has in place, satisfactory AML/CFT/CPF systems, controls and procedures, and that those policies and procedures are up to date, to reflect changes in requirements of Gibraltar legislation and these Notes.

5.2 Appointment and role of the Money Laundering Reporting Officer

The overall responsibility for money laundering prevention lies with senior management and controllers of a firm.

R3 The MLRO is responsible for the oversight of the firm's anti-money laundering activities and is the key person in the implementation of the anti-money laundering strategy of the firm.

R4 The MLRO needs to be senior, to be free to act on his own authority and be informed of any relevant knowledge or suspicion in the firm.

! The type of person appointed as MLRO will vary according to the size of the firm and the nature of its business, but he should be sufficiently senior to command the necessary authority but not, generally, be a member of senior management themselves. Larger firms may choose to appoint a senior member of their compliance, internal audit or fraud departments. In smaller firms, it may be appropriate to designate the Operations Manager.

When several subsidiaries operate closely together within a group, there is much to be considered for designating a single MLRO at group level. The MLRO shall be an employee of the firm, whether as part of its governing body, management or staff and be primarily based in Gibraltar.

R5 The MLRO will act as the "appropriate person" required to be appointed under Section 28 to receive and process internal and external suspicious transaction reports.

R6 The MLRO will act as a central point of contact with law enforcement agencies, in order to handle the reported suspicions of their staff regarding money laundering, terrorist financing and proliferation financing.

R7 It is not appropriate, in the case of multinational firms or branches operating in Gibraltar (and for the purposes of the Proceeds of Crime Act 2015) for the MLRO to be located outside Gibraltar.

! Where a firm has branches or offices in other jurisdictions, the functions of the MLRO may be delegated to other persons within those branches or offices. Where such functions are delegated, the GFSC will expect the MLRO to take ultimate responsibility for ensuring that the requirements of the Notes are applied to those operations. See 5.4 below for more information.

5.2.1 Roles of the MLRO

Section 28 imposes on the MLRO, a significant degree of responsibility. He is required "to determine" whether the information or other matters contained in the transaction report he has received gives rise to knowledge or suspicion that a customer is engaged in money laundering, terrorist financing or proliferation financing.

! The MLRO must take steps to validate the suspicion in order to judge whether or not a report should be submitted to GFIU. In making this judgement, he must consider all other relevant information available to him, concerning the transaction or applicant to whom the report relates. This may require a review of other transaction patterns or business in the same name, the length of the business relationship and referral to identification records held. If after the review, he decide that there are no facts that would negate the suspicion, then he must disclose the information to GFIU. The MLRO also needs to pass onto GFIU issues that he thinks is appropriate and can be expected to liaise with GFIU on any questions of whether to proceed with a transaction in the circumstances.

R8 Section 28 requires that the MLRO has reasonable access to information that will enable him to undertake his responsibility. In addition, the reference in Section 28 to "determination" implies a process with some formality. It is important therefore that the MLRO keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of his reasons for his decision.

The MLRO is expected to act honestly and reasonably, to make his determinations in good faith. Provided the MLRO or an authorised deputy acts in good faith in deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgement is later found to be wrong.

! Care should be taken to guard against a report being submitted as a matter of routine to GFIU without undertaking reasonable internal enquiries to determine that all available information has been taken into account**.**

5.3 Reporting by the MLRO to Senior Management

! An MLRO will support and co-ordinate senior management focus on managing the money laundering/terrorist financing/proliferation financing risk in individual business areas. He will also help ensure that the firm's wider responsibility for forestalling and preventing money laundering/terrorist financing/proliferation financing is addressed centrally, allowing a firm-wide view to be taken of the need for monitoring and accountability.

R9 A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure they manage the money laundering/terrorist financing risk effectively. Oversight of the implementation of the firm's AML/CFT/CPF policies and procedures, including the operation of the risk-based approach is the responsibility of the MLRO, under delegation from senior management. He must therefore ensure that appropriate monitoring processes and procedures across the firm are established and maintained.

R10 At least annually, the senior management of a firm, with five or more full-time employees, must commission a report from its MLRO that assesses the operation and effectiveness of the firm's systems of control in relation to managing money laundering, terrorist financing and proliferation financing risks. The report must include:

a. The numbers and types of internal suspicious transaction reports that have been made internally and the number of, and reasons why, these have or have not been passed onto GFIU;
b. bringing to the attention of senior management, areas where the operation of AML/CFT/CPF controls should be improved, and proposals for making appropriate improvements;
c. the progress of any significant remediation programs; and
d. the outcome of any relevant quality assurance or internal audit reviews of the firm's AML/CFT/CPF processes, as well as the outcome of any review of the firm's risk assessment procedures

! The MLRO's Annual Report can be found under the Templates section on the GFSC's Financial Crime Approach web page.

In practice, senior management should determine the depth and frequency of information they feel necessary to discharge their responsibilities. The MLRO may also wish to report to senior management more frequently than annually, as circumstances dictate.

R11 A firm's senior management must consider the MLRO's annual report, and take any necessary action to remedy deficiencies identified in it, in a timely manner**.**

5.4 Applicability of systems of control to overseas branches, subsidiaries or outsourcing of functions

Gibraltar is concerned with money laundering which takes place in Gibraltar and does not seek to apply its money laundering legislation extra-territorially (i.e. within other countries).

R12 Where a Gibraltar firm has overseas branches, subsidiaries or associates where control can be exercised, it is required that a group policy be established to the effect that all overseas branches and subsidiaries must ensure that its anti-money laundering strategies, internal controls, procedures and processes are undertaken at least to the standards required under Gibraltar law and Notes or, if the standards in the host country are more rigorous, to those higher standards.

R13 Reporting procedures and the offences to which the money laundering legislation in the host country relates must nevertheless be adhered to in accordance with local laws and procedures. Where local laws prohibit the application of Gibraltar equivalent practices, or higher standards, the firm must inform the GFSC of this. Where meeting local requirements would result in a lower standard than in Gibraltar, this should be resolved in favour of Gibraltar.

Where suspicions of money laundering in overseas operations of a firm arise, these must be reported within the jurisdiction where this arose and records of the related transactions are held. There may also be a requirement for a report to be made to the GFIU.

R14 Where operational activities are undertaken by staff in other jurisdictions (for example, overseas call centres), those staff must be subject to the AML/CFT/CPF policies and procedures that are applicable to Gibraltar-based staff, and internal reporting procedures be implemented to ensure that all suspicions relating to Gibraltar-related accounts, transactions or activities are reported to the nominated officer in Gibraltar. Service level agreements will need to cover the reporting of management information on money laundering prevention, and information on training, to the MLRO in Gibraltar.

In some circumstances, the outsourcing of functions can actually lead to increased risk - for example, outsourcing to businesses in jurisdictions with less stringent AML/CFT/CPF requirements than in Gibraltar.

R15 All firms that outsource functions and activities should therefore assess any possible AML/CFT/CPF risks associated with the outsourced functions, record the assessment and monitor the risks on an ongoing basis.

R15A A payment institution which uses agents must ensure it;

1. includes such agents within the policies and procedures;
2. communicate the policies and procedures to the agents; and
3. monitor the agents' compliance with such policies and procedures.

5.5 Independent Audit

Section 26(1A) of POCA introduced the following requirement:

A relevant financial business must undertake an independent audit function for the purposes of testing the policies, controls and procedures referred to in subsection (1), and such function shall have regard to the size and nature of the business.

Subsection (1) states as follows:

A relevant financial business must establish and maintain appropriate and risk-sensitive policies, controls and procedures, proportionate to its nature and size, relating to:

a) customer due diligence measures and ongoing monitoring;
b) reporting;
c) record-keeping;
d) internal control;
e) risk assessment and management;
f) compliance management including the allocation of overall responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level (being director, senior manager, or partner); and
g) employee screening.

The policies, controls and procedures referred to above shall be proportionate to the nature and size of the business. The business must also monitor their implementation, including enhancing these where higher risks are identified.

Frequency/Scope

The frequency and scope of the independent audit is to be determined by the firm, adopting a risk based approach.
An assessment is expected to be conducted at least annually, to consider the extent and scope of an independent audit for the year.

Independence

The Independent Audit function should be performed by individuals who are not involved with a firm's compliance function. It is the responsibility of a firm to determine the independence of individuals. Individuals tasked with performing the function may be from within the firm or external, having regard to ensuring the independence of the role. Some firms may have the capacity and resources for an in-house audit function, whereas others may wish to outsource this function to a reputable firm familiar with undertaking audits of this nature. An external audit may prove to be a useful tool irrespective of whether a firmfirm has an in-house audit team as an additional check on the effective operation of a firm'sfirm's compliance programme, however, there is no requirement to engage the services of an

outside firm in order to carry out this function. It is the responsibility of the firm to determine the independence of the individuals and this should be evaluated at least annually.

The Role of Senior Management

Senior Management should monitor and review the effectiveness of the Independent Audit function.

CHAPTER VI

SP2 **Firms must adopt a risk-based approach to these statements of principle and their requirements.**

6 Risk-Based Approach

The level and intensity of any firm's approach to the mitigation of the risks it faces must be based on a suitable methodology which address the issues and concerns that it faces. No two firms are the same and the scope of their risk mitigation programme must be determined, therefore, by the existing systems of control in place as well as a number of external factors that are borne to bear on the firm.

Whereas it was traditionally the case that a firm's processes to mitigate risks were customer centric, this is no longer applicable, as the complexity of the requirements has increased.

6.1 Risk Profiling a Business Relationship

R16 A risk-profile of a business relationship needs to take into consideration the following four risk elements that are present in every business relationship:

a. Customer Risk
b. Product Risk
c. Interface Risk
d. Country Risk

Together, the four risk elements above are combined to produce a risk-profile. It is the results of this risk profile and the firm's risk appetite that will determine the intensity of the documentation and other process that will need to be obtained at the commencement of a business relationship or as an ongoing requirement.

R17 A firm will need to be able to demonstrate that it has a methodology for assessing the risk profile of a business relationship, and that this methodology is suitable for the size and nature of the firm's business and that practice matches the methodology. An appropriate client risk matrix that considers the four elements of a risk-based approach, as well as other key risk factors should be developed and employed to accurately assess the risk a client poses to the firm, from a money-laundering, terrorist financing, proliferation financing and other illicit activities perspective.

The GFSC will verify that a methodology has been successfully designed and implemented through its on-site and risk-assessment supervisory processes.

See Appendix 2 for further information on how to construct a client risk assessment.

6.2 The four elements of a risk-based approach

6.2.1 Customer Risk

This is the identification of the risk posed by the type of customer.

Each firm will have a different view of the type of customer that it wishes to service and those that it does not. That decision has normally already been made either tacitly or implicitly through the business plan, strategy of the firm or by the product range that it offers.

R18 These Notes require that an assessment be conducted on the risk that different types of customers pose in relation to the threat that they will launder proceeds of crime, fund terrorist activity or be involved in other types of illicit activities. The intensity of the due diligence conducted on the individual must therefore increase with the perceived or potential threat posed by that business relationship.

6.2.1.1 Individuals

The threats posed by different types of individuals is mainly attributable to the nature of their economic activity or source of wealth. For example, the risk to a firm that a salaried employee whose only transactions through a business relationship are those derived from electronic payments made by his employer are going to be much lower than an individual whose transactions are cash based with no discernible source for this activity. The country in which the individual created, or sourced their income also needs to be considered in the overall threat environment.

Proof of identity ensures that the risks arising out of identity theft and other fraudulent activity are mitigated.

R19 Firms must include, in their methodology, a statement of the basis upon which business relationships with individuals will be scored in light of their source of income or wealth.

6.2.1.1.1 Known or Suspected Terrorists and individuals subject to sanctions or other economic measures

Individuals, charities, non-profit organizations or companies themselves may be associated with, or be suspected or known to be terrorists or involved with terrorist activities. Similarly, individuals may themselves be subject to sanctions or other international initiatives, which may sometimes be linked to close family members.

Irrespective of the risk score of the customer obtained above, the firm is required to introduce enhanced due diligence checks on the customer, the moment it knows or suspects that the customer may fall into this category. (See section 6.2.4.3 for more information)

In many cases, this will trigger a requirement to inform the authorities of the presence of these individuals.

The issue that concerns most firms is how to ensure that an individual who has already been through the application process is not then found to have been added to one of the list of names of known or suspected terrorists.

Lists of known or suspected terrorists are published by various international and national agencies. Third party providers are also able to provide consolidated lists. Lists relevant to Gibraltar can be found on the GFSC website at - https://www.fsc.gi/financialcrime/sanctionsandterrorism

! See 8.4 below for requirements in relation to named or suspected terrorists and Appendix 3 – Countries and territories with equivalent legal frameworks or those requiring enhanced due diligence for measures that need to be applied against undertakings and individuals subject to international sanctions.

6.2.1.1.2 Politically Exposed Persons

The term "politically exposed persons" is defined as:

"natural persons who are or have been entrusted with prominent public functions."

For these purposes;

1. 'natural persons who are or have been entrusted with prominent public functions' include the following:
   (a) heads of State, heads of government, ministers and deputy or assistant ministers;
   (b) members of parliaments or similar legislative bodies;
   (c) members of governing bodies of political parties;
   (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
   (e) members of courts of auditors or of the boards of central banks;
   (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
   (g) members of the administrative, management or supervisory bodies of State-owned enterprises; and
   (h) directors, deputy directors and members of the board or equivalent function of an international organization.
2. 'family members' includes the following:
   (a) a spouse;
   (b) a partner considered by national law as equivalent to the spouse;
   (c) children and their spouses or partners; and
   (d) parents.
3. 'persons known to be close associates' shall include the following:
   (a) any individual who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in paragraph 1; and
   (b) any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 1.

! Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function, the firm must, for at least 12 months after ceasing to be so entrusted, take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

The concerns relating to this type of risk are mitigated by having adequate processes through which a firm can determine the source of income or wealth.

Specific risk based measures need to be adopted to reduce the risks inherent in dealing with PEPs.

Under the MLD, family members or close associates of a PEP may not be considered PEPs themselves, unless they themselves meet the definition of a PEP. Nonetheless, they should be subject to the same due diligence and ongoing monitoring requirements as PEPs.

R20 The systems of control that firms must adopt to reduce the risks associated with establishing and maintaining business relationships with PEPs are that:

a. the firm must establish and document a clear policy and internal guidelines, procedures and controls regarding such business relationships;
b. maintain an appropriate risk management system to determine whether a potential customer or an existing customer is a PEP;
c. decisions to enter into business relationships with PEPs to be taken only by senior management; and
d. business relationships which are known to be related to PEPs must be subject to proactive monitoring of the activity on such accounts.

! The monitoring of the accounts is necessary so that any changes are detected, and consideration can be given as to whether such change suggests corruption or misuse of public assets. This includes scrutiny of receipts of large sums from government bodies, state owned activities, or governments and central bank accounts. See Section 7.8 for more information on the monitoring requirements under the Notes.

See section 6.2.4.2 for more requirements on PEPs re Country Risk.

6.2.1.2 Legal Entities

Corporate structures, trusts and partnerships are recognised internationally as vehicles through which opacity in financial transactions can easily be introduced. These entities could be used by criminals to add layers between criminal activity and those benefiting from the same.

Additionally, facilities which add layers of complexity, e.g. nominee shareholdings, declarations of trust, powers of attorney have their place in legal structures, tax and estate planning scenarios but are just as attractive to criminals for the same reasons. It should be noted that corporate nominee shareholders may pose a greater risk and firms should ensure that in these cases the ultimate beneficial owner is always identified and verified i.e. the natural person who ultimately owns or controls the legal entity as detailed under R61.

! Firms must recognise the risks that facilities which add complexity or opacity to a legal entity pose to their business and have adequate systems of control to ensure that these risks are properly mitigated.

As with other legal forms, legal entities may come in a variety of different shapes and sizes but their economic activity will be much more varied.

Firms need to include in their risk assessment process, a recognition of the risk posed by the economic activity being conducted through the legal entity.

It is evident that in order for the above requirement to be effective, a firm must have sufficient information about the client companies and its activities, as far as it is appropriate for the services being provided to it. (See Section 7.7.2 on the requirements in relation to the documentation in relation economic activity.)

Legal entities do not run themselves, they are directed by their directors and controlled by its members and beneficial owners or its assets controlled by the trustees. The influence that these persons can have on the client company/trust or partnership is just as an important factor in the risk assessment process as the entity's activities.

! Firms must ensure that the risks posed by the beneficial owners, officers, shareholder, trustees, settlors and managers of a legal entity are reflected in the risk profile of the client company.

6.2.1.2.1 - Publicly listed entities

No further steps to verify identity over and above usual commercial practice, will normally be required where the applicant for business is known to be a listed entityentity (as defined in Section 7 of POCA).

It shall be necessary only for the relevant financial business to record the Listed Entity's entry in the public register of the regulated market in which the Listed Entity's shares are trading, and to retain a copy of such entry.

6.2.1.2.2 - Credit or Financial Institutions

Verification of identity is not required when there are reasonable grounds for believing that the applicant for business is itself a financial institution in Gibraltar or a jurisdiction with an equivalent AML/CFT/CPF regime. What constitutes reasonable grounds is not defined, but these might mean ensuring that the credit or financial institution does actually exist (e.g. that it is listed in the Bankers' Almanac, or is a member of a regulated or designated investment exchange); and that it is also regulated. In cases of doubt, the relevant regulator's list of institutions can be consulted. Additional comfort can also be obtained by obtaining, from the relevant institution evidence of its authorization to conduct financial and/or banking business.

For Gibraltar based firms, the GFSC publishes a list of regulated firms on its website (www.fsc.gi). Verification that the applicant for business appears on these lists is sufficient to satisfy the minimum due diligence measures. Care, however, must be taken to distinguish between those that fall under the definitions of Credit Institutions or Financial Institutions, which fall under this exemption, and those that do not (e.g. company managers, professional trustees, insurance managers or insurance intermediaries).

Unregulated credit or financial businesses should be subject to further verification in accordance with the procedures for companies or businesses

6.2.2 Product Risk

This is the risk posed by the product proposition itself. Some products are inherently less attractive to criminals than others are.

R21 Firms must document their product range against the perceived attraction for the products to be used for criminal activity and implement systems of control to mitigate or reduce these risks.

Firms must undertake the risk assessment for new products, business practices, delivery mechanisms and developing technologies (for both new and existing products) prior to the launch of these. Consequently, it must act appropriately to manage and mitigate the risks.

6.2.2.1 Anonymous Accounts/Products that offer a layer of opacity

Because one of the primary aims of a criminal is to create as much distance between himself, the criminal act and the proceeds from that act. Anonymous accounts/business relationships or

facilities that allow the customers to establish a business relationship using false or fictitious names are specifically prohibited.

Firms must subject the owner and beneficiary of an existing anonymous account or anonymous passbook or anonymous safe-deposit box to customer due diligence measures as soon as possible and in any event before such account or passbook is utilised.

R22 Firms may not permit their products to be used using obviously fictitious names or where the customer's name is not identified.

! There are many circumstances where a firm may not want to include the customer's name or details on the account name or customer file in order to provide a level of privacy within the organisation itself. However, this does not mean that the customer is not known to the firm and these details may be kept in a more secure environment within the firm itself. The due diligence records of that customer must, however, be made available to the senior management, MLRO, enforcement agencies and the regulators, should this be required.

6.2.2.2 Bank accounts

The range of bank accounts offered by modern financial institutions are varied and the characteristics of each type of bank account may increase the risk posed to the firm.

At the lowest end of the risk spectrum will be passbook type accounts that require the customer to be physically present to make withdrawals and where there are no third party payments permitted. The highest risk bank account will be those where the account can be accessed and operated on-line and through which third party payments can be effected.

The risks associated with the interface risk, particularly on-line transactions, are covered in 6.2.3.6 below.

6.2.2.3 Correspondent Banking Relationships

Correspondent banking relationships create a risk that the other banks' customers may be using that bank to launder funds. It is not necessarily possible to conduct due diligence on that bank's customer base and as such, these relationships require additional care and attention to guard against becoming unwilling participants in this activity.

R23 The following controls need to be implemented for correspondent banking relationships;

a. a firm must not maintain relationships with shell banks that have no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks;
b. a firm must gather sufficient information about a respondent institution to understand fully, the nature of their business;
c. senior management approval must be obtained prior to establishing new correspondent relationships;
d. the firm must assess the respondent institution's anti-money laundering, terrorist financing and proliferation financing controls;
e. the relationship and its transactions must be subject to annual reviews by senior management. The volume and nature of transactions flowing through correspondent accounts with institutions from high risk jurisdictions, or those with material deficiencies should be monitored against expected levels and destinations, and any material variances should be explored;
f. the respective responsibilities for each institution must be properly documented; and

g. the firm must be able to demonstrate that the information described above is held for all existing as well as new correspondent relationships.

! The firm must determine, from publicly available sources, the reputation of that institution and quality of supervision, including whether it has been subject to any money laundering investigation, terrorist financing investigation, proliferation financing investigation or regulatory action.

! Staff dealing with correspondent banking accounts should be trained to recognise high-risk circumstances, and be prepared to challenge correspondents over irregular activity, whether isolated transactions or trends, submitting a suspicion report where appropriate.

6.2.2.3.1 Payable through accounts

A payable-through account is generally an account through which banks extend payment facilities to the customers of other institutions; often foreign banks. Because "payable through accounts" pose an additional risk, the following must also be satisfied:

R24 The firm must verify that the respondent bank has verified the identity of and have performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data to the firm, upon request.

R25 Firms must terminate the accounts of correspondents who fail to provide satisfactory answers to reasonable enquiries including, where appropriate, confirming the identity of customers involved in unusual or suspicious transactions.

6.2.2.4 Powers of Attorney

R26 The authority to deal with assets under a power of attorney constitutes a business relationship and therefore firms must establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates where control of the legal entity's assets is exercisable by that power of attorney.

! Records of all transactions undertaken in accordance with the power of attorney should be kept in accordance with the provisions of these Notes.

! Because enduring general powers of attorney pose additional risks to firms these should not generally be accepted by firms unless there are compelling reasons for their issuance in the first place.

6.2.2.5 Bearer Instruments

Bearer shares and share warrants to bearer can provide a significant level of anonymity, which may be abused by those seeking to use companies for a criminal purpose. Furthermore, fictitious bearer instruments can be used to perpetrate fraud. There are, however, legitimate reasons for the use of bearer shares and their issue is permitted in many jurisdictions. Firms are required to have adequate and properly documented due diligence policies and procedures in place to ensure that their issue is controlled effectively to prevent abuse. Where a company has issued share warrants to bearer these must be kept immobilised under the control of a licensee. This is because the Guidance Notes cannot be complied with and due diligence in accordance with the Guidance Notes cannot be carried out, where beneficial ownership can change without the knowledge of the licensee.

R27 Where a transaction involves bearer instruments, verification evidence must be obtained for the following transactions:

- bearer shares converting to registered form; and
- surrender of coupons for payment of dividend, bonus, or capital event.

! The middle market price quoted in the Financial Times, Bloomberg or Reuters etc. on the day of receipt should normally be used to establish share value.

R28 In the case of transfers from bearer to registered shares, evidence of identity of the registered holder must be obtained in line with the procedures set out in these Notes.

! The submission of coupons in exchange for a cheque in payment of dividends, bonuses or capital events, does not require the identity of the owner to be verified unless the value of the cheque is in excess of €15,000, and the requested payee is not a regulated financial sector firm based in Gibraltar or a jurisdiction with an equivalent AML/CFT/CPF regime. As the identity of the holder of bearer certificates from which the coupons are derived is not known, identification evidence must be obtained in respect of the payee of the requested cheque before the cheque is issued.

6.2.2.6 Wire Transfers

The Wire Transfer Regulations EU (2015/847) (WTR) were published by the Official Journal of the EU on 26 June 2017 and came into force on the date of publication, without the need for transposition into local legislation.

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

For the purposes of this part, the following definitions shall apply:

'payer' means either a natural or legal person who holds an account and allows a transfer of funds from that account, or, where there is no account, a natural or legal person who places an order for a transfer of funds;

'payee' means a natural or legal person who is the intended final recipient of transferred funds;

'payment service provider' means a natural or legal person whose business includes the provision of transfer of funds services;

'intermediary payment service provider' means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds;

'transfer of funds' means any transaction carried out on behalf of a payer through a payment service provider by electronic means, with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person;

'batch file transfer' means several individual transfers of funds which are bundled together for transmission;

'unique identifier' means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the transfer of funds.

R29 The requirements of this section of the Notes apply to transfers of funds, in any currency, which are sent or received by a payment service provider established in Gibraltar other than the following cases of transfers of funds:

1. carried out using a credit or debit card, provided that:
   (a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services; and
   (b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such transfer of funds.
2. using electronic money except where the amount transferred exceeds €1,000;
3. carried out by means of a mobile telephone or any other digital or Information technology device, when such transfers are pre-paid and do not exceed €150; and
4. carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:
   (a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;
   (b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds; and
   (c) the payment service provider is subject to the obligations set out in MLD.
5. within Gibraltar to a payee account permitting payment for the provision of goods or services if:
   (a) the payment service provider of the payee is subject to the obligations set out in MLD;
   (b) the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services; and
   (c) the amount transacted is €1,000 or less.
6. where the payer withdraws cash from his or her own account;
7. where there is a debit transfer authorization between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds, enabling the natural or legal person to be traced back;
8. where truncated cheques are used;
9. to public authorities for taxes, fines or other levies within a Member State; and
10. where both the payer and the payee are payment service providers acting on their own behalf.

R30 Where both the payment service provider of the payer and the payment service provider of the payee are situated in the European Community, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier as long as it allows the transaction to be traced back to the payer.

If so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

R31 For domestic wire transfers, payment service providers should ensure that the information accompanying the wire transfer includes originator information the same as is indicated for cross-border wire transfers, unless this information can be made available to the beneficiary institution and appropriate authorities if required.

R31A Transfers of funds where the payment service provider of the payee is situated outside the European Community shall be accompanied by complete information on the payer.

1. Complete information on the payer shall consist of his name, address and account number.
2. The address may be substituted with the date and place of birth of the payer, his customer identification number or national identity number.
3. Where the payer does not have an account number, the payment service provider of the payer shall substitute it by a unique identifier that allows the transaction to be traced back to the payer.
4. The payment service provider of the payer shall, before transferring the funds, verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source.
5. In the case of transfers of funds from an account, verification may be deemed to have taken place if:
   (a) a payer's identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in these notes; or
   (b) the payer is a relevant financial business.

R32 Without prejudice to the requirement to apply due diligence measures when money laundering,terrorist financing or proliferation financing is known or suspected. In the case of transfers of funds, the payment service provider of the payer shall verify the information on the payer only where the amount exceeds €1,000, unless the transaction is carried out in several operations that appear to be linked and together exceed €1,000.

R32A Intermediary payment service providers must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it. They should also take reasonable measures to identify cross-border wire transfers that do not contain all required originator and/or beneficiary information.

R33 Payment service providers must ensure they maintain all originator and beneficiary information collected in keeping with the record keeping requirements detailed under Section 25 of POCA.

R34 In the case of batch file transfers from a single payer where the payment service providers of the payees are situated outside the Community, the requirements in R31A shall not apply to the individual transfers bundled together therein, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

R34A Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, payment service providers should ensure that the batch file contains required and accurate originator information, and full beneficiary information as listed in Requirement 32A, that is traceable within the beneficiary country. Payment service providers are required to include the originator's account number or unique transaction reference number.

R34B Payment service providers must have risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information, and the appropriate follow-up action in these cases.

R34C Where a payment service provider acts for both the payer and payee of the wire transfer, it should:

a. take into account all the information from both the payer and payee parties in order to determine whether a disclosure report must be filed to GFIU; and

b. if applicable, file a report in any country affected by the suspicious wire transfer, and make relevant transaction information available to the GFIU

R34D Payment service providers should take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, in line with the obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, namely UNSCRs 1267[4] and 1373[5], and their successor resolutions.

6.2.2.6.1 - Obligations on the Payment Service Provider of the Payee

R35 The payment service provider of the payee shall detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system. Such provider shall have effective procedures in place in order to detect whether the following information on the payer is missing:

a) for transfers of funds where the payment service provider of the payer is situated in the Community, the information required under R30;
b) for transfers of funds where the payment service provider of the payer is situated outside the Community, complete information on the payer as referred to in Requirement R31, or where applicable, the information required under R38; and
c) for batch file transfers where the payment service provider of the payer is situated outside the Community, complete information on the payer as referred to in R34 in the batch file transfer only, but not in the individual transfers bundled therein.

6.2.2.6.2 - Transfers of funds with missing or incomplete information on the payer

R36 The payment service provider of the payee should take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

R36A If the payment service provider of the payee becomes aware, when receiving transfers of funds, that information on the payer required under this section of the notes is missing or incomplete, it shall either reject the transfer or ask for complete information on the payer and on a risk based-approach decide whether a report to GFIU should be made**.**

R37 Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider. The payment service provider of the payee shall report that fact to the GFIU.

6.2.2.6.3 - Technical Limitations

R38 Where the payment service provider of the payer is situated outside the Community and the intermediary payment service provider is situated within Gibraltar;

a) Unless the intermediary payment service provider becomes aware, when receiving a transfer of funds, that information on the payer required under these Notes is missing or incomplete,

[4] UNSCR 1267 can be accessed here: http://unscr.com/en/resolutions/doc/1267
[5] UNSCR 1373 can be accessed here: http://unscr.com/en/resolutions/doc/1373

it may use a payment system with technical limitations which prevents information on the payer from accompanying the transfer of funds to send transfers of funds to the payment service provider of the payee.

b) Where the intermediary payment service provider becomes aware, when receiving a transfer of funds, that information on the payer required under these Notes is missing or incomplete, it shall only use a payment system with technical limitations if it is able to inform the payment service provider of the payee thereof, either within a messaging or payment system that provides for communication of this fact or through another procedure, provided that the manner of communication is accepted by, or agreed between, both payment service providers.

c) Where the intermediary payment service provider uses a payment system with technical limitations, the intermediary payment service provider shall, upon request from the payment service provider of the payee, make available to that payment service provider all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request.

In the cases referred to in paragraphs (a) to (c) above, the intermediary payment service provider shall for five years keep records of all information received by all parties.

6.2.2.7 Reduced due diligence measures

An institution may apply reduced due diligence where it 1) identifies an area of low risk,2) it has ascertained that the business relationship or transaction presents a low risk. A non-exhaustive list of factors and types of evidence of potentially lower risk can be found in Schedule 6 of POCA.

Irrespective of the size and nature of the transaction or customer, reduced due diligence measures must not be applied where money laundering, terrorist financing or proliferation financing is known, believed or suspected. Furthermore, where higher risk scenarios or factors apply, a payment service provider should not apply reduced due diligence measures.

6.2.2.7.1 - Occasional Transactions: Single or Linked (S10B(b))

Some products may be innocuous enough not to attract a risk to the firm if conducted as a single transaction. These may be of low value or a low risk product. However, when made in multiples, these transactions could be seen as a conduit through which criminals could layer or integrate proceeds of criminal activity into the system.

! Verification of identity is not normally needed in the case of a single occasional transaction when payment by, or to, the applicant is less than €15,000.

! For the purpose of these Guidance Notes, transactions that are separated by an interval of three months or more need not, in the absence of specific evidence to the contrary, be treated as linked.

R39 Section 11(5) requires that identification procedures should be undertaken for linked transactions that together exceed the exemption limit, i.e. where in respect of two or more one off transactions:

a. it appears at the outset to a person handling any of the transactions that the transactions are linked and that the aggregate amount of these transactions will exceed €15,000; or
b. at any later stage, it comes to the attention of such a person that the transactions are linked, and that the €15,000 limit has been reached.

! In respect of Bureau de Change and Money Transmission services, this level is reduced to €5,000.

R40 Firms must implement systems of control to be able to identify where one or more "occasional" transactions are linked to the same person.

The requirement to aggregate linked transactions is designed to identify people who might structure their dealings to avoid the identification procedures. It is not meant to cause inconvenience for genuine business transactions. There is clearly no need to count both ends of the same transaction, e.g. a purchase and a subsequent sale.

R41 Where a series of occasional transactions are linked and this gives rise to a suspicion or knowledge of money laundering, terrorist financing or proliferation financing, this must be reported.

6.2.2.8 Enhanced due diligence measures

Firms must apply enhanced due diligence measures:

1. for relationships established with correspondent banking;
2. for PEPs, family members of PEPs and close associates of PEPs, whether they be as a customer or a beneficial owner;
3. when dealing with a customer established in a high risk country; and
4. where the firm has risk scored the customer as high risk;
5. where a risk has been identified as high by the Minister by way of notice in the Gazette; or
6. where a risk has been identified as high within any information that is made available to relevant financial business pursuant to the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016.

Where a branch or majority owned subsidiary of an entity is located in a high-risk third country, enhance due diligence does not need to be applied; subject to the group complying with equivalent AML/CFT/CPF standards to Gibraltar.

A non-exhaustive list of factors and types of evidence of potentially higher risk can be found in Schedule 7 of POCA. In addition to these factors, financial institutions are required to include the beneficiary of any life assurance policy as a relevant risk factor in determining whether to apply enhanced due diligence measures.

6.2.2.8.1 – Enhanced due diligence for third country correspondent relationships

With respect to cross-border correspondent relationships involving the execution of payments and other similar relationships, in addition to enhanced due diligence, firms must:

1. gather sufficient information to understand the nature of the respondent's business, to determine the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF/PF investigation or regulatory action;
2. obtain senior management approval prior to establishing the relationship;
3. clearly understand and document the respective responsibilities of each institution;
4. be satisfied that the respondent does not permit its accounts to be used by shell banks; and
5. with respect to payable-through accounts, verify the identity of, and perform ongoing due diligence on, the customers having direct access to accounts of the correspondent institutions, and that it is able to provide relevant due diligence data to the correspondent institution upon request.

Additionally, if a firm is a credit institution or a financial institution, which is in a correspondent relationship with a third country respondent institution in a high-risk country, it may be required to review, amend or terminate the correspondent relationship with that respondent institution.

6.2.2.8.2 – Enhanced due diligence for high-risk third countries

In relation to business relationships or transactions involving high-risk third countries identified, a firm must apply the following enhanced customer due diligence measures:

a) obtain additional information on the customer and on the beneficial owners;
b) obtain additional information on the intended nature of the business relationship;
c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owners;
d) obtain information on the reasons for the intended or performed transactions;
e) obtain the approval of senior management for establishing or continuing the business relationship; and
f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

The GFSC may require Increased external audit requirements from firms which have branches or subsidiaries that are located in a high-risk country.

6.2.3 Interface Risk

Firms face interface risk because of the mechanism through which the business relationship is commenced and transacted.

Where it is physically possible to verify a customer's likeness to documents evidencing identity this will also help to satisfy or mitigate the customer risk as well as the interface risk. Receiving instructions through face-to-face contact will also enable a firm to address any concerns the front-line staff may have about any proposed transaction, which can reduce the number of suspicions. Transactions conducted online, for example, removes the human element and firms must therefore build a degree of artificial intelligence and monitoring over such activity that would produce the same or better results.

R42 Firms must document how they mitigate or reduce the risks posed by each of the delivery mechanisms through which their product(s) is delivered.

6.2.3.1 Face-to-face

It is recognised that where a customer makes face-to-face contact with a firm, this may be perceived to lower the risk to the firm. Not only does this present an opportunity for the firm's staff to verify that the likeness of the person in front of them physically matches that of the documents being presented to support this but is also an opportunity for staff to identify any inconsistencies, etc.

Where the customer also has to give instructions in person, e.g. by having to present a passbook or produce identity before a transaction takes place the potential risk to the firm is considerably reduced.

6.2.3.2 Non Face-to-face

Any mechanism through which the customer is allowed to interact with a firm in a non-direct manner increases the firm's exposure to risk. Not only does this allow third parties to have access to assets or property through impersonation but also disguise the true owner of that property by, for example, provision of false identification documentation.

! Firms must put into place systems of control that appropriately address the risks posed by non-face to face contact for customers either at the opening of the business relationship or through the operation of that relationship.

R43 Additional controls are required in respect of non face-to-face customers; for example, applying one or more of the following measures of control:

a. ensuring that the customer's identity is established by additional documents, data or information;
b. supplementary measures to verify the documents supplied, or requiring an eligible introducer to certify the customer identification documents be required;
c. ensuring that the first payment of the operation is carried out through an account in the customer's name at a credit institution;
d. landline telephone contact with the customer on a number which has been verified; or
e. sending information or documents required to operate the business relationship to a physical address that has been verified.

A common mechanism adopted by many firms is to permit the use of certified customer identification documents provided in lieu of having had sight of the originals.

R44 In drawing up the list of persons approved to certify identification documents for a firm, the Money Laundering Reporting Officer (MLRO) will need to provide documentary evidence of the following:

a. That the person:
   i. adheres to ethical and/or professional standards;
   ii. is readily contactable;
   iii. exercises his or her profession or vocation in a jurisdiction with effective anti-money laundering measures; and
b. The MLRO has obtained senior management agreement to permit such a person from certifying documents for these purposes.

! There is obviously a wide range of documents that might be provided as evidence of identity. It is for each firm to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents that are easily forged or which can be easily obtained using false identities.

! In the instance that certified documents are produced, they should be accompanied by suitable wording that confirms that the individual certifying the documentation has had sight of the original document(s). For photographic identity document(s), the wording should also confirm that it is a true likeness of the individual.

6.2.3.3 Introducers

R45 The ultimate responsibility for meeting the customer identification requirements for introduced business lies with the senior management of the firm.

Every institution must retain adequate documentation to demonstrate that its KYC procedures have been properly implemented, and that it has carried out the necessary verification itself.

There are, however, certain circumstances in which it may be possible for institutions to rely on KYC procedures carried out by third parties. Whereas the procedures listed below refer to the obtaining and verification of original documentation.

Institutions may not rely on a third party that is established in a high risk third country, with the exemption of branches and majority-owned subsidiaries of entities where the group fully complies with equivalent AML/CFT/CPF standards.

R46 None of the provisions for dealing with introducers, exempt institutions from the requirement to have copies of all documentation in their possession, or to have ready access to the original documentation.

Introductions from Intermediaries

R47 Where a business relationship is being instituted the institution is obliged to carry out KYC procedures on any client introduced to it by a third party, unless the third party is an eligible introducer able to provide the institution with copies of all documentation required by the institution's KYC procedures.

R48 To be an eligible introducer, a third party must meet ALL FOUR of the following conditions:

a. it must be regulated by the GFSC, or an equivalent institution if it carries on business outside Gibraltar;
b. it must be subject to equivalent legislation;
c. it must be based in Gibraltar or a country which has an effective AML,CFT and CPF regime; and
d. there must be no secrecy or other obstacles which would prevent the Gibraltar firm from obtaining the original documentation if necessary.

! A firm must be able to demonstrate, for each person that they have defined as an "eligible introducer", how the above four conditions are met**.**

In Gibraltar, "eligible introducers" would be all persons caught by these Guidance Notes who are subject to the GFSC's regulatory regime. Essentially all persons listed in 2.1 with the exception of Bureau and Money Transmission agents as KYC requirements are only required in these cases for occasional transactions of €15,000 or above. Firms should be aware, however that similar activities conducted outside of Gibraltar may not meet all the requirements stated above particularly as some activities are regulated by professional bodies and not by a public or quasi-public regulatory body.

Where an introducer satisfies the definition of eligible introducer, a firm may place reliance upon the KYC procedures of the eligible introducer, and simply obtain copies of the relevant documentation rather than be required to see the original documentation. Exemptions for postal applications do not apply in these circumstances.

Where reliance is to be placed on an eligible introducer, the introducer must complete and return the Eligible Introducer Certificate (F1) (this can be found in the Guidance Notes section of the GFSC's Financial Crime Approach web page). Copies of all the necessary documentation must also be immediately supplied. The documentation must be the same as the firm would require to satisfy its own KYC procedures. A business relationship may not commence until the completed Introducer's Certificate has been received, together with copies of the required documentation.

Group Introducers

Institutions that form part of a group may accept other group entities as eligible introducers subject to the following:

a. the information is provided by a person that is part of the group;

b. group applies customer due diligence measures, record keeping, and programs against money laundering, terrorist financing and proliferation financing in accordance with this Act or equivalent; and
c. the implementation of the requirements noted in (b) is supervised by a supervisory authority in Gibraltar or in a third country.

Introduction of Occasional Transactions from Overseas

Where an applicant for business who is affecting an occasional transaction is introduced by an overseas branch or subsidiary in the same group as the firm, or by a regulated institution from a country with an equivalent AML/CFT/CPF regime, Section 14(1)(a-c) provides that the institution need not verify identity even if the transaction exceeds €15,000, as long as the introducer has provided the name of the customer and given the firm a written assurance that evidence of identity has been taken and recorded. This assurance can be given separately by the introducer for each new customer, or by way of a written general assurance. However, the Section 14(1)(c) exemption is only applicable provided condition (ii) of 14(i)(c) is fulfilled, namely that there are reasonable grounds for believing that the non-Gibraltar introducer:

- acts in the course of a business in relation to which an overseas regulatory authority exercises regulatory functions;
- the introducer will supply, upon request, the underlying identification documents without delay upon request;
- is based, or incorporated in, or formed under the law of, a country other than countries with equivalent AML/CFT/CPF regimes, particularly in respect of verification of identity and record keeping; or
- operates under a rigorous group policy in accordance with Gibraltar standards and provides some form of group introduction certificate that evidence of identity has been taken and recorded.

! A firm must be able to demonstrate that these four conditions have been met.

This exemption applies only to occasional transactions. If the person being introduced is forming a business relationship with the firm, then the firm must obtain the evidence of identity.

6.2.4.1 Intermediary's Client Accounts

An intermediary is different from an introducer.

An intermediary plays an active role in the financial affairs of the underlying customer, for example, a stockbroker, whereas the function of an introducer is merely to introduce business to a firm. The distinction is very important when considering the requirements under these Notes.

Stockbrokers, fund managers, solicitors, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with institutions. Such accounts may be pooled or omnibus accounts holding the funds of many clients, or they may be opened specifically for a single client or for a number of clients.

In all cases, regardless of the jurisdiction where the intermediary is based, firms must ensure that they establish the identity of the person(s) for whom the intermediary is acting.

_'

6.2.4.1.1 – Client accounts operated by regulated firms

! Client accounts operated by regulated firms are those operated by regulated firms on behalf of a customer, a client company or pooled clients. For these, firms must ensure that due diligence information is sought and maintained on all persons who are signatories to client accounts.

A bank account opened in the name of the client company but whose signatories are the firm's own corporate director companies is not subject to any form of exemption from the due diligence requirements.

In the case of pooled client accounts, these are subject to various provisions regarding their operation by the regulated firm itself. There is no requirement to conduct due diligence on every client for which transactions are put through the pooled client account. Where unusual activity occurs, this would require additional monitoring and investigation be conducted of the transactions that led to the unusual event taking place. Should the investigations and enquiries made, not prove satisfactory then a report as required under Chapter VIII should be made.

6.2.4.2 The "Postal" Concession

Where a customer would normally be required to produce evidence of identity before transacting business (whether directly or introduced by an intermediary).

! Where it is reasonable in all the circumstances for payment to be made by post, or electronically, or for the details of the payment to be given by telephone, then if payment is to be made from an account held in the customer's name (or jointly with one or more other persons) at an authorised financial or credit institution, identification requirements may be waived.

The postal concession can be used without additional identity verification for mail-shot, off the page, coupon business, or business placed over the telephone. However, in such cases a record should be maintained indicating how the transaction arose and detailing the credit institution's details and the number of the account from which the cheque or payment is drawn.

Whilst a payment can be made directly between accounts with credit institutions or by cheque or debit card, the accepting institution must be able to confirm that the account is held in the sole or joint name(s) of the investor. (Payments to or from a joint account, where only one party is involved in the transactions, are not regarded as third party payments.)

If a firm relying on the concession has grounds to believe that the identity of the customer has not previously been verified by the credit institution that the payment has been drawn, then taking a risk-based approach, additional measures to verify identity must be sought.

R50 The concession for postal/coupon business does not apply where:

a. initial or future payments can be received from third parties;
b. cash withdrawals can be made, other than by the investors themselves on a face-to face basis where identity can be confirmed, e.g. passbook accounts where evidence of identity is required for making withdrawals; and
c. redemption or withdrawal proceeds can be paid to a third party or to a bank account that cannot be confirmed as belonging to the investor, other than to a personal representative named in the Grant of Probate or Letters of Administration on the death of the investor.

R51 The following repayment restrictions must exist for the postal concession to apply:

a. repayments made to another institution must be subject to confirmation from the receiving firm that the money is either to be repaid to the investor or reinvested elsewhere in the investor's name;
b. repayments made by cheque must be sent either to the named investor's last known address and crossed "account payee only", or to the investor's bank with an instruction to credit the named investor's account; and
c. repayments via BACS should ensure that the stipulated account is in the name of the investor;

It should not be possible to change the characteristics of products or accounts at a future date to enable payments to be received from, or made on behalf of, third parties.

6.2.4.3 Online and internet access

On-line payment systems, internet access to operate accounts and web-based marketing and promotion have significantly increased the risks of money laundering to any firm offering such services.

The risks increase from the lowest for an "image advertisement web-page" through to the highest where the firm allows customers to make payments to third parties etc.

Some firms may permit the establishment of the business relationship to be conducted entirely using the internet.

R52 Where a firm relies on electronic verification of customer identification documentation, its records must clearly demonstrate the basis on which these were effected and these must be in accordance with the risk-based approach and other requirements of these Notes.

R53 Where a firm permits payment processing to take place via online services these must be subjected to the same monitoring requirements as the rest of the activities of the institution and subject these to the same risk based methodology.

6.2.5 Country Risk

Country risk is used to describe the risk posed to the firm by the geographic providence of the economic activity of the business relationship. This is wider than just the country of residence of the customer and will, for example, include where the client company is trading.

R54 Firms must assess and document the risks posed by different countries and territories, or classes of countries and territories, and what additional systems of control it will implement to mitigate these risks.

Appendix 3 – Countries and territories that may have equivalent legal frameworks or those requiring enhanced due diligence contains various lists which can assist a firm in taking a view as to the equivalence of a jurisdiction or when enhanced due diligence needs to be conducted on business emanating from certain jurisdictions.

6.2.5.1 The "Effectiveness" test

The Notes make a number of references to countries or territories that operate an effective AML/CFT/CPF regime. Business emanating from these jurisdictions carry a lower risk as it is inferred that these have already been subjected to stringent measures and systems of controls that will have addressed the money laundering, terrorist financing or proliferation financing risks.

Conversely, doing business with a country that does not have an effective AML/CFT/CPF regime increases the risk to the firm that the customer's business may be involved in illicit activities.

Firms, however, need to take their own view on how the effectiveness test will be conducted.

R55 In making a determination of an effective AML/CFT/CPF regime the following three factors have to be taken into consideration:

- Legal Framework
- Enforcement and Supervision
- International Co-operation

6.2.4.1.1 - Legal Framework

Given that each country will transpose AML/CFT/CPF requirements in accordance with their own judicial and legal systems, there is no one legislative model against which it would be possible to verify that effective legislative provisions to those of Gibraltar have been included in that country's statute books.

6.2.4.1.2 - Enforcement and Supervision

The effectiveness of the judicial, law enforcement and administrative functions is a crucial element of as without the proper enforcement of the legal provisions the legislation is ineffective.

In order to assist firms in taking a view of the effectiveness of a jurisdiction's enforcement and supervisory powers both the FATF and IMF publish regular reports on the evaluation of a jurisdiction's compliance with the FATF recommendations.

These reports are available on-line and should be subject to review by a firm in order to assess the risk posed to the firm. These reports can be downloaded from the following addresses;

FATF Reports: http://www.fatf-gafi.org

IMF Reports: http://www.imf.org/external/country/index.htm

6.2.4.1.3 - International Co-operation

An essential requirement in combating money laundering, terrorist financing and proliferation financing is that law enforcement agencies are able to co-operate fully and extensively. Launderers and terrorist financers will therefore seek jurisdictions where this lack of cooperation assists their aims.

R56 Firms must guard against customers or introductions from countries where the ability to co-operate internationally is impaired either via failings in the judicial or administrative arrangements and subject these business relationships to enhanced due diligence requirements.

R57 FATF maintain a list of Non-Cooperative Countries and Jurisdictions (see Appendix 3 – Countries and territories with equivalent legal frameworks or those requiring enhanced due diligence). Firms must take additional measures with transactions of business relationships whose source of funds derives from NCCT or sanctioned countries and territories.

! However, firms must ensure that they understand the basis under which a country has been removed from the list as it may be the case that the removal is based on an undertaking to correct deficiencies as opposed to actual correction of the deficiency.

6.2.4.2 Countries with a high propensity for corruption

R58 Firms whose policy includes the acceptance of Politically Exposed Persons (PEPs) as customers need to take additional measures to mitigate the additional risk that the firm is exposed to from such persons originating in countries with a high propensity for bribery and corruption. This includes

a. conducting and documenting an assessment of the countries which are more vulnerable to corruption; and
b. the application of additional monitoring over customers from high risk countries whose line of business is more vulnerable to corruption (e.g. oil or arms sales).

Transparency International publishes a Corruption Perception Index that is available at www.transparency.org. This publication may be a useful reference to firms in assessing the risk of corruption posed by different countries.

6.2.4.3 Sanctioned Countries

In addition to the above, a number of countries and territories, as well as undertakings and individuals connected to them, are subject to sanctions and other measures that requires institutions to take action to prohibit:

- the export of goods to those countries or territories;
- the transfer of technology;
- the facilitation of technical assistance; and
- the facilitation of funds.

In certain circumstances, institutions are required to freeze funds from designated undertakings and/or individuals.

As the legislation prohibits the above unless a licence has been granted, institutions may find themselves participants in arrangements that breach these provisions, through the activities of their customers, and as such must take the necessary measures to ensure that these sanctions are not being breached.

These restrictions are imposed under the Export Control Act 2005 and various Orders made there under.

At present the Orders that are in force are; Export Control (Sanctions Etc.) Order 2005 and Export Control (Sanctions Etc.) Order 2006.

For country specific data please refer to Appendix 3 – Countries and territories with equivalent legal frameworks or those requiring enhanced due diligence. Further legislative provisions exist which impose restrictions on carrying out transactions with Countries/Territories and designated undertakings and/or individuals. The GFSC website includes a web page on which country specific sanctions applicable to Gibraltar are maintained, with links to the pertinent legislation hosted on the Gibraltar Laws website. Please refer to https://www.fsc.gi/financialcrime/sanctionsandterrorism Institutions should ensure that the provisions of these statutory instruments are not being breached through the activities of their customers.

CHAPTER VII

SP3 **All firms must know their customer to such an extent as is appropriate for the risk profile of that customer.**

7 Knowing your customer

Having sufficient information about your customer - "knowing your customer" - and making use of that information underpins all anti-money laundering, combating the financing of terrorism, and combating proliferation financing efforts, and is the most effective defence against being used to launder the proceeds of crime. If a customer has established an account using a false identity, they may be doing so to defraud the institution itself, or to ensure that they cannot be traced or linked to the crime the proceeds of which the firm is being used to launder. A false name, address, or date of birth will usually mean that law enforcement agencies cannot trace the customer if they are needed for interview as part of an investigation.

Section 11 of the Proceeds of Crime Act requires all firms to seek satisfactory evidence of the identity of those with whom they deal (referred to in these Guidance Notes as "customer identification documentation"). Unless satisfactory evidence of the identity of potential customers is obtained in good time, the business relationship must not proceed.

When a business relationship is being established, the nature of the business that the customer expects to conduct with the firm must be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to be able to judge whether a transaction is or is not suspicious, firms need to have a clear understanding of the business carried on by their customers. This must entail such ongoing monitoring of the business relationship, as is appropriate to the nature and scale of the business and the risks posed by the customer. This ongoing monitoring must include scrutiny of the transactions being conducted to ensure that these are consistent with the knowledge of that customer, the business and the risk profile and the source of funds. It must also include reviews of existing records (and updating these where necessary) to ensure that the documents, data or information obtained for the purpose of applying CDD measures is kept up-to-date and relevant.

A firm must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorised to operate the business relationship. Whenever possible, the prospective customer should be interviewed personally.

The verification procedures needed to establish the identity of a prospective customer should, be the same, regardless of the type of account or service is required. The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process.

! The overriding principle is that every institution must know who their customers are, and have the necessary customer identification documentation, or data to evidence this. Where a firm is unable to complete its CDD measures because it has formed a suspicion or knowledge of ML,TF or PF and completing the process is likely to tip-off the customer, it is expected to make a disclosure to the GFIU in line with Section 6B of POCA. This decision must be appropriately recorded by the firm in line with the record keeping requirements under Section 25 of POCA

7.1 Overriding requirements for customer due diligence measures

The application of customer diligence measures can be complex, in order to come to a set of documents that are collectively known as the "customer identification documents". The customer identification documents form the basis of the firm's knowledge of the underlying customer and is what will drive the risk-profiling and therefore the intensity of the measures that are to be applied.

The requirements for customer due diligence can be summarised in the diagram below and the following sections describe in more detail what is required for each.

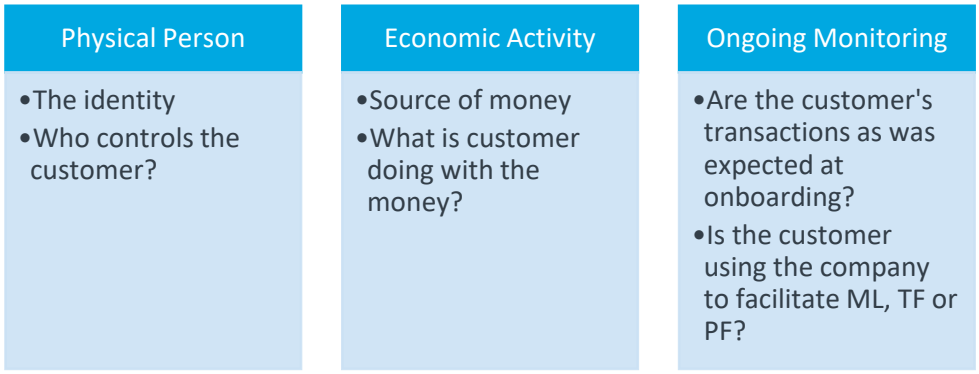


Figure – Customer due diligence measures and customer identification documentation summarised.

7.1.1 Applying customer due diligence measures

R59 Firms must apply customer due diligence measures:

a. When establishing a business relationship;
b. When carrying out an occasional transaction amounting to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
c. Whether the customer is a natural or legal person or legal arrangement;
d. When a transfer of funds is carried out by electronic means through a payment service provider exceeding €1,000;
e. Where there is a suspicion of money laundering, terrorist financing or proliferation financing, regardless of any derogation, exemption or threshold; and
f. When there are doubts over the veracity or adequacy of previously obtained customer identification data.

A relevant financial business must also apply customer due diligence measures at other appropriate times to existing customers on the basis of materiality and on a risk-sensitive basis, including at times when the relevant circumstances of the customer change or a legal duty arises under POCA or any regulations made under POCA, to contract the customer for the purpose of reviewing any information relating to the beneficial owner.

When determining to what extent to apply customer due diligence measures a relevant financial business must, at least, take into account the following list of risk variables:

a. the purpose of an account or relationship;
b. the level of assets to be deposited by a customer or the size of transactions undertaken;
c. the regularity or duration of the business relationship, and

d. (d) whether the customer or beneficial owner is a politically exposed person.

The issue of materiality is important as it requires firms to take into consideration not just the risk profile of a customer but also the impact that the customer may have on the firm. For example, a customer may be risk-profiled as low risk but yet the RFB handles a substantial portion of its assets for that customer or the customer represents a substantial part of the firm's turnover and therefore would be material for the RFBs consideration, triggering the need for a risk assessment.

Where a relevant financial business is required to apply customer due diligence measures to a trust, corporate or legal entity which is subject to the registration of beneficial ownership information pursuant the Money Laundering Directive, the relevant financial business shall collect proof of registration *or* an excerpt from the relevant register where access to such register is available in the respective jurisdiction. Additionally, collecting proof of registration from the customer directly would also suffice.

7.1.2 What constitutes customer due diligence measures

R60 Customer due diligence measures shall comprise of the following, but the extent to which each of this is applied shall be determined on the basis of materiality and on a risk-sensitive basis:

a. identifying the customer;;
b. identifying the beneficial owner;
c. understanding the ownership and control structure of the customer; understanding the ownership and control structure of the customer;
d. understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship or occasional transaction;
e. taking a risk-based approach to the verification of the identity of the customer and all beneficial owners, on the basis of documents, data or information obtained from a reliable and independent source including, where available, electronic identification means or relevant trust services as set out in the Electronic Identification Regulation or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the EIR supervisory body, so that the relevant financial business is satisfied that it knows who the customer and beneficial owners are;
f. taking a risk-based approach to the verification of the source of funds and wealth of the customer and beneficial owners;
g. determining whether the customer, or its beneficial owner, is a politically exposed person;
h. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the firm's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and reviewing existing records (and updating these where necessary) to ensuree that the documents, data or information held are up to date and relevant; and
i. keeping records of all the actions taken under this section, as well as any difficulties encountered during the process.

R60A For customers that are legal persons or legal arrangements, the firm should verify the customer's identity through:

a. the name, legal form and proof of existence;
b. the powers which regulate and bind that legal person or legal arrangement;

c. the names of the relevant persons having a senior management position in the company; and
d. the address of the registered office and if different, a principal place of business.

The above list is not exhaustive and firms are required to conduct appropriate due diligence on each customer as required and on a case-by-case basis.

7.1.2.1 Beneficial owner

R61 The term "beneficial owner" is to be interpreted throughout these Notes as meaning the following;

"(a) in the case of a natural person-

(i) where a person is conducting a transaction or activity on his own behalf, that natural person; or
(ii) where a transaction or activity is being conducted on behalf of another person, the person on whose behalf the transaction or activity is being conducted.

(b) in the case of a Listed Entity, or a majority-owned subsidiary of such a Listed Entity, the Listed Entity.

(c) in the case of a corporate or legal entity, other than a Listed Entity, or a majority owned subsidiary of a Listed Entity:

(i) the natural person who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings;
(ii) if, after having exhausted all possible means,
(a) there is doubt as to whether the person identified under subparagraph (i) is the beneficial owner;
(b) no person under subparagraph (i) is identified, the natural person exercising control via other means;
(iii) if, after having exhausted all possible means,
(a) there is doubt as to whether the person identified under subparagraph (ii) is the beneficial owner; or
(b) no person under subparagraph (ii) is identified, the person is specified under subparagraph (iv);
(iv) for the purposes of subparagraph (iii) the specific person is,
(a) if the company or legal entity is ultimately owned or controlled through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, by a Listed Entity or a majority owned subsidiary of a Listed Entity, the Listed Entity; and
(b) in all other cases, the natural person who holds the position of senior managing official;

Please note that subparagraph (c) above includes protected cell companies.

(d) in the case of trusts -
(i) the settlor or settlors;
(ii) the trustee or trustees;
(iii) the protector or protectors, if any;
(iv) the beneficiaries, or where the individuals benefiting from the trust have yet to be determined, the class of persons in whose main interest the trust is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

(e) in the case of legal entities, such as foundations, and legal arrangement similar to trusts, the natural person holding equivalent or similar positions to those referred in subparagraph (d):

i. the Founder;
ii. the foundation councilors;
iii. the Guardian, if any;
iv. the beneficiaries; and
v. any other natural person exercising control over the foundation.

Where any of the positions noted in subparagraphs (a) to (d), such as director, senior managing official, settlor, trustee, protector, beneficiary, foundation councilor, etc; is held by a corporate entity, the measures as set out in R61, point (a), apply.

7.2 When customer due diligence measures need to be applied

R62 Generally, a firm should never establish a business relationship until all the relevant parties to the relationship have been identified and the nature of the business they expect to conduct has been established.

Once an ongoing relationship has been established, any regular business undertaken for that customer should be assessed at regular intervals against the expected pattern of activity of the customer. Any unexpected activity can then be examined to determine whether there is a suspicion of money laundering. (See 7.8 below on monitoring requirements)

! A firm may complete the verification of the identity of the customer and beneficial owner during the establishment of the business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering, terrorist financing or proliferation financing occurring. In these situations, these procedures shall be completed as soon as practicable, after the initial contact and in all cases, before completion of the transaction.

Section 13 states that what constitutes an acceptable time span must be determined in the light of all the circumstances including the nature of the business, the geographical location of the parties, and whether it is practicable to obtain evidence before commitments are entered into, or money passes.

! In cases where CDD may not be able to be completed by an insolvency practitioner prior to initiating the business relationship, such as where an appointment is made at a Decision Procedure or by Court Order, reliance may be placed, in part, on the order of the appointment by the Court. Nonetheless, the insolvency practitioner must complete the appropriate CDD as soon as possible. The CDD process would be expected to be commenced within five working days of the appointment.

A reminder that any reliance on the court order does not absolve the insolvency practitioner from their requirements under POCA. They are still required to consider whether potential illicit activity has taken place including carrying out appropriate CDD and a client risk assessment. Additionally, the insolvency practitioner must prioritise these steps prior to continuing with the business relationship.

R63 Section 15 stipulates that if satisfactory evidence of identity has not been obtained it must not carry out a transaction or establish a business relationship.

! A firm can start processing business immediately, if at the same time it is taking steps to verify the customer's identity. Clearly, every effort should be made to complete verification before settlement takes place unless this is impracticable for good reasons. Of course, the verification must be completed even if settlement has occurred.

! A credit institution or financial institution involved in life insurance or other investment-related insurance activities must, in addition to the customer due diligence and ongoing monitoring requirements, conduct the following customer due diligence measures as soon as the beneficiaries are identified or designated:

- where the beneficiaries have been identified as named persons or legal arrangements, taking details of the person; and
- where the beneficiaries are designated by characteristics, by class, or by other means, it is required to obtain sufficient information about the beneficiaries to satisfy itself that it will be able to establish the beneficiary when payout is required.

R64 Firms may permit opening of bank accounts if there are adequate safeguards to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer identification measures has been achieved.

R65 Where a person is unable to comply with customer due diligence requirements of a firm, the firm may not carry out a transaction through a bank account, or establish a business relationship, in certain circumstances, a firm may have to freeze (see 7.2.1 below) or cancel a transaction after it has dealt but before settlement. The firms must also consider making a suspicious transaction report to GFIU in accordance with Chapter VIII.

7.2.1 Freezing

Where satisfactory evidence of identity is required, a firm should "freeze" the rights attaching to the transaction pending receipt of the necessary evidence.

The customer may continue to deal as usual, but, in the absence of the evidence of identity, proceeds should be retained. Documents of title should not be issued, nor income remitted (though it may be re-invested).

Where an investor exercises cancellation rights, or cooling off rights, the sum invested must be re-paid (subject to any shortfall deduction where applicable). The repayment of money arising in these circumstances does not constitute "proceeding further with the business". However, this could offer a readily available route for laundering money.

R66 Firms should be alert to any abnormal exercise of cancellation/cooling off rights by any customer, or in respect of business introduced through any single intermediary. In the event that abnormal exercise of these rights becomes apparent, this should be regarded as suspicious, and reported via the usual channels (see Chapter VIII below).

7.2.2 Acquisition of One Financial Sector Business by Another

When a company acquires the business of another financial services company or firm, either in whole, or as a product portfolio (e.g. the mortgage book), it is not necessary for the identity of all existing customers to be verified again, provided that all customer account records are acquired with the business, and that the due diligence enquiries prior to acquisition do not give rise to doubt

that anti-money laundering, combating the financing of terrorism and combating proliferation financing procedures followed by the business accorded with Gibraltar requirements.

R67 In the event that the AML,CFT and CPF procedures previously undertaken by the acquired firm have not been in accordance with Gibraltar requirements, or the procedures cannot be checked, or the customer records are not available to the acquiring firm, verification of identity and KYC procedures will need to be undertaken for all transferred customers as soon as practicable.

7.2.3 Applying the customer due diligence measures retrospectively

R68 Customer due diligence measures in these Notes must be applied, not only to new customers but also, at appropriate times to existing customers on the basis of materiality and a risk-sensitive basis.

Firms will need to consider what an "appropriate time" is. Many firms may consider certain "trigger events" to be the main driver for revising the customer identification documentation held on the customer. Firms may decide to implement the revised measures in a staggered approach. For example, a customer's change of address might only trigger the verification of the address to be invoked, yet a customer wanting a new product or service should merit a complete risk profiling.

! Nothing in these Notes requires that firms conduct an identification or remediation programme of the existing customer base.

However, if money laundering, terrorist financing or proliferation financing is known or suspected or the firm doubts the veracity of previously conducted customer due diligence measures, then the requirements of these Notes need to be applied.

7.2.4 Potential Tipping Off

R68A If during the course of applying customer due diligence measures, the firm considers that continuing its due diligence checks could result in tipping off the person, because of any suspicions or knowledge of MLMLML/TF/PF, the firm shall cease to apply customer due diligence and make a relevant disclosure to the GFIU without delay in line with Section 6B of POCA. This decision must be appropriately recorded by the firm in line with the record keeping requirements under Section 25 of POCA.

7.3 To whom customer due diligence measures need to be applied

The meaning of "Applicant for Business", "Business Relationship" and "Occasional Transaction" are essential to an understanding of this guidance, and these terms are defined below.

It is important to determine whether the applicant for business is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship as this can affect the verification requirements. The same transaction may be viewed differently by a firm and by an introducer depending on their respective relationships with the applicant for business. Therefore, where a transaction involves an intermediary, both the firm and the intermediary must separately consider their positions, and ensure that their respective obligations regarding verification of identity and associated record keeping are met.

For example, from a life company's viewpoint, most dealings with an applicant will fall within the definition of a business relationship, as even with single premium contracts there will generally be an intention to establish an on-going relationship with the customer. For a unit trust manager, an applicant may be making an occasional purchase, or entering into a business relationship in the

form of a regular savings plan. If an intermediary is involved, it may be dealing with an applicant to a life company or a fund operator within the context of a business relationship, or as an occasional customer undertaking an occasional transaction. Most transactions undertaken by exchange bureau will be occasional transactions.

7.4 Minimum Due Diligence Requirements versus Additional Information

A firm may conclude, under its risk-based approach, that the minimum due diligence requirements are insufficient in relation to the money laundering, terrorist financing or proliferation financing risk, and that it should obtain additional information about a particular customer. Nothing in these Notes prevents a firm from taking a stronger view of the minimum requirements so long as it can justify that the approach is within a risk-based approach.

! As a part of a risk-based approach, firms may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:

- to inform its risk assessment process, and thus manage its money laundering/terrorist financing/proliferation financing risks effectively; and
- to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

The extent of additional information sought, and of any monitoring carried out in respect of business relationship will depend on the money laundering, terrorist financing or proliferation financing risk that the risk profile of the business relationship presents to the firm.

In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

R69 A firm should hold a fuller set of customer identification documentation in respect of those business relationships assessed as carrying a higher money laundering, terrorist financing or proliferation financing risk.

At all times, firms should bear in mind their obligations under the Data Protection Act only to seek information that is needed for the declared purpose, not to retain personal information longer than is necessary, and to ensure that information that is held is kept up to date.

At the time this guidance comes into effect, firms are not expected to obtain additional information in respect of existing customers, or classes/categories of customer. However, firms should have regard to 7.2.4 above, which give guidance on what they should do in respect of existing customers.

7.5 "Applicant for Business"

The person whose identity must be verified is described throughout the Sections as an "applicant for business". Who this is will vary:

- a customer dealing on his own behalf is clearly the applicant for business;
- when a customer is acting as agent for a principal (for example, as authorised manager of a discretionary investment service for clients) and deals in his own name on behalf of an underlying client, then it is the customer acting as the agent, and not his client, who is the

institution's applicant for business. The underlying client may well be, in turn, an applicant for business so far as the agent is concerned;

- when a person wants an investment to be registered in the name of another (e.g. a grandchild), it is the person who provides the funds who should be regarded as the applicant for business, rather than the registered owner;
- when an intermediary introduces a client to an institution, but in the client's name rather than that of the intermediary is given as the investor, it is the underlying client who is the institution's applicant for business;
- when a customer seeks advice, or access to an execution-only dealing service, in his own name and on his own behalf, he is clearly the applicant for business;
- when a professional agent introduces a third party to an institution so that the third party may be given advice, and/or make an investment in his own name, then it is the third party (not the introducer) who is the institution's applicant for business;
- when an individual claiming to represent a company, partnership or another legal entity applies for business, then the applicant for business will be the entity, the identity or existence of which should be verified, rather than that of any individual claiming to represent it;
- when a company manager or company formation agent introduces a client company, it is the client company which is the applicant for business; and
- when a trust is introduced, it is the settlor that is the applicant for business.

These distinctions are important since they are relevant in determining the correct procedures for verification of identity where this is required.

7.6 "Business Relationship" And "Occasional Transactions"

R70 It is necessary to determine, from the outset, whether the applicant for business is seeking to establish a "business relationship" with the institution, or is an occasional customer undertaking an "occasional transaction".

Section 8 defines a "business relationship" as a business, professional or commercial relationship which is connected with the professional activities of a relevant financial business and which is expected at the time when contact is established, to have an element of duration.

An "occasional transaction" means any transaction carried out other than in the course of an established business relationship. The Sections cover sales transactions as well as purchases. Where business is undertaken whether on an occasional basis, or when a series of small deals is placed whether with the same or different product provider, identification procedures will be required on the part of the firm if these, as single or linked transactions, amount to €15,000 or more.

7.7 What comprises the customer identification documentation?

The demonstration of a person's identity is particularly complex in the context of supporting the due diligence measures of a firm.

Customer identification documentation consists of two distinct elements:

- The physical person
- The nature of the economic activity

Both of the above are inextricably linked to the country from which they originate, as this will have a direct bearing on the assessment of the country risk and the customer's risk profile.

7.7.1 The physical person

R71 Irrespective of the nature and risk profile of the customer, other than where specific exemptions are provided for, a firm is required to document and maintain a record of all the customer identification documentation which includes recording how and when each of the due diligence requirements steps were satisfactorily completed by the firm.

The customer due diligence measures in R60 need to be applied on a risk sensitive basis that includes an escalation by the firm of the measures that are proportionate to the firm's risk methodology.

! The objectives of the Notes in relation to customer identification documentation are first, that the evidence offered is reasonably capable of establishing the customer's identity, and secondly, that the person who is assessing the evidence is satisfied that the customer is the person he claims to be.

R72 The requirements in relation to the completion of satisfactory customer identification documentation are that:

a. the applicant for business will produce satisfactory evidence of his identity; or
b. procedures established by the firm will produce such satisfactory evidence.

7.7.1.1 Individuals

R73 For individuals perceived to present a low risk, a firm can satisfy the minimum customer identification documentation requirements by confirming the name and likeness by gaining sight of a document from a reliable and independent source that bears a photograph or from reliable and independent data sources.

For face-to-face customers a Gibraltar issued ID, Passport or local driving licence would easily meet this requirement. There is obviously a wide range of other documents that might be provided as evidence of identity. It is for each firm to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which might be easily forged or which can be obtained using false identities.

! With identity theft becoming more of a concern, firms must remain vigilant to guard against the provision of false or stolen customer identification documentation being used to open and operate business relationships. Nothing in these Notes requires firms to put in place additional controls to check the veracity of the documents provided other than what would normally be required as part of good business practice. However, firms may wish to use electronic verification and other such processes to verify that customer supplied documents have not been forged.

R74 The customer identification documentation, or data, obtained should demonstrate that a person of that name exists at the address given, and that the applicant for business is that person.

! The address of the applicant for business can also generally be determined from the same document and if the customer's risk profile is low, there is no requirement to seek additional documentary evidence.

R75 Where the document provided above does not contain details of the address, the address provided does not match that provided for the business relationship or the customer risk profile presents a higher risk, a firm will need to conduct separate address verification.

A firm can easily satisfy this requirement using electronic sources of data without having to ask the customer. This is preferred as this also then satisfies the independent criteria as this is sought by the firm itself.

! Care should be taken about applying this requirement too stringently, for example, where the address verification only shows up the spouse or family member of the applicant for business. In such cases, the firm needs to document the linkage between the applicant for business and the person at the given address.

R76 In respect of business relationships where the surname and/or address of the applicants for business differ, the name and address of all applicants, not only the first named, must be verified in accordance with the procedures set out above.

Any subsequent change to the customer's name, address, or employment details of which the institution becomes aware should be recorded as part of the know your customer process. Generally, this would be undertaken as part of good business practice and due diligence but also serves for money laundering, terrorist financing and proliferation financing prevention.

! The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard.

! An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for due diligence measures as set out in these Notes**.**

7.7.1.2 Bodies Corporate

R77 Where the applicant for business is a body corporate, the firm must ensure that:

a. it fully understands the company's legal form, and
b. it understands the company's structure and ownership.

Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, firms should take account of the availability of public information in respect of different types of company.

! The structure, ownership, purpose and activities of many corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering, terrorist financing or proliferation financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering, terrorist financing or proliferation financing. Similarly, where a company has issued share warrants to bearer these must be kept immobilised under the control of a licensee. This is because the Guidance Notes cannot be complied with and due diligence in accordance with the Guidance Notes cannot be carried out, where beneficial ownership can change without the knowledge of the licensee.

R78 Firms must put into place additional due diligence measures when establishing business relationships with non-Gibraltar registered companies, or companies with no direct business link to Gibraltar.

Such companies may be attempting to use geographic or legal complexities to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without an effective AML/CFT/CPF regime. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

R79 For corporates perceived to present a low risk, a firm can satisfy the minimum due diligence requirements by obtaining the following:

a. Either:
    1. Obtaining a copy of the certificate of incorporation/certificate of trade or equivalent which should include the:
        - full name; and
        - registered number.

OR

    2. Performing a search in the country of incorporation that confirms the items in (1) above.

a. registered office business addresses;
b. copy of the latest report and accounts, is available and audited if applicable; and
c. copy of the board resolution to open the relationship and the empowering authority for those who will operate any accounts.

Where the business relationship is being opened in a different name from that of the applicant, the institution should also make a search, or equivalent trading name search for the second name.

R80 The following persons and beneficial owners as (i.e. individuals or legal entities) must also be identified in line with 7.7.1.1 above:

a. the beneficial owner(s) of the company as defined in 7.1.2.1;
b. the shareholders of the company (if different from the beneficial owners) who own or control through direct or indirect ownership of 25% plus one share or the voting rights in the company including through the bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; and
c. The natural person(s) who otherwise exercise control over the management of the company.

R81 For corporate customers with multi-layered ownership structure, firms are required to document their understanding of the ownership and control structure of the natural and legal persons at each stage in the structure.

The key requirements are that such understanding is documented and must be obtained through reliable and verifiable sources. Such sources may include, for example, eligible introducers or group sources that the firm has determined and documented as reliable for these purposes or where documents have been obtained by the firm to demonstrate this.

The minimum level of detail to satisfy the documentation requirements required in these circumstances, for the intermediate legal entities, must include independently verifiable documents of the entity's existence and its registered shareholdings and management.

It will be on the basis of the firms' understanding of the ownership and control structure and the firm's assessment, of the Money Laundering, Terrorist Financing and Proliferation Financing Risk presented by the structure, that the firm will determine which of the natural persons are beneficial owners or exercise control of, more than 25% of, the applicant for business and whose identity needs to be verified in accordance with 7.7.1.1.

It will be up to the firm itself to demonstrate that, in accordance with its risk assessment, the documentation obtained is sufficient to meet the requirements.

A simple example would be to obtain for each entity a comprehensive company search report from a reliable company registry or registered agent. However just as there are alternatives to a passport and utility bill, so there are alternatives to a company search and another example might be to obtain a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party.

7.7.1.3 Partnerships and Unincorporated Businesses

R82 In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of all partners should be verified in line with the requirements for personal customers. In cases where the identified partner is not a natural person, steps should be taken to identify and verify beneficial ownership of the entity in line with the relevant requirements.

Where a formal partnership agreement exists, a mandate from the partnership authorising the opening of an account and conferring authority on those who will operate it should be obtained.

7.7.1.4 Retirement Benefit Schemes:

Approved Schemes where a Retirement Benefit Scheme has Income Tax Office approval, a firm's customer identification documentation can be met by confirming the scheme's approval.

Retirement Benefit Schemes approved by the Income Tax Guidance Notes are formed under an irrevocable trust. In other cases, a Retirement Benefit Scheme should be treated for AML/CFT/CPF purposes, and minimum due diligence requirements obtained, according to its legal form.

For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more pension trustees (or equivalent) to give the firm such instructions.

! The identities of individual signatories of Retirement Benefit Schemes need only be verified on a risk-based approach.

! Any payment of benefits by, or on behalf of, the trustees of an occupational pension scheme will not require verification of identity of the recipient.

R83 Where individual members of a Retirement Benefit Scheme are given personal investment advice, their identities must be verified. However, where the trustees and principal employer have been satisfactorily identified (and the information is still current), it may be appropriate for the employer to provide confirmation of identities of individual employees.

7.7.1.5 Charities, Church Bodies and Places of Worship

Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations.

R84 In each case, a charity should be treated for AML/CFT/CPF purposes, and the minimum due diligence requirements met by obtaining the necessary customer due diligence documentation, according to its legal form.

Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

7.7.1.6 Legal Persons, Trusts and Similar Legal Arrangements

There are a wide variety of trusts, ranging from large, internationally active organizations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs.

Firms must take measures to understand and obtain information on the purpose and intended nature of the business relationship.

R85 In carrying out their risk assessments firms take account of the different money laundering, terrorist financing or proliferation financing risks that trusts of different sizes and areas of activity present.

Most trusts and similar arrangements are not separate legal entities – it is the trustees collectively who are the customer. In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself. The purpose and objects of most trusts are set out in a trust deed.

R86 In respect of trusts, the firm should obtain the following information:

a. full name of the trust;
b. nature and purpose of the trust (e.g., discretionary, testamentary, bare);
c. country of establishment;
d. identity of the settlor or grantor;
e. identity of all trustees;
f. identity of any protector;
g. where the beneficiaries have already been determined, the identity of the natural person(s) who is the beneficial owner of the property; and
h. where the individuals that benefit from the legal arrangement have yet to be determined, the class of persons in whose main interest the arrangement is set up.

! The formal documentation of a beneficiary's identity need only be conducted prior to the distribution of trust assets and not when the trust is established or during its lifetime.

! Where a trustee is itself a regulated entity, or a publicly quoted company, or other type of entity, the identification procedures that should be carried out should reflect the standard approach for such an entity.

! Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

! Firms should take adequate measures in ascertaining whether the trustees of the trust hold basic information on other regulated agents of, and service providers to, the trust. This can include, but is not limited to, investment managers or advisors, accountants and tax advisors. The information to be held is s set in Section 61(2) of the Trustees Act.

R87 Firms must make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

For trusts presenting a lower money laundering, terrorist financing or proliferation financing risk, the minimum due diligence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering, terrorist financing or proliferation financing risk. In addition, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering.

R88 Where a trust is assessed as carrying a higher risk of money laundering, terrorist financing or proliferation financing, the firm must seek additional information in order to satisfy the customer identification documentation.

7.7.1.7 Clubs and societies

Where an application is made on behalf of a club or society, firms should make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

For many clubs and societies, the money laundering, terrorist financing or proliferation financing risk will be low.

R89 The following minimum due diligence must be conducted on clubs and societies:

a. Full name of the club/society
b. Legal status of the club/society
c. Purpose of the club/society
d. Names of all officers

R90 The firm should verify the identities of the officers of a club or society who have authority to operate an account or to give instructions concerning the use or transfer of funds or assets.

Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

7.7.2 Economic activity

The risks associated with money laundering, the financing of terrorism and proliferation financing stem from the associated activity either: that the funds that are going to be put through a business relationship derive from criminal activity and will use the business relationship to channel these

funds or, that proceeds of criminal activity will be mixed with legitimate economic activity in order to disguise their origin.

A two-pronged approach is therefore necessary if a firm is to properly address these risks.

The first of these entails identifying the source of the income or wealth that will form the basis of the business relationship. By determining that the source is not from criminal activity, the firm substantially mitigates the customer risk.

The second part of the approach is to identify the purpose and intended nature of the business relationship. By establishing this, the firm will be able to adequately monitor the activity on the business relationship and how this correlates to the intended activity. In the assessment of where these differ, the firm is able to ascertain better if money laundering, the financing of terrorism or proliferation financing is taking place.

7.7.2.1 The nature or source of wealth or funds

By seeking information on the nature or source of the business relationship's income or wealth, a firm is able to ascertain the risk posed to it in respect of money laundering, the financing of terrorism or proliferation financing by addressing both the customer risk as well as the country risk. In certain cases, the product risk will also be affected by the determination of the source of the economic activity.

See Appendix 4 for further guidance on source of wealth and funds.

R91 The minimum due diligence requirements to satisfy customer identification documentation on nature and source of income or wealth is ascertained by documenting this to a level of "plausible verifiability".

The term "plausible verifiability" is made up of two constituents:

- Plausible.
  This is the documentation that the customer's economic activity is commensurate with the information that the firm will have before it through its due diligence processes. It should be clear to a firm when a customer is providing a source of economic activity that it is incompatible with the information before it. In such cases, the firm should consider the implications of such a statement or evidence and whether, as a result, a suspicious transaction report should be made to GFIU.

- Verifiability.
  This is documentation of the economic activity to a level of detail that would enable the firm, law enforcement agencies or other bodies to independently verify the source of income or wealth if the customer's risk profile increased, or money laundering, financing of terrorism or proliferation financing was known or suspected. It is clear from this that a description of "business man" would clearly be inappropriate, as this is not verifiable. A description of "Management Consultant, MD of owner owned company X Management Consultants Limited of Number 1 The High Street, London, W23 1PX, UK" would be verifiable as the business and the address would be easily verifiable and the activity on the business relationship could easily be matched to the description provided. Again, any discrepancies between the information provided and the actual activity should prompt the firm to independently verify this information themselves or to make a suspicious transaction report.

! A firm will be able to identify the country risk posed to it from the source of the income or wealth of the business relationship.

R92 As the business relationship's risk profile increases, the firm must move away from "plausible verifiability" to "independent verification" of economic activity in order to satisfy the customer identification documentation requirements in relation to the source of income or wealth.

R93 Independent verification requires that firms seek additional information on the economic activity of the business relationship from reliable and independent sources.

7.7.2.2 Purpose of and intended nature

R94 At the commencement of the business relationship, a firm must document the purpose and intended nature of that relationship. This information must form part of the customer identification documentation.

The extent and detail of this information must be sufficient to allow the firm to readily identify variances between actual activity and the stated intended nature of the relationship and to increase information requirements in order to satisfy itself that money laundering, the financing of terrorism or proliferation financing has not taken place and where it is not satisfied as to the information received, to make a suspicious transaction report to GFIU. Section 7.8 below expands on the monitoring requirements further.

7.8 Monitoring Requirements

The requirement to monitor customer activity is derived from Article 12(2) of the MLD. These provisions have been incorporated into the Statements of Principles as well as the specific requirement of R94B. These are summarised below:

SP3 All firms must know their customer to such an extent as is appropriate for the risk profile of that customer.

R94A Conducting ongoing monitoring of the business relationship including the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions or activity being conducted are consistent with the firm's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and reviewing existing records. These records must be updated where necessary) to ensure that the documents, data or information held are up to date.

R95 Firms must pay special attention to any activity, which they regard as particularly likely, by its nature, to be related to money laundering, terrorist financing or proliferation financing. Such activity may include:

a) complex transactions;
b) unusually large transactions;
c) activity conducted in an unusual pattern;
d) activity which does not have an apparent economic or lawful purpose;

and in particular, a relevant financial business shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

7.8.1 What is monitoring?

R96 The essentials of any system of monitoring are that:

a. it flags up transactions and/or activities for further examination;
b. these reports are reviewed promptly by a senior independent person and where these raise a knowledge or suspicion of ML,TF or PF, report them to the MLRO; and
c. appropriate action is taken on the findings of any further examination.

Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken. In either case, unusual transactions or activities should be flagged for further examination, and do not necessarily require sophisticated electronic systems.

Monitoring may be by reference to specific types of transactions, to the risk profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

! Firms should also have systems and procedures to deal with:

- customers who have not had contact with the firm for some time, in circumstances where regular contact might be expected; and
- dormant accounts or relationships, to be able to identify future reactivation and unauthorised use.

! In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the customer, interface, country and product risk.

Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Higher risk accounts and customer relationships will generally require more frequent or intensive monitoring.

A monitoring system may be manual, or automated. One or other of these approaches may suit most firms. In the relatively few firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary.

The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters that determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of 'false positives', which require excessive resources to investigate and may be unnecessary.

Ongoing monitoring for specific activities related to TCSPs

TCSPs are not expected to scrutinise every transaction carried out by a trust, company or other legal entity to whom the TCSP provides services, however, the firm is required to carry out ongoing monitoring of its customer, regardless of the type of services it provides. It is imperative that the TCSP conducts adequate ongoing monitoring to ensure that the nature and activity of the client is in line with what is expected. Although the GFSC recognises that ongoing monitoring in cases where the firm does not provide directorship services may be more onerous, the requirements are still relevant. Furthermore, it may be argued that the AML/CFT/CPF risk posed increases where a TCSP solely provides registered office and/or secretarial services as it may have less oversight of the activities that the customer is carrying out.

Where the continued administration and management of the legal persons and arrangements (e.g. asset disbursements and corporate filings) would also enable the relevant TCSPs to develop a better understanding of the activities of their clients, there are several ways in which the firm can carry out ongoing monitoring of its customers dependant on the customer's risk profile and nature of their activity which may vary (e.g. asset holding company, trading company, consultancy company etc). This is a non-exhaustive list of examples of documents which could be requested from the client to assist in satisfying the ongoing monitoring requirement:

- Bank statements
- Annual Accounts
- Payment Receipts
- Invoices
- Board Minutes
- Rental agreement
- Contractual agreement
- Third party agreement
- Maintenance receipts (eg. of a property or a yacht)

In addition to the above examples and as part of the ongoing monitoring requirements, we would expect:

- TCSP firms to maintain its clients' accounting records at the registered office; and
- TCSP firms which provide directorship services to its clients, to maintain minutes from director's meetings at the registered office.

CHAPTER VIII

SP4 **Effective measures must be in place that require firms to have both internal and external reporting requirements whenever money laundering, terrorist financing or proliferation financing is known or suspected.**

8 Reporting Requirements

! Throughout these Notes, and this Chapter in particular, the term "suspicious transaction report" includes known as well as suspected activity of money laundering, terrorist financing or proliferation financing whether these are generated by a member of staff or automated monitoring systems.

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

There is a statutory obligation on all staff to report suspicions of money laundering, terrorist financing or proliferation financing. Section 28 contains the requirement to report to the "Appropriate Person" (for the purpose of these Notes called the Money Laundering Reporting Officer- see section 5.2) in accordance with internal procedures. In line with accepted practice, some businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting on to the MLRO or an appointed deputy.

! Once employees have reported their suspicions to the MLRO, they have fully satisfied the statutory obligations.

8.1 Knowledge, belief or suspicion or reasonable grounds

Both the legislation and Notes refer to the obligation to make a report either internally to the MLRO or by the MLRO to the GFIU if there is knowledge or suspicion or has reasonable grounds to suspect. It should be noted that under the Terrorism Act, the requirement to make a disclosure is if there is a "suspicion or belief". Before proceeding to explain the requirements of the reporting obligations, it is useful to consider the meaning of these two terms.

Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge could be inferred from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. However, the knowledge must have come to the firm (or to the member of staff) in the course of business. Information that comes to the firm or staff member in other circumstances does not come within the scope of the firms obligation to make a report.

A belief is less onerous than a knowledge but stronger than a suspicion. Therefore, the requirement to make a disclosure under the Terrorism Act is much wider in scope than that under the Proceeds of Crime Act.

Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:

"A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not";

and

"Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation." In a recent UK case[6] clarification on the basis upon the level of suspicion which leads to a suspicious transaction report is provided. Although the case refers, to the UK's Criminal Justice Act 1998 the legislation is comparative to the Proceeds of Crime Act and it is likely that should such a case occur in Gibraltar these precedents would apply.

In providing the judgement, LJ Longmore said that the existence of a suspicion was a subjective fact - there was no requirement that there should be reasonable grounds for the suspicion. Whilst it was misleading to use the words "inkling" or "fleeting thought", suspicion in this context meant only that the defendant must "think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts", or based upon "reasonable grounds"". In K Ltd, the court said that this definition of suspicion should also be applied to civil cases.

K Ltd and Da Silva now also provide some degree of clarity about the meaning of suspicion in the context of the UK's Proceeds of Crime Act regime. The "more than fanciful possibility" test also has a significant indirect effect, in that it confirms that the standard required for reporting suspicious transactions is extremely low. It is therefore all the more important for firms wishing to minimise the risk of prosecution for a failure to report to have training procedures in place for staff so that money laundering risks are recognised, and to have robust reporting procedures.

A transaction that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. Therefore, the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

A member of staff, including the MLRO, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

8.1.1 Reporting requirements in attempted money laundering scenarios

The POCA requires a firm to make a suspicious transaction report if money laundering is known or suspected. The requirement applies to all firms that conduct a relevant financial business so long

[6] R v Da Silva [2006] All ER(d) 131 (Jul)

as this knowledge or suspicion came about in the course of its trade, business, employment or during the application of customer due diligence measures.

R97 Where a potential or existing business relationship attempts to conduct money laundering through a new or established relationship but fails, the obligation to report to GFIU remains as this knowledge or suspicion came about from the firm's trade, business, profession or during the application of customer due diligence measures.

8.2 Internal Reporting

All members of a firms staff are obliged to report a knowledge, belief or suspicion of money laundering, terrorist financing or proliferation financing.

R98 Firms must establish clear processes for the reporting, processing, reporting and subsequent co-operation with law enforcement agencies arising out of an internal report. These processes must ensure that:

a. the reporting lines between the member of staff and the MLRO are as short as possible and that all members of staff have direct access to the MLRO;
b. the firm's MLRO must consider each such report and be considered in the light of all other relevant information held on the customer, and determine whether it gives grounds for knowledge or suspicion;
c. until the MLRO advises the member of staff making an internal report that no report to GFIU is to be made, further transactions or activity in respect of that customer, whether of the same nature or different from that giving rise to the previous suspicion, should be referred to the MLRO as they arise;
d. if the MLRO determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to GFIU in accordance with the requirements of 8.3 below as soon as is reasonably practicable after the information comes to him;
e. all reports to the MLRO are properly documented even if initially the reporting procedures permit a verbal report to be made, these must be appropriately documented at the earliest possible opportunity;
f. the MLRO should formally acknowledge receipt of the report which includes a reminder to the person who submitted the report of the "tipping off" provisions of the legislation; and
g. the records of suspicions and their associated investigations and documentation, including those not made externally be kept for at least five years.

8.3 External Reporting

The POCA and TO both refer to the Gibraltar Financial Intelligence Unit (GFIU) as the person to whom reports of suspected or known money laundering, terrorist financing or proliferation financing should be reported.

R99 For the purposes of these Notes, all suspicious transaction reports should be addressed to the Gibraltar Financial Intelligence Unit (GFIU):

The central agency for disclosure of suspicions is:
The Gibraltar Financial Intelligence Unit (GFIU)
Suite 832
Europort
Gibraltar

Tel 200 70211

Fax 200 70233
E-Mail admin@gfiu.gov.gi

The GFIU was established in January 1996 to facilitate the receipt, analysis and dissemination of suspicious transaction reports or suspicious activity reports (STRs/ SARs) made by financial and other institutions in accordance with the Drug Trafficking Act 1995, Terrorism Act 2018, Gambling Act 2005, Proceeds of Crime Act 2015 and Sanctions Act 2019. Since 2004, GFIU has been a member of the Egmont Group of Financial Intelligence Units.

8.3.1 Format of report

The use of a standard format in the reporting of disclosures is important and all firms are encouraged to use the GFIU's online reporting system (Themis). Access to this system can be obtained from the GFIU (https://www.gfiu.gov.gi/reporting). Further information and advice on Themis can be obtained from GFIU.

Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, to enable the investigating officer to conduct appropriate enquiries. The suspected criminality should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay.

Where additional relevant evidence is held that could be made available to the investigating officer, this should be added to the disclosure. Themis allows for the disclosure of additional information in various formats

The receipt of all disclosures will be acknowledged by GFIU. In the majority of cases, written consent will also be given to continue processing the transaction. However, in exceptional circumstances such as the imminent arrest of a customer and restraint of assets, consent may not be given. The reporting institution concerned will be made aware of the situation and should follow the directions of the Police or Customs officer in charge of the investigation.

R100 Where a firm has submitted a suspicious transaction report to GFIU or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the authorities even though the five-year limit may have been reached.

8.3.2 After a report has been submitted

Following receipt of a disclosure and initial research within GFIU, the information contained in the disclosure (not the disclosure itself) is allocated to a designated, trained financial investigator in either the Royal Gibraltar Police or HM Customs Gibraltar. An investigation will be mounted if appropriate, which will seek to obtain admissible evidence of criminal activity, leading ultimately to prosecution. As the investigation proceeds, evidential material may also be sought from the institution that made the original disclosure, generally by way of a Court Order. Where appropriate, information contained in the disclosure may also be copied to designated officers at the relevant regulatory authorities in Gibraltar.

The customer is not approached in the initial stages of the investigation and will not be approached unless criminal activity is identified. Courts generally recognise the need to protect sources of sensitive intelligence, and it is the duty of investigators to seek in such circumstances to obtain the relevant evidence by independent means.

The money laundering and terrorism legislation is drafted in such a way that reports submitted to GFIU may be allocated only to Police or Customs Officers for investigation.

Access to the information contained in disclosures is restricted to designated officers within the Royal Gibraltar Police, HM Customs Gibraltar and other regulatory authorities in Gibraltar. Whilst other officers may be involved in a subsequent investigation, the original information is restricted to GFIU and these designated officers. Maintaining the integrity of the confidential relationship that has developed between law enforcement agencies and disclosing institutions is of paramount importance.

It is therefore important that all disclosures be made to GFIU in accordance with these procedures. It is recognised however that there may be occasions when an urgent operational response is required which can only be effected by direct contact with RGP or Customs. In such circumstances, GFIU must be advised as soon as practicable and a written disclosure submitted as usual.

Whilst the legislation permits disclosure to any Police or Customs Officer, only GFIU will issue letters of acknowledgement and consent.

Following the submission of a disclosure report, a firm is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a "tipping-off" offence. Close liaison with GFIU and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

8.3.3 Feedback from the Investigating Authorities

The provision of feedback by the investigating agency to the disclosing firm is recognised as an important element of the system. Case officers in charge of investigations are encouraged to provide feedback, in general terms, as to the progress of investigations. GFIU may also provide feedback on such cases, and will provide to the institutions on a regular basis, feedback as to the volume and quality of disclosures and on the levels of successful investigations arising from them. Such information, whether provided verbally or in written form should not be used as the basis of subsequent commercial decisions.

Firms should ensure that all contact between particular sections of their organization and law enforcement agencies is reported back to the MLRO, so that an informed overview of the situation may be obtained. The MLRO should ensure that there is an established close co-operation and liaison with GFIU. In addition, Police or Customs will continue to provide information on request to a disclosing firm in order to establish the status of a specific investigation.

Disclosing firms should not be disheartened by a perceived lack of an immediate result following a disclosure, and should guard against dismissing further suspicions based on similar circumstances. Criminal investigations by their very nature, can take weeks, months or even years to result in arrest and conviction.

A disclosure may be the very first piece in a complex puzzle, or it may be the final piece that completes the picture.

8.4 Suspected Terrorists or Terrorist Financing Activities - additional requirements

The Terrorism Act provides for different types of terrorist related offences:

- Encouragement of Terrorism (s12-15)
- Preparation of terrorist acts and terrorist training (s16-24)
- Radioactive and Nuclear Terrorism Offences (s25-29)
- Other offences e.g. Hostage-taking (s30-34)
- Terrorist Financing (s35-39)

The full list of terrorist offences can be found in Schedule 1 of the Terrorism Act. Please note that any act which constitutes an offence under any other enactment relating to terrorism is also considered a terrorist offence.

R101 Where a firm has a suspicion or belief that terrorist financing is taking place it must ensure that the transaction or activity does not proceed any further until a disclosure to GFIU has been made and consent for the transaction or activity to proceed has been given.

R102 A disclosure made under the Terrorism Act must be accompanied with the information on which the suspicion or belief is based and must be made as soon as is practicable after the suspicion or belief was raised.

Two other items of legislation which are applicable in Gibraltar are the Terrorism (United Nations Measures) (Overseas Measures) Order 2001[36] and The Al-Qa'eda and Taliban (United Nations Measures)(Overseas Territories) Order 2002[37] (the "Terrorism Orders"). These Orders make provisions for the freezing and reporting of accounts held with financial institutions of named individuals.

R103 Firms are required, in order to comply with the provisions of the Terrorism Orders to search their customer base to ascertain whether any individuals named in them are matched. If a positive match is discovered, firms are required to freeze these business relationships and report this to the Governor.

8.5 Data subjects, access rights, suspicious transaction reports and the Data Protection Act

Occasionally, a request for access to personal data held by a data controller (a firm) under Section 14[38] the Data Protection Act will include within its scope one or more money laundering/terrorist financing/proliferation financing suspicious transaction reports, which have been submitted in relation to that customer to GFIU. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it.

On making a request in writing to a data controller, an individual is normally entitled to have made available to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data. Section 19[39] of the Data Protection Act provides that personal data is exempt from disclosure under Section 14 of the Act in any case where the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e. firms) should provide as much information as they can in response to a request.

Where a firm withholds a piece of information in reliance on the section 19 exemption, it is not obliged to tell the individual that any information has been withheld. The information in question can be omitted and no reference made to it when responding to the individual who has made the request.

In the absence of evidence to the contrary the disclosure of a suspicion report is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. In determining whether the Section 19 exemption applies, it is legitimate to take account of the fact that although the disclosure does not, in itself, provide clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime. It is also

legitimate to take account generally of the confidential nature of suspicious transaction reports when considering whether the exemption under Section 19 might apply.

In cases where the fact that a disclosure had been made had previously been reported in legal proceedings, or in a previous investigation, and the full contents of such a disclosure had been revealed, then it is less likely that the exemption under Section 19 would apply. However, caution should be exercised when considering disclosures that have been made in legal proceedings for the purposes of the Section 19 exemption, as often the disclosure will have been limited strictly to matters relevant to those proceedings, and other information contained in the original report may not have been revealed.

To guard against a tipping-off offence, MLROs should ensure that no information relating to suspicious transaction reports is released to any person without the MLRO's authorization. Further consideration may need to be given to suspicion reports received internally that have not been submitted to GFIU.

R104 A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off and/or the availability of the Data Protection Act's Section 19 exemption from access to personal data.

CHAPTER IX

SP5 **The firm will establish and maintain effective training regimes for all of its officers and employees.**

9 Training Requirements

The obligations in Section 27 of the Proceeds of Crime Act 2015 are expanded and clarified in the Notes.

The specific requirements in the Notes that refer to training are;

R2 b That appropriate training on money laundering is identified, designed, delivered and maintained to ensure that employees are aware of, and understand;

R2b.1 their legal and regulatory responsibilities and obligations;

R2b.2 their role in handling criminal property and terrorist financing;

R2b.3 the management of the money laundering, terrorist financing andand proliferation financing risk;

R2b.4 how to recognise money laundering, terrorist financing and proliferation financing transactions or activities; and

R2b.5 the firm's processes for making internal suspicious transaction reports.

R14 Where operational activities are undertaken by staff in other jurisdictions (for example, overseas call centres), those staff must be subject to the AML/CFT/CPF policies and procedures that are applicable to Gibraltar-based staff, and internal reporting procedures implemented to ensure that all suspicions relating to Gibraltar related accounts, transactions or activities are reported to the nominated officer in Gibraltar. Service level agreements will need to cover the reporting of management information on money laundering prevention, and information on training, to the MLRO in Gibraltar.

It is clear from the above requirements that the training obligations on all firms are extensive in both depth and scope.

The requirement is that training be appropriate. This is to say, that one training programme will not be suitable for all levels of employees. New employees' requirements will be different to those that have been with a firm for some time and are already aware of the firm's processes. Similarly, the appropriateness will be determined by the role played by that employee within the firm.

It is senior management's responsibility to ensure that the training programme is maintained. Therefore, one-off training would not be appropriate to meet this requirement as this calls on a firm to have a regular process through which the training needs of staff are considered.

The requirement also imposes an obligation on the firm to ensure that the staff "understand" the subject on which training has been provided and it is expected that training not be solely a passive exercise.

9.1 Legal and regulatory responsibilities and obligations

Training on the legal and regulatory responsibilities needs to include awareness training on the legislative provisions of the Proceeds of Crime Act, Terrorism Act and the UN Orders as well as the

regulatory requirements of these Notes as far as all of these are appropriate to the employees being trained.

9.2 Handling of criminal property and terrorist financing

Individuals need to receive training on their, as well as their employer's, liability if found to be involved in money laundering, terrorist financing or proliferation financing activities or if the obligations under the legislation or regulatory requirements are not met.

9.3 Risk Management

Staff are required to have an understanding of how a firm is managing the money laundering, terrorist financing and proliferation financing threats and how risk management techniques have been applied at the firm.

9.4 Recognition

The front-line of defence in any AML/CFT/CPF scenario is the awareness and alertness of staff in recognising suspicious activity. Specific and appropriate training on money laundering, terrorist financing and proliferation financing typologies must be provided to appropriate staff so that these may more readily detect suspicious activity.

9.5 Reporting

The firms internal reporting requirements must be understood by all staff so that if money laundering, terrorist financing or proliferation financing is known or suspected a report to the MLRO can be lodged in an effective and efficient manner.

9.6 Overseas branches or subsidiaries

Training to these same standards must be delivered and maintained to all overseas branches or subsidiaries including providers of relevant outsourced functions.

CHAPTER X

SP6 **Firms must be able to provide documentary evidence of their compliance with the legislation and these Notes**

10 Providing Documentary Evidence

10.1 Compliance Documentation

Documenting the processes a firm has in place becomes a vital component of compliance with the Notes. It is not enough to just provide documentary evidence of the due diligence performed on the customer but firms need to demonstrate that all the other processes have been given effect.

The requirements of these Notes also extend to how a firm has complied with the statements of principle, the senior management's responsibilities have been satisfied, the risk based approach designed and implemented, how each of the risks have been mitigated, how the firm's due diligence measures are escalated (or reduced) depending on the risk profile of the customer and how reports to GFIU considered and reported.

The Notes highlight the specific requirements that each firm must meet if it is to be held to be in compliance. In order to assist firms in this, the Compliance Report Template contains a checklist of all the statements of principles and requirements of these Notes. This can be found on the Financial Crime Approach web page[7]. Firms should complete this checklist at the earliest possible opportunity and design an action plan to address any deficiencies that are identified.

R105 As part of the FSC's risk-based methodology for assessing regulated firms, the Compliance Report and its accompanying action plan will be requested together with any risk questionnaires that form part of the normal risk assessment process.

It is therefore important that firms have in place a clear action plan to deal with deficiencies. The FSC does not expect full compliance with the revised requirements contained in these Notes immediately that they have come into force but does need to see senior management commitment to attaining full compliance within a reasonable period.

The risk-assessment on-site work conducted by the FSC will sample whether the practice of a firm matches the responses given by the firm.

10.2 Customer identification documentation

The requirement contained in Section 25 of the Proceeds of Crime Act to keep records of customers' identification and transactions is an essential constituent of the audit trail that the Sections seek to establish.

! In determining what relevant records are, firms need to also consider that Notes, e-mail exchanges and correspondence will augment the firm's knowledge of the customer and would therefore normally also be caught by the term relevant records.

If the law enforcement agencies investigating a money laundering case cannot link funds passing through the financial system with the original criminal money, then confiscation of those funds cannot be made. Often, the only valid role required of a firm in a money laundering, terrorist financing or proliferation financing investigation is as a provider of relevant records, particularly

[7] http://www.fsc.gi/fsc/financialcrime

where the money launderer, terrorist financier or proliferation financier has used a complex web of transactions specifically for the purpose of confusing the audit trail.

R106 The records prepared and maintained by any firm on its customer relationships and transactions should be such that:

a. requirements of legislation are fully met;
b. competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
c. any transactions effected via the institution can be reconstructed in such a manner as to provide evidence for prosecution of criminal activity, if necessary;
d. it includes results from any analysis undertaken by the firm;
e. the firm can respond swiftly to any enquiries or court orders from the appropriate authorities as to disclosure of information, including all CDD information and transaction records; and
f. businesses must maintain a record that:
    i. indicates the nature of the evidence obtained; and
    ii. comprises either a copy of the evidence or (where this is not reasonably practicable) contains such information as would enable a copy of it to be obtained.

R107 These records must be kept for at least five years from the date when the relationship with the customer has ended. In accordance with Section 25, this is the date of:

a. the carrying out of the occasional transaction, or the last in a series of linked occasional transactions; or
b. the ending of the business relationship; or
c. the commencement of proceedings to recover debts payable on insolvency.

This includes, where available, electronic identification means or relevant trust services as set out in the Electronic Identification Regulation (EIR)[8] or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the EIR supervisory body[9];

Where formalities to end a business relationship have not been undertaken but a period of five years has elapsed since the date when the last transaction was carried out, then the five year retention period commences on the date of the completion of that last transaction.

10.3 Transaction Records

R108 Section 25(3) requires firms to retain, for at least five years, records of all transactions undertaken in respect of relevant financial business. After 5 years, all personal data has to be deleted unless retention of the information is required by another enactment or the Minister issues an Order.

These should include the supporting evidence and records of all transactions (both domestic and international), including account files and business correspondence, results of any analysis undertaken, and any information that may be necessary to identify transactions. TheThe objective is to ensure, in so far as is practicable, that in any subsequent investigation the company/business can provide the authorities with its section of the audit trail. These record keeping requirements

[8] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

[9] This is the Gibraltar Regulatory Authority in its capacity as the supervisory body appointed under regulation 4 of the Electronic Identification and Trust Services for Electronic Transactions Regulations 2017;

are separate from those of the financial services regulators, but there is a considerable degree of overlap.

For each transaction, firms are expected to retain as a minimum, a record of:

- the name and address of its customer;
- the name and address (or identification code) of its counterparty;
- what the transaction was used for, including price and size;
- whether the transaction was a purchase or a sale;
- the form of instruction or authority;
- the account details from which the funds were paid (including, in the case of cheques, sort code, account number and name);
- the form and destination of payment made by the business to the customer; and
- whether the investments, etc. were held in safe custody by the business or sent to the customer or to his/her order and, if so, to what name and address.

10.4 Record Keeping By Eligible Introducers

Section 25(4) to (7) specifically addresses the responsibility for record keeping in respect of business introduced by eligible introducers. If the eligible introducer is itself authorised under the Financial Services, Banking, or Insurance Companies Acts for relevant financial business, the principal can rely on an assurance that the eligible introducer will keep, on the principal's behalf, the necessary records in respect of both verification of identity and transactions. It is of course necessary for the principal to keep copies of the records itself.

10.5 Format and Retrieval of Records

R109 To satisfy the requirements of the law enforcement agencies, it is important that all types of records are capable of retrieval without undue delay.

It is not necessary to retain documents in their original hard copy form, if the firm has reliable procedures for holding records in microfiche or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, an institution may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the institution itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

The Regulations do not state the location where relevant records should be kept but the overriding objective is for financial sector businesses to be able to retrieve relevant information without undue delay.

When setting document retention policy, firms must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or his agent, it is of assistance to the law enforcement agencies if these original documents are kept for at least one year to assist forensic analysis, and this can provide evidence to a financial institution when conducting its own internal investigations. However, this is not a requirement of the anti-money

laundering legislation and there is no other statutory requirement in Gibraltar that would require the retention of these original documents.

It is also of assistance to law enforcement, particularly in cases where a third party has been relied upon, to undertake verification of identity procedures or to confirm identity, that copies of all records relating to verification of identification are retained in Gibraltar.

! Institutions are asked to ensure that when original documents that would normally have been destroyed are required for investigation purposes, they check that the destruction policy has actually been adhered to before informing the law enforcement agencies that the documents are not available.

Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. However, if the documents are held in another jurisdiction, they must wherever possible (subject to local legislation) be freely available on request within the group, or otherwise be available to the investigating agencies under due legal procedures and mutual assistance treaties. Access to group records must not be impeded by confidentiality or data protection restrictions.

Financial sector businesses should also take account of the scope of money laundering legislation in other countries, and should ensure that group records kept in other countries that are needed to comply with Gibraltar legislation are retained for the required period. Particular care needs to be taken to retain or hand over the appropriate records when an introducing branch or subsidiary ceases to trade or have a business relationship with a customer whilst the relationship with other group members continues, or where a company holding relevant records becomes detached from the rest of the group.

10.6 Record keeping and legal proceedings

If legal proceedings commenced prior to 25 June 2015, require the retention of data, firms may retain the information until 25 June 2020.

After the 25 June 2020, all personal data shall be deleted unless retention of the information is required by another enactment or the Minister issues an Order.

CHAPTER XI

Appendix 1 – Explanation of the business risk assessment

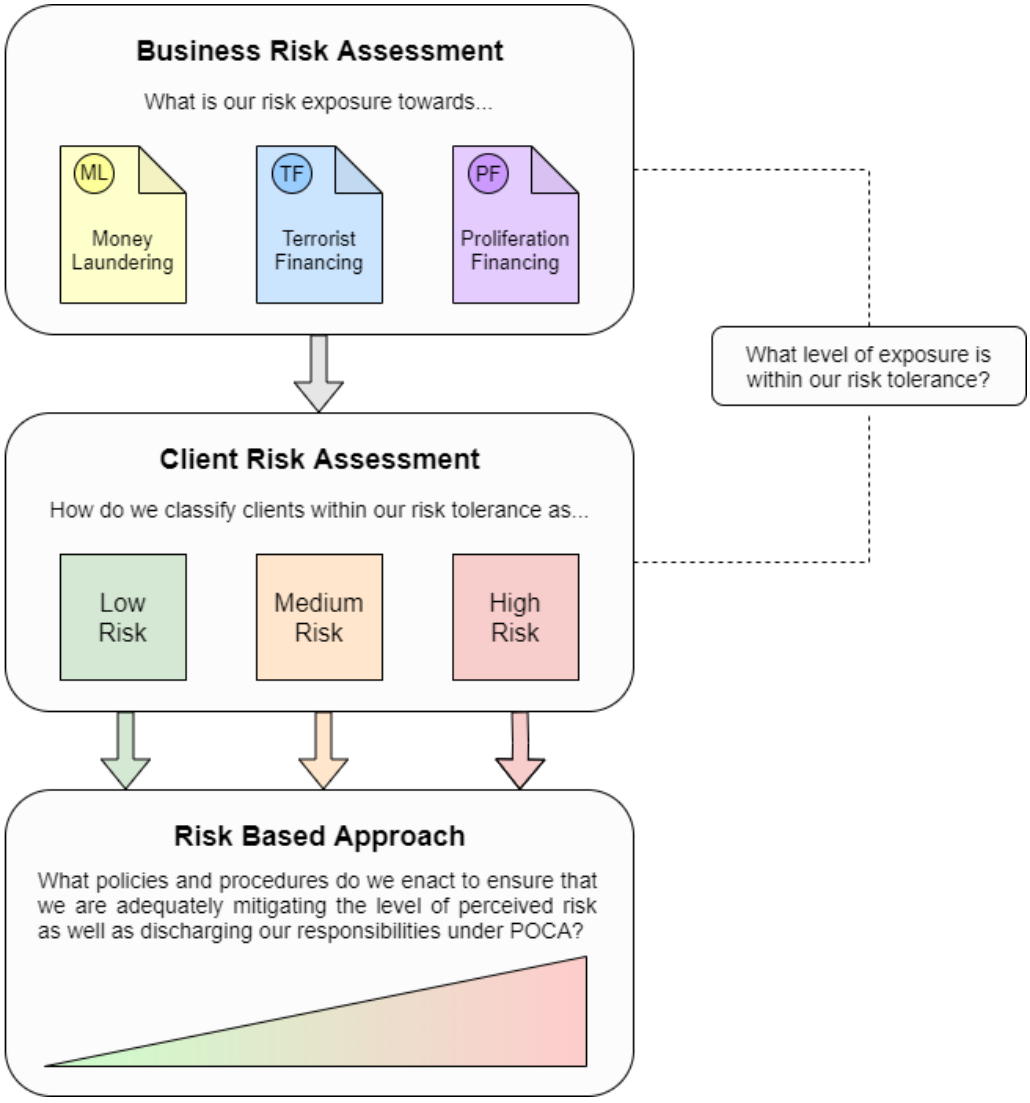
Purpose of the Business Risk Assessment

The business risk assessment should form the **basis** forfor all policies, procedures, methodologies and standards relating to anti-money laundering ("AML"), countering the financing of terrorism ("CFT") and counter proliferation financing ("CPF")")").). This should form part of each firms' wider risk management framework.

Fully understanding the inherent risks associated with a firm then allows that firm to determine what its **risk appetite** is (i.e. what subsequent business relationships it is willing to establish). For those business relationships that fall within its risk appetite, the firm must determine what systems of control must be in place to mitigate the level of risk posed by that relationship. The application of a **risk-based approach** allows for a proportionate application of these measures thatthat is commensurate to the level of risk posed by that relationship/client.

Figure 1 visually demonstrates the relationship between the business risk assessment, client risk assessments and the implementation of a risk-based approach.

Figure 1 – Business risk assessments, client risk assessments & the risk-based approach.



When considering the business risk assessment, it is important note that the assessment must:

1. "*Be proportionate to the size and nature of the relevant financial business*" (Section 25A(2), POCA); and
2. *"Be documented, kept up-to-date and made available to the relevant competent authorities concerned"* (Section 25A(3), POCA).

The principle of proportionality ensures that each firm is able to determine bespoke systems of control that are suitable to the size and nature of its business, while adequately combating the risk of ML/TF/PF and discharging its obligations under POCA. It is therefore the responsibility of each entity to determine the modality by which it will identify, assess, and mitigate the ML/TF/PF risks faced by its business operations.

Firms must also be able to demonstrate that their assessment of ML/TF/PF risks is documented and accessible. This is both to ensure that the information is available to the relevant competent authorities (such as the GFSC) when requested, as well as to warrant that relevant members of staff are fully aware of the ML/TF/PF risks faced by the business.

Conducting the Business Risk Assessment

Overview

As detailed above, it is the responsibility of each firm to determine the modality by which they conduct their business risk assessment. The execution of the business risk assessment, however, should in some form encompass the following basic steps:

1. Identification of the inherent ML, TF & PF related-risks associated with the business model;
2. Assessment/scoring of each of the identified risks;
3. Identification & application of risk reduction controls;
4. Assessment of the level of residual risk, considering implementation of the controls; and
5. Identification/application of any additional controls in cases outside of the business' risk tolerance.

The risk assessment process should be continuous, in that each regulated firm must periodically review the assessment to ensure that it still adequately encompasses all risks. As an example, deviation in business model or client base may mean that a business' risk exposures may change. Advancements in technologies, trends and vulnerabilities in the exploitation of financial businesses for the purposes of facilitating financial crime may also pose additional risks that were not originally considered. It is therefore imperative that the business remains continuously informed of both its regulatory obligations, and the advancement of international standards.

Regulated firms are able to seek professional assistance in conducting the risk assessment should they consider it to be appropriate. The obligations and liabilities under POCA, however, will remain with the regulated entity. It is therefore the responsibility of the regulated entity to ensure that the assessment adequately addresses the risk exposure of its business operations.

Identification of ML, TF & PF Risks

A firm's inherent exposure to risks relating to ML, TF & PF should be assessed by considering the following factors:

- The jurisdictions involved in the provision of services;
- The nature of the client base;
- The nature of the products and services offered; and
- The channels through which those products and services are delivered.

The nature of the risks associated with ML, TF & PF are often distinct and may vary in line with consideration of each of the above factors. A particular set of activities, for example, may exhibit a greater level of inherent vulnerability to one form of financial crime, while being less likely to be exploited for another. The individual

conducting the risk assessment must therefore have a robust understanding of the characteristics which may impact the assessment of ML, TF & PF.

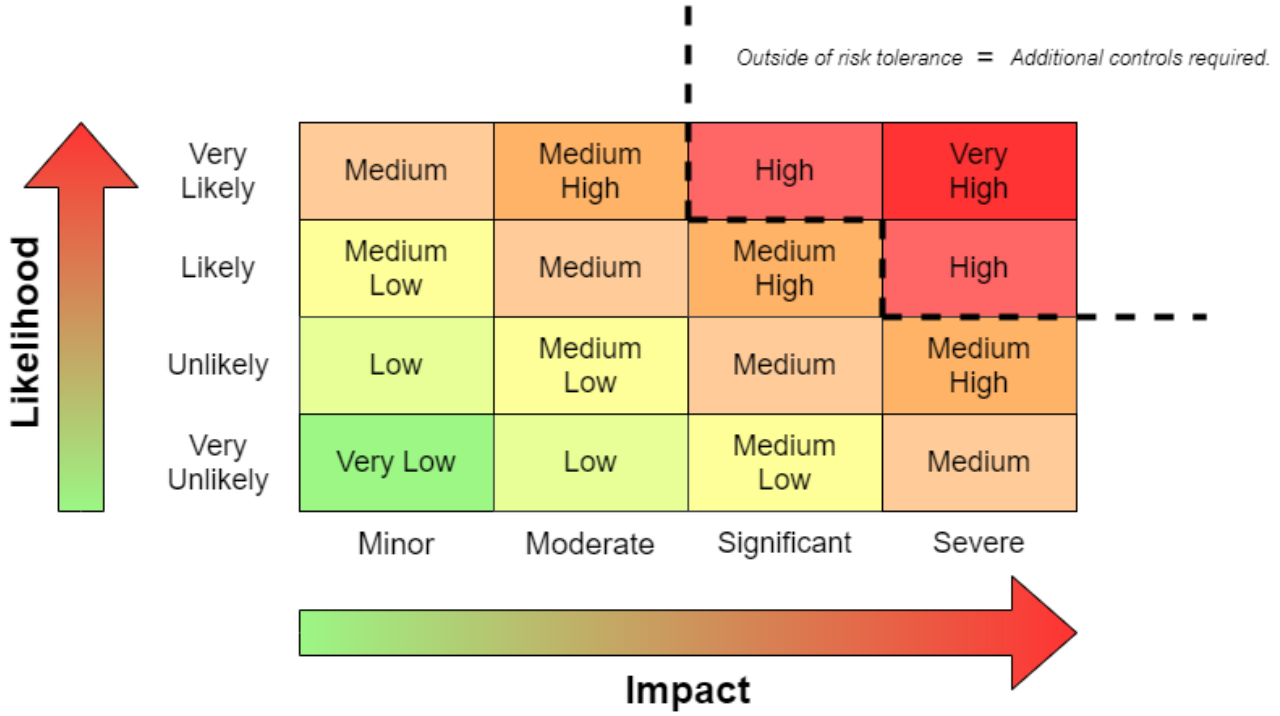
When conducting the assessment, relevant financial businesses must ensure to consult the **National Risk Assessment for AML/CFT and PF** published by HM Government of Gibraltar. This publication summarises the risks of ML, TF and PF specific to Gibraltar as a jurisdiction, including breakdowns of the risks associated with each of the relevant sectors within Gibraltar's financial services industry. For further guidance on business risk assessments specific to TF and PF, it is also recommended that reporting entities refer to the **Gibraltar Financial Intelligence Unit** ("GFIU") **Counter Proliferation Financing Guidance Notes** and **Counter Terrorist Financing Guidance Notes**.

Risk Scoring

Firms may employ varying methodologies when scoring the inherent/residual risks associated with their business operations. The scoring process allows for firms to determine which risks may be outside of their tolerance levels, and may require the implementation of additional mitigating controls or the re-consideration of risk appetite.

Below (**Figure 2**) shows an example of a risk scoring matrix which relies on an assessment of the likelihood of a risk materialising, as well as the impact of that materialisation taking place. Please note that firms are required to adequately document whichever scoring parameters are used for their assessment.

Figure 2 – Example risk scoring matrix.



Application of Risk Mitigation Controls

Once all inherent ML, TF and PF-related risks associated with the entities business operations have been identified and assessed, the entity must then determine what controls must be put in place in order to mitigate that risk and satisfy its regulatory and legislative requirements. This should be conducted on a continuous basis in order to assess both existing and novel risks.

When determining risk appetite, each firm should form an understanding of what level of risk is considered to be outside of itsits risk tolerance. Risks that arise outside of this should therefore trigger the need to establish additional controls. The persistence of risks outside of a business' risk tolerance may also be indicative that the firm should re-assess its risk appetite criteria.

Each firm should record its assessment in a format that is live and updated on a continuous basis. A risk register is an example of an appropriate live document used to record the assessment of risk faced by a business.

Appendix 2 – Explanation of the client risk assessment

Risk Methodology and risk factors

It is the responsibility of each firm to determine the method by which they will determine the level of risk posed by each of their client relationships. There are however, certain elements that must always be considered when risk assessing each client. These are:

1. Customer risk;
2. Product risk;
3. Interface risk; and
4. Country risk.

Note that a given client risk assessment methodology does not necessarily have to strictly be composed of each of the above elements in turn, as long as they are included within the scoring in one way or another. The client risk assessment should also be continuous.

The overall risk profile of a client will indicate the level of risk posed by the client to the firm's business, and hence will determine the level of due diligence expected to be carried out by a firm to manage and mitigate the potential risk.

Each regulated firm must therefore periodically review the assessment to ensure that it still reflects its clients' risk profile. The frequency of this review should be conducted on a risk-based approach.

Constructing Client Risk Assessment Methodology

In order to understand the risk of a potential client relationship, it is necessary to first have a solid understanding of the inherent risks facing thethe business, and the firm's risk appetite. When scoring the risk posed by each client, the portfolio of risks that are scored against should derive primarily from thethe firm's business risk assessment. This allows for greater emphasis or weight to be placed on a particular risk that is considered to be of greater impact or materiality to thethe firm's business model.

Below is an example of a client risk methodologymethodology that considers all four of the above-mentioned risk elements equally. Please note that each of the figures provided in this section are purely for example purposes and are not intended to be used directly by regulated entities. Each firm should determine what risk weighting they consider appropriate, in line with their assessment of their risk profile.

#	Risk Element	Risk Score	Risk Weight
1	Customer Risk		25%
2	Product Risk		25%
3	Interface Risk		25%
4	Country Risk		25%

Figure – Client Risk Assessment

As noted above, the risk weightings for each of the four elements should be considered and adjusted, according to the firm's own business risk assessment. For example, if a firm considers itsits exposure to interface risk as generally low, this element could be assigned a lower risk weighting, and the risk weighting be redistributed to a risk element considered of higher importance. For example:

#	Risk Element	Risk Score	Risk Weight
1	Customer Risk		30%
2	Product Risk		30%
3	Interface Risk		10%
4	Country Risk		30%

Figure – Client Risk Assessment

Other risk elements may be considered in line with the firm's own business risk assessment. If the firm has determined that a particular risk element is material, it should be considered within the client risk methodology.methodology. For example, source of wealth and/or source of funds, could be considered a risk that is specificspecific and material to a particular firm's client base.

#	Risk Element	Risk Score	Risk Weight
1	Customer Risk		25%
2	Product Risk		25%
3	Interface Risk		10%
4	Country Risk		30%
5	Source of Funds/Wealth Risk		10%

Figure – Client Risk Assessment

The risk score should reflect the level of risk that client poses for that particular element. A firm should develop guidelines for the scoring of each risk, in line with itsits assessment of itsits client base and risk tolerance. For example, firms could employ a risk scoring scale of 1-5, with 1 being the lowest risk and 5 being the highest risk.

#	Risk Element	Risk Score	Risk Weight
1	Customer Risk	1	25%
2	Product Risk	1	25%
3	Interface Risk	1	10%
4	Country Risk	1	30%
5	Source of Funds/Wealth Risk	1	10%

Figure – Client Risk Assessment

Overall Risk Scoring & Weighting

Following the completion of the client risk assessmentassessment, the scores and weight assigned to each element may be combined to produce an overall client risk score. To note that this is not necessary and firms may determine the follow up actions on each individual risk factors.

The example below highlights how a client scored as low risk on each of the elements would have an overall risk score of low.

#	Risk Element	Risk Score	Risk Weight
1	Customer Risk	1	25%
2	Product Risk	1	25%
3	Interface Risk	1	10%
4	Country Risk	1	30%
5	Source of Funds/Wealth Risk	1	10%
	Overall Risk Score	**1.00**	

Overall Client Risk	**Low Risk**

Figure – Client Risk Matrix – low risk

In the example below, a client who scores high risk for product risk and customer risk would score as a medium risk client.

#	Risk Element	Score	Weight
1	Customer Risk	4	25%
2	Product Risk	5	25%
3	Interface Risk	1	10%
4	Country Risk	1	30%
5	Source of Funds/Wealth Risk	1	10%
	Risk Score	**2.78**	
	Client Risk	**Medium Risk**	

Figure – Client Risk Matrix – medium risk

In the example below, a client who scores high risk for product risk and customer risk, medium risk for interface risk and source of funds/wealth risk and low risk for country risk would score as a high-risk client.

#	Risk Element	Score	Weight
1	Customer Risk	5	25%
2	Product Risk	5	25%
3	Interface Risk	3	10%
4	Country Risk	1	30%
5	Source of Funds/Wealth Risk	3	10%
	Risk Score	**3.43**	
	Client Risk	**High Risk**	

Figure – Client Risk Matrix – high risk

Alternatively, firms may consider it appropriate to set the overall risk score of a client as the score of the highest risk element. This is an alternative method to assessing the weight of each risk category as outlined in the example below.

#	Risk Element	Score
1	Customer Risk	1
2	Product Risk	1
3	Interface Risk	1
4	Country Risk	1
5	Source of Funds/Wealth Risk	5
	Risk Score	**5**
	Client Risk	**High Risk**

High Risk Factors

It is important to note that there are several factors which would lead to a client being automatically scored as high risk, regardless of thethe scoring on other risks. These clients would therefore be required to be subjected to enhanced due diligence and ongoing monitoring processes. These factors include:

- PEP status;
- High risk third countries; and
- Cases of increased ML, TF or PF risk (as identified by the firm or Minister by notice in the Gazette).

A firm may determine additional factors which are considered material and high risk to its own business, and would automatically lead to a client being scored as high risk, in line with itsits own risk tolerance levels and business risk assessment. A firm may determine, for example, that a particular set of client activities may pose a higher level of risk and would warrant that client being subjected to enhanced due diligence and monitoring processes.

Appendix 3 – Countries and territories with equivalent legal frameworks or those requiring enhanced due diligence

Countries and territories with equivalent legal frameworks

The jurisdictions that may be regarded as having equivalent legal frameworks for due diligence requirements purposes fall into the categories of:

- EU Member States
- EEA Countries
- UK Crown Dependencies

EU Member States (and the UK)

All member states of the European Union (which, for this purpose, includes Gibraltar as part of the UK) are required to enact legislation and financial sector procedures in accordance with the European Money Laundering Directives.

However, EU Directives are drawn up as a series of high-level requirements and significant variations currently exist in the measures that have been taken to transpose the Directives into national laws and regulations. It should also be noted that, whilst many EU Member States are also members of FATF, some have not yet implemented the revised FATF Recommendations that were approved and published in June 2003 and that evaluations completed before this date will be based on the 1996 version of the FATF Recommendations.

EU member states are listed here - https://europa.eu/european-union/about-eu/countries/member-countries_en

The United Kingdom has now left the EU. The Money Laundering Regulations transposed the EU Money Laundering Directives into UK law. The UK is also a member of the FATF.

EEA Member Countries & Switzerland

All EEA countries and Switzerland have undertaken to implement the European Money laundering Directives and some are also FATF member countries. However, as with EU Member States, variances can be expected to occur in the nature of their laws and regulations to prevent money laundering and to counter terrorist financing and the standards of compliance monitoring in respect of credit and financial institutions will also vary.

EEA Member Countries can be found here - https://en.wikipedia.org/wiki/European_Economic_Area

UK Crown Dependencies

The Isle of Man, Guernsey and Jersey (the UK Crown Dependencies) all voluntarily undertake to implement anti-money laundering, terrorist financing and proliferation financing legislation, regulation, and financial sector measures that meet international standards and that are broadly equivalent to the EU Directive and measures in place within Gibraltar. Following successful FATF-style mutual evaluations that were undertaken during 2000, IMF evaluations were completed on all three jurisdictions in 2003.

The IMF evaluators made a number of recommendations for change in each jurisdiction to bring them into line with the revised FATF recommendations and these changes are currently being implemented.

Non-Cooperative Countries And Territories (NCCT's)

In February 2000, FATF published a Report setting out the criteria for identifying those countries and territories that are not cooperative in the international fight against money laundering.

When constructing their internal procedures, firms should have regard to the need for additional monitoring procedures for transactions from countries that remain NCCT classified. Additional monitoring procedures will also be required in respect of correspondent relationships with financial institutions from countries on the non-cooperative country list. When considering what additional procedures are required, firms should take into account the following FATF assessment of the progress that has been made.

The countries classified as NCCT can be found on the FATF website - https://www.fatf-gafi.org/; and on the GFSC's website - https://www.fsc.gi/fsc/financialcrime

Countries and Territories on which sanctions apply

The EU implements all sanctions imposed by the United Nations Security Council ("UNSC"). When it comes to counterterrorist sanctions against individuals or entities, the EU has taken over the listing of terrorist suspects on behalf of Gibraltar. The EU implements the 1267 sanctions regime by instituting asset freezes, travel bans and arms embargoes against those included on the UNSC list. Moreover, the EU may impose autonomous sanctions against suspected individuals and entities, in line with its obligations under UNSCR 1373. Like the UNSC, the EU insists on the preventative/ administrative nature of the restrictive measures.

The EU gave effect to the UNSC 1267 sanctions regime by means of Common Position 2002/402/CFSP, implemented by Council Regulation (EC) No 881/2002, both adopted on 27 May 2002. The Annex to Regulation 881/2002 includes all the names on the 1267 Sanctions List to which EU restrictive measures will apply. The EU has amended the Regulation each time the UNSC or the Sanctions Committee has modified its sanctions list. In addition, Council Common Position 2003/140/CFSP of 27 February 2003 incorporates UNSC Resolution 1452(2002) allowing for humanitarian exceptions.

In 2011, when the UNSC created a separate sanctions regime for the Taliban, Council Common Position 2002/402/CFSP was amended accordingly to apply only to the individuals/entities associated with Al-Qaeda (Council Decision 2011/487/CFSP).

Following the adoption of UNSCR 2253(2015), the Council adopted Decision (CFSP) 2016/368 on 14 March 2016 amending the Common Position 2002/402/CFSP to extend the scope of application of restrictive measures to certain persons, groups, undertakings and entities associated with ISIL/Da'esh. Regulation 881/2002 was amended by Council Regulation (EU) 2016/363 accordingly.

On 20 September 2016, the Council adopted Council Decision (CFSP) 2016/1693 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them, and repealing Common Position 2002/402/CFSP. Since the Council decision establishes additional

restrictive measures, a new Council Regulation (EU) 2016/1686 was adopted, instituting an asset freeze against the persons and entities to be listed in its Annex I.

Council Decision (CFSP) 2016/1693 fulfils two objectives. The first is to continue to implement/transpose the sanctions against ISIL (Da'esh) and Al-Qaeda associates and supporters as designated on the UNSC Sanctions List. Secondly, it institutes the possibility of 'autonomous' restrictive measures against persons associated with ISIL (Da'esh) and Al-Qaeda or any group deriving thereof, in addition to those listed by the UNSC, to be designated in an annex to the Council Decision. The Council decides unanimously on the composition of the list and modifications to it on a proposal from any Member State or from the HR/VP.

As regards EU sanctions implementing the UNSC Sanctions List, each time the UNSC list is modified, the Regulation implementing the asset freeze at EU level – its annex listing the individuals and entities – is amended accordingly. The Commission was given the power to amend the annexes, 'for reasons of expediency'.

The Terrorist Asset Freezing Regulations 2011 ('TAFR') transposed Council Regulation (EC) No. 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism into Gibraltar law and thereby supplements the EU framework in respect of UNSCR 1373.

A designation under TAFR results in the freezing of the funds or economic resources owned, held or controlled by the designated person. Moreover, TAFR prohibits making funds, economic resources or financial services available directly or indirectly to or for the benefit of a designated person where the person making them available knows or has reasonable cause to suspect that they are doing so (and, in the case of economic resources, that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services).

A registration process through the below link must be completed in order to obtain access to the EU sanctions listings:

https://webgate.ec.europa.eu/europeaid/fsd/fsf

Institutions are requested to check whether they maintain any accounts for the entities and/or individuals listed and, if they do, are asked to freeze the accounts and report their findings to -

Gibraltar Financial Intelligence Unit

Suite 832 Europort

Gibraltar

Tel: (+350) 200 70211/200 70380

Fax: (+350) 200 70233

E-mail: gfiu@gcid.gov.gi

These checks are also to be undertaken as part of the client take-on process, at other intervals and on trigger events throughout the duration of a client relationship, as determined by an institutions risk based approach.

Appendix 4 – Guidance on source of wealth and funds

Purpose of establishing/verifying source of wealth and funds

Under Section 10F of the Proceeds of Crime Act 2015 ("POCA"), the application of customer due diligence measures includes "taking a risk-based approach to the verification of source of funds and wealth of the customer and beneficial owners". As defined by the Financial Action Task Force (FATF), source of funds ''refers to the origin of the funds or assets which are the subject of the business relationship between the firm and its client and the transactions the firm is required to undertake on the client's behalf (e.g., the amounts being invested, deposited or remitted)".

The FATF defines source of wealth as referring "to the origin of the entire body of wealth (i.e., total assets) of the client".

The purpose of obtaining a customer's source of wealth and funds is to assist the firm in developing an assessment of the economic profile of each customer. This profile should be scrutinised throughout the length of the business relationship to aid in the identification of any suspicious activity.

Plausible verifiability

The minimum due diligence requirements to satisfy customer identification documentation on source of funds and wealth is to document it to a level of plausible verifiability. This should be applied to low and medium risk clients.

The term "*plausible verifiability*" is made up of two parts:

Plausible

This is the documentation which evidences that the customer's economic activity is commensurate with the information obtained by the firm through its due diligence process. It should be clear to a firm that the funds a customer is providing are in line with the information held on the customer.

Verifiability

This is documentation relating to the economic activity of a client to a level of detail that would enable the firm, law enforcement agencies or other bodies to verify the source of income/wealth if the customer's risk profile increased, or money laundering or financing of terrorism was known or suspected.

Independent verification

In cases of higher risk, it is no longer considered adequate to apply standard due diligence and firms must apply enhanced due diligence measures. In these cases, firms are required to independently verify the source of funds and wealth of their customer. The information required should be considered on a case-by-case basis in line with the type and risk posed by the customer.

Independent verification requires that a firm corroborates the information provided by the client using reliable and independent sources.

Independent verification must be applied for PEPs, family members and close associates of PEPs. It must also be applied where the firm has risk profiled the customer as high risk.

In the case of high-net-worth individuals it may be difficult to assess the entirety of their income or wealth. In these cases, the extent of verification required should be in line with the risk profile of the individual and include independent verification of at least the majority of the customer's income or wealth.

Open-source information can be used for verification purposes, however, the information must be from a reputable and independent source.

Corporate clients

In the case of corporate clients, the requirement to establish or verify source of funds and wealth extends to its ultimate beneficial owners (UBOs), regardless of whether the funds or wealth of the entity are derived from the UBOs. This is due to the risk that the UBOs are in a position to transmit illicit funds through the entity.

In the case of the activity of the corporate itself, audited financial statements are typically sufficient for verifying source of funds and wealth. Where this is not an option, other documentation should be considered on a case-by-case basis.

Corroborating Examples of Source of Funds/Wealth Information

(This list is not exhaustive).

Source of funds/wealth	Examples
Employment income	• Name and address of employer; • Nature of business; • Annual salary and bonuses; • Recent payslip; • Latest accounts/tax declaration (if self-employed).
Savings	• Bank statement and enquiry on source of wealth.
Property sale	• Details of the property; • Copy of contract sale; • Title deed
Sale of shares or other investment	• Copy of contract; • Sale value of shares sold; • Statement of account from agent; • Transaction receipt/confirmation; • Shareholder's certificate; • Date of sale.
Loan	• Loan agreement; • Amount, date and purpose of loan; • Name and address of lender; • Details of any security.
Gift	• Date received; • Total amount; • Relationship to applicant; • Letter from donor explaining reason for the gift; • Certified identification documents of donor; • Source of wealth documentation of donor.
Maturity/Surrender of life policy	• Amount received; • Policy provider; • Policy number/reference; • Date of surrender.
Company sale	• Copy of the contract of sale;

	• Internet research of Company Registry; • Name and address of Company; • Total sales price; • Applicants' share participation; • Nature of business; • Date of sale and receipt of funds; • Media coverage.
Company profits/dividends	• Copy of latest audited financial statements; • Copy of latest management accounts; • Board of Directors approval; • Dividend distribution; • Tax declaration form.
Inheritance	• Name of deceased; • Date of death; • Relationship to applicant; • Date received; • Total amount; • Solicitor's details; • Tax clearance documents.

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor