TECHNICAL RELEASE 01/2019

Anti-Money Laundering Guidance for Members of the Bodies affiliated to the Consultative Committee of Accountancy Bodies in Ireland (CCAB-I)

Issue Date: 17th May 2019

This publication is based on requirements of Irish legislation regarding anti-money laundering and prevention of terrorist financing. It has been developed having appropriate reference to the Consultative Committee of Accountancy Bodies (CCAB) document 'Anti-Money Laundering Guidance for the Accountancy Sector (UK)'. Members of CCAB-I acknowledge the permission given by CCAB for the use of their document in the development of this publication.

DISCLAIMER

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland, The Association of Chartered Certified Accountants, The Institute of Certified Public Accountants and Chartered Institute of Management Accountants.

The content of this publication is provided as a guide only and does not purport to give professional advice. It should, accordingly, not be relied upon as such. No party should act or refrain from acting on the basis of any material contained in this publication without seeking appropriate professional advice. While every reasonable care has been taken by the member bodies of the Consultative Committee of Accountancy Bodies - Ireland (CCAB-I) in the preparation of this publication we do not guarantee the accuracy or veracity of any information or opinion, or the appropriateness, suitability or applicability of any practice or procedure contained therein. The member bodies of the CCAB-I are not responsible for any errors or omissions or for the results obtained from the use of the information contained in this publication.

To the fullest extent permitted by applicable law, the member bodies of the CCAB-I exclude all liability for any damage, costs, claims or loss of any nature, including but not limited to indirect or consequential loss or damage, loss of business profits or contracts, business interruption, loss of revenue or income, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or loss, damage to or corruption of data, whether arising from the negligence, breach of contract or otherwise of the member bodies of the CCAB-I, their committee members, employees, servants or agents, or of the authors who contributed to the text, even if advised of the possibility of such damages.

Similarly, to the fullest extent permitted by applicable law, the member bodies of the CCAB-I shall not be liable for any indirect or consequential losses including but not limited to, loss of business profits or contracts, business interruption, loss of revenue, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or damage to or corruption of data, nor shall it be liable for any damage, costs or losses of any nature (whether direct or indirect) occasioned by actions, or failure to act, by users of this publication or by any third party, in reliance upon the contents of this publication, which result in damages or losses incurred either by users of this publication, for whom they act as agents, those who rely upon them for advice, or any third party, or for any breach of contract by the member bodies of the CCAB-I in respect of any inaccurate, mistaken or negligent misstatement or omission contained in this publication.

All rights reserved. No part of this publication is permitted to be reproduced for resale, stored in a retrieval system for resale, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise for resale, or for any other purpose, without the prior and express written permission of the copyright holder. Nor is any right granted for any part of this publication to be copied or otherwise used in any presentation or training course without the prior and express written permission of the copyright holder. For professional advice on any of the matters referred to above, please contact the relevant member body of the CCAB-I.

Any issues arising out of the above will be governed by and construed in accordance with the laws of Ireland and the courts of Ireland shall have exclusive jurisdiction to deal with all such issues.

© Institute of Chartered Accountants in Ireland, Association of Chartered Certified Accountants, Institute of Certified Public Accountants, Chartered Institute of Management Accountants, 2019

Introduction

Accountants, together with other professionals and *financial institutions,* are key gatekeepers for the financial system, facilitating vital *transactions* that underpin the Irish economy. As such, they have an important role to play in ensuring their services are not used to further or assist a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity.

This Anti-Money Laundering Guidance has been developed by a *CCAB-I* working party comprising staff and volunteer practitioners and has been approved for issue by bodies affiliated to the CCAB-I. **This guidance is based on the law as of November 2018. It covers the prevention of money laundering and the countering of *terrorist financing*. It is intended to be read by any member who provides audit, accountancy, tax advisory, insolvency, or trust and company services in the Republic of Ireland.**

CONTENTS

1 ABOUT THIS GUIDANCE

- What is the purpose of this guidance?
- Who is the guidance for?
- What is the legal status of this guidance?

1.1 What is the purpose of this guidance?

1.1.1 **The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 has been amended by the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018, which gives effect to certain provisions of the Fourth Money Laundering Directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015).** In this document, the '*2010 Act*' refers to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by the Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing (Amendment) Act 2018.

1.1.2 Key changes introduced by the amending Act include greater emphasis on identification of beneficial owners of businesses, a wider definition of politically exposed persons, a requirement to apply procedures based on an enhanced risk based approach to assess and respond to potential money laundering or terrorist financing, enhanced requirements relating to client identification, and the removal of an earlier duty to report in relation to conduct of business with parties connected with a *high risk jurisdiction*, regardless of specific assessed risks arising from such business. This guidance has been prepared to help accountants undertaking activities that bring them within the definition of *designated persons* as set out in section 25 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2019 (see paragraph 1.2.1) to fulfil their obligations under the updated Irish legislation (in effect from 26 November 2018) to prevent, recognise and report money laundering. Compliance with it will assist compliance with the relevant legislation (including that related to counter *terrorist financing*) and professional requirements.

1.1.3 Terms that appear in *italics* in this Guidance are explained in the Glossary.

1.1.4 The term 'must' is used throughout to indicate a mandatory legal or regulatory requirement. *Accountancy firms* may seek an alternative interpretation of the Irish anti-money laundering and terrorist financing (AML) regime, but they must be able to justify their decision to their competent authority.

1.1.5 Where the law requires no specific course of action, 'should' is used to indicate good practice sufficient to satisfy statutory and regulatory requirements. *Accountancy firms* should consider their own particular circumstances when determining whether any such 'good practice' suggestions are indeed appropriate to them. Alternative practices can be used, but *firms* must be able to explain their reasons to their *competent authority*, including why they consider them compliant with law and regulation.

1.1.6 The Irish anti-money laundering regime applies only to *defined services* carried out by designated *businesses*. This guidance assumes that many a*ccountancy firms* will find it easier to apply certain AML processes and procedures to all of their services, but this is a decision for the *firm* itself. It may be unnecessarily costly to apply anti-money laundering provisions to services that do not fall within the *Irish AML regime*.

1.1.7 This guidance takes account, where relevant, to guidance issued by bodies other than *CCAB-I*. When those bodies revise or replace their guidance, the references in this document should be assumed to refer to the latest versions.

1.1.8 An *accountancy firm* may use AML guidance issued by other trade and professional bodies, where that guidance is better aligned with the specific circumstances faced by the *firm*. Where the *firm* relies on alternative guidance, it must (in accordance with 1.1.2 of this guidance) be in a position to explain this reliance to their *competent authority.*

1.1.9 The law which comprises the *Irish AML regime* is largely contained in the following legislation and relevant statutory instruments (SIs):

Legislation:

- Criminal tice (Money Laundering and Terrorist Financing) Act 2010;
- Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018;
- Criminal Justice (Corruption Offences) Act 2018;

- Criminal Justice Act 2011;
- Criminal Justice Act 2013, Part 2;
- Criminal Justice (Terrorist Offences) Act 2005.

Statutory Instruments:

- SI 486 of 2018 Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 (Commencement) Order 2018
- SI 487 of 2018 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018;
- SI 298 of 2018 Criminal Justice (Corruption Offences) Act 2018 (Commencement) Order 2018;
- SI No. 342 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Commencement) Order 2010
- SI No. 453 of 2016 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016;
- SI No. 79 of 2014 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority) Regulations 2014;
- SI No. 167 of 2013 Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2013;
- SI No. 347 of 2012 Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2012;
- SI No. 348 of 2010 Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010;
- SI No. 343 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2010;
- SI No. 342 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Commencement) Order 2010.

1.1.10 The *2005 Act* and *2010 Act* contain the Money Laundering and Terrorist Financing offences that can be committed by *individuals* or organisations. The *2010 Act* sets out the systems and controls that *firms* are obliged to possess, as well as the related offences that can be committed by *firms* and key *individuals* within them.

1.2 Who is this guidance for?

1.2.1 The guidance is addressed to those *designated persons* which are *accountancy firms* and members of the *CCAB-I* bodies, covered by Section 25 of the *2010 Act, who* act in the course of a business carried on by them in Ireland as

- an auditor,
- *an external accountant,*
- an insolvency practitioner,
- a *tax advisor*
- a provider to of investment advice under the Investment Business Regulations, and
- those who act in the course of business as *trust or company service providers* under Section 84 of the *2010 Act*.

For the purposes of this guidance the services listed above are collectively referred to as *defined services*. The scope of what would be considered carrying on business in Ireland is broad, and would include certain cross border business models where day to day management takes place from an Irish registered office or Irish head office.

1.2.2 Section 24 of the *2010 Act* defines an *external accountant* as someone who provides *accountancy services* to other persons by way of business. There is no definition given for the term *accountancy services*, however for the purposes of this guidance it includes any service which involves the recording, review, analysis, calculation or reporting of financial information, and which is provided under arrangements other than a contract of employment.

1.2.3 This guidance does not cover any other services, guidance for which may be available from other sources.

1.2.4 Guidance related to secondees and subcontractors can be found in APPENDIX A.

1.3 What is the legal status of this guidance?

1.3.1 This guidance has been prepared to assist accountants fulfil their legal obligations under legislation in force at the time of issue. This guidance is not intended to be exhaustive. If in doubt, seek appropriate advice or consult your supervisory authority. A copy of the guidance has been provided to the Department of Justice for information: however, formal approval has not been issued. The guidance will be updated for any matters of concern notified to us by the Department.

If a supervisory authority is called upon to judge whether an *accountancy firm* has complied with its general ethical or regulatory requirements, it is likely to be influenced by whether or not the *firm* has applied the provisions of this guidance.

2 MONEY LAUNDERING DEFINED

- What is money laundering?
- What is the legal and regulatory framework?

2.1 What is money laundering?

2.1.1 Definitions can be found in the Glossary section of this guidance. In this section, the definition of money laundering is discussed.

2.1.2 Money laundering is defined very widely in Irish law. It includes all forms of handling or possessing the *proceeds of criminal conduct* (as well as facilitating the use or possession) regardless of how it was obtained.

2.1.3 The '*proceeds of criminal conduct*' may take any form, including:

- Money or money's worth;
- Saved costs;
- Securities; and
- Tangible or intangible property.

Money laundering can involve the proceeds of offences committed in Ireland but also, in certain circumstances, of conduct overseas that; (i) is an offence in the place where the conduct takes place; and (ii) would have been an offence had it taken place in Ireland. There is no need for the proceeds to pass through Ireland. For the purposes of this guidance, except where otherwise stated, money laundering also includes *terrorist financing*. There are no materiality or 'de minimis' exceptions to *money laundering* or *terrorist financing* (*MLTF*) *offences*.

2.1.4 Money laundering activity can include:

- A single act (for example, possessing the proceeds of one's own crime);
- Complex and sophisticated schemes involving multiple parties;
- Multiple methods of handling and transferring the *proceeds of criminal conduct*; or
- Concealing the *proceeds of criminal conduct* or entering into arrangements to assist others to do so.

2.1.5 *Accountancy firms* need to be alert to the risks posed by:

- *Client*s;
- Suppliers;
- Employees; and
- The customers, suppliers, employees and associates of *client*s.

2.1.6 Neither the *firm* nor its *client* needs to have been party to money laundering for a reporting obligation to arise (see Section 6 of this guidance).

2.2 What is the legal and regulatory framework?

2.2.1 Sections 6 to 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the "***2010 Act***") define the primary *money laundering offences*. Inside or outside the *regulated sector* someone commits a *money laundering offence* if they, knowing or believing (or being reckless as to whether or not) that property is or 'probably comprises' the *proceeds of criminal conduct*, engages in any of the following acts in relation to the property:

- Concealing or disguising the true nature, source, location, disposition, movement or ownership or the property, or any rights relating to the property;
- Converting, transferring, handling, acquiring, possessing or using the property;
- Removing the property from, or bringing the property into, the State.

Any of these offences is punishable by up to 14 years' imprisonment and/or an unlimited fine.

2.2.2 None of these offences is committed if:

- The persons involved did not know or suspect (and were not reckless as to whether or not) that they were dealing with the *proceeds of criminal conduct*; or

- In advance of the possession or handling of the *proceeds of criminal conduct*, a report of the suspicious *transaction* is made promptly either by an *individual* internally in accordance with the procedures established by the accountancy firm (an *internal report*) or by an *individual* or an *accountancy firm* direct to:
    - *FIU Ireland* within the Garda Síochána (via the GoAML online reporting system); and
    - The Revenue Commissioners,

  before the act is committed. Section 42(7) of the *2010 Act* allows for such a report to be made immediately afterwards if it is not practicable to delay or stop the *transaction* or service from proceeding or the *accountancy firm* is of the reasonable opinion that failure to proceed with the *transaction* or service may result in the other person suspecting that a report may be (or may have been) made or that an investigation may be commenced or in the course of being conducted ('*tipping off*'); or
- The conduct giving rise to the *proceeds of criminal conduct* has taken place outside of Ireland, and the conduct was in fact lawful under the criminal law of the country/territory in which the act occurred.

2.2.3 The following offences apply to *designated persons* and *individuals* connected with a *designated person*:

- Failure to report (Section 42 of the *2010 Act*) a suspicion (or reasonable grounds for suspicion) of money laundering. Remember: there is **no 'de minimis' threshold value for reporting**.
- Disclosing that a suspicious transaction report *(STR)* has been made, or is required to be made, in a way that is likely to prejudice any subsequent investigation (which may also be referred to as a '*tipping off*' offence . For further information on the offences of ***prejudicing and investigation*** or ***tipping off'*** (Section 49 of the *2010 Act*) see Section 6 of this guidance.

2.2.4 In addition, there are reportable offences under the Criminal Justice (Terrorist Offences) Act 2005 (the "***2005 Act***"). These offences focus on the expected use of funds, regardless of their source.

3 RESPONSIBILITY & OVERSIGHT

- What are the responsibilities of *Accountancy firms*?
- What are the responsibilities of *senior management*, *MLRO* or other *nominated officer*?
- What policies, procedures and controls are required?

3.1 What are the responsibilities of *Accountancy firms*?

3.1.1 For *Accountancy firms* providing *defined services*, the *2010 Act* requires anti-money laundering systems and controls that meet the requirements of the *Irish anti-money laundering regime*. The *2010 Act* imposes a duty to ensure that persons involved in the conduct of the *firm's* business (see Section 8 of this guidance) are kept aware of these systems and controls and are trained to apply them properly. *Accountancy firms* are explicitly required to:

- Monitor and manage their own compliance with the *2010 Act*; and
- Ensure that policies, controls and procedures adopted in accordance with the *2010 Act* are approved by *senior management* and that such policies, controls and procedures are kept under review, in particular when there are changes to the business profile or risk profile of the *firm*.

3.1.2 *Accountancy firms* need to establish systems that create an internal environment or culture in which people are aware of their responsibilities under the *Irish anti-money laundering* regime and where they understand that they are expected to fulfil those responsibilities with appropriate diligence. In deciding what systems to install, an *accountancy firm* will need to consider a range of matters including:

- the type, scale and complexity of its operations;
- the different business types it is involved in;
- the types of services it offers, and its *client* profiles;
- how it sells its services;
- the risks associated with each area of its operations in terms of the risks of the *accountancy firm* or its services being used for *money laundering* or terrorist operations, or the risks of its *clients* and their counterparties being involved in such operations.

3.1.3 If a *firm* fails to meet its obligations under the *2010 Act*, civil penalties or criminal sanctions can be imposed on the *firm* and any *individuals* deemed responsible. This could include anyone in a senior position who neglected their own responsibilities or agreed to something that resulted in the compliance failure.

3.1.4 The primary *money laundering offences* defined under the *2010 Act* (see 2.2 of this guidance) can be committed by anyone inside or outside the regulated sector but *the 2010 Act* imposes specific provisions on *designated persons*.

3.1.5 *Accountancy firms* must have systems and controls capable of: assessing the risk associated with a *client*; performing CDD; *monitoring* existing *client*s; keeping appropriate records; and enabling staff to make an internal *STR* (i.e. *to the firm's Money Laundering Reporting Officer* ('*MLRO*') or other nominated person having responsibility for oversight of the *firm's* anti-money-laundering and reporting procedures. *).*

3.1.6 All persons involved in the conduct of the *accountancy firm's* business must be trained appropriately so that they understand both their own personal AML obligations and the firm-wide systems and controls that have been developed to prevent *MLTF*.

3.1.7 Effective internal risk management systems and controls must be established and the relevant *senior management* responsibilities clearly defined.

3.1.8 The *Competent Authority* for the *Accountancy firm* may, by formal request in writing, require that the *firm:*

- Appoint an *individual* at management level, (to be called a 'compliance officer') to monitor and manage compliance with, and the internal communication of, internal policies, controls and procedures adopted by the *designated person*;
- Appoint a member of *senior management* with primary responsibility for the implementation and management of anti-money laundering measures; and/or

- Undertake an independent, external audit to test the effectiveness of the internal policies, controls and procedures outlined in this section.

3.2 What are the responsibilities of *Senior Management*/*MLRO*?

3.2.1 The *2010 Act* defines *senior management* as: an officer or employee of the *Accountancy firm* with sufficient knowledge of the *firm's MLTF* risk exposure, and with sufficient authority, to take decisions affecting its risk exposure.

3.2.2 The *2010 Act* requires that the approval of *senior management* must be obtained:

- for the *firm's business risk assessment* (section 30A(5) of the *2010 Act*)
- for the policies, controls and procedures adopted by the *firm* (*2010 Act* section 54(4)).

3.2.3 Members of *senior management* undertaking such responsibilities should receive Continuing Professional Development (CPD) appropriate to their role.

3.2.4 Where requested under the *2010 Act* sections 54(7) or 54(8) to appoint an *individual* at management level to monitor and manage the *Accountancy firm's* internal policies, controls and procedures or to appoint a member of *senior management* with primary responsibility for the implementation and management of the *Accountancy Firm's* anti-money laundering measures the appointed *individual* should have:

- an understanding of the *accountancy firm*, its service lines and its *client*s;
- sufficient seniority to direct the activities of all members of staff (including senior members of staff);
- the authority to ensure the *firm's* compliance with the regime;
- the time, capacity and resources to fulfil the role;
- authority to represent that firm in legal proceedings.

3.2.5 A Money Laundering Reporting Officer ("*MLRO")* or other *nominated officer* may be appointed by the *accountancy firm* to manage its internal reporting procedures, taking responsibility for receiving internal *STRs* and making external *STRs* to the State Financial Intelligence Unit (*FIU Ireland*) and the Revenue Commissioners. This individual should also have the characteristics noted above.

3.2.6 Although not required under the *2010 Act*, unless requested by the *Competent Authority* under section 54 of the *2010 Act*, depending on the size, complexity and structure of an *Accountancy firm*, the *firm* may find it beneficial to appoint an *individual* at management level or to appoint a member of *senior management* with responsibility for ensuring the *firm's* compliance with the Irish anti-money laundering regime.

3.2.7 This role of ensuring the *firm's* compliance with the Irish anti-money laundering regime and that of the *MLRO* may be combined in a single *individual* provided that person has sufficient seniority, authority, governance responsibility, time, capacity and resources to do both roles properly. This guidance primarily describes the situation in which one *individual* fulfils the combined role, referred to in this guidance as the *MLRO.* The role of the *MLRO* is not defined in legislation but has traditionally included responsibility for internal controls and risk management around *MLTF*, in accordance with sectoral guidance. *Accountancy firms* with an *MLRO* should periodically review the *MLRO*'s brief to ensure that:

- it reflects current law, regulation, guidance, best practice and the experience of the *firm* in relation to the effective management of *MLTF* risk; and
- the *MLRO* has the seniority, authority, governance responsibility, time, capacity and resources to fulfil the brief.

3.2.8 The *accountancy firm* should ensure that there are sufficient resources to undertake the work associated with the *MLRO*'s role. This should cover normal working, planned and unplanned absences and seasonal or other peaks in work. Arrangements may include appointing deputies and delegates. When deciding upon the number and location of deputies and delegates, the firm should have regard to the size and complexity of the *firm's* service lines and locations. Particular service lines or locations may benefit from a deputy or delegate with specialised knowledge or proximity. Where there are deputies, delegates or both (or when elements of *firm's* AML policies, controls and procedures are outsourced), the *MLRO* retains ultimate responsibility for the *firm's* compliance with the Irish anti-money laundering regime.

3.2.9 All *MLROs*, deputies and delegates should undertake CPD appropriate to their roles.

3.2.10 The *MLRO* should:

- have oversight of, and be involved in, *MLTF* risk assessments;
- take reasonable steps to access any relevant information about the *firm*;
- obtain and use national and international findings to inform their performance of their role;
- create and maintain the firm's risk based approach to preventing *MLTF*;
- support and coordinate management's focus on *MLTF* risks in each individual business area. This involves developing and implementing systems, controls, policies and procedures that are appropriate to each business area;
- take reasonable steps to ensure the creation and maintenance of *MLTF* documentation;
- develop *Customer Due Diligence (CDD)* and on-going *monitoring* policies and procedures (including whether a customer is a 'politically exposed person' or '*PEP*'), consultation with and internal reporting to the *MLRO* (where applicable) or other *individual*(s) within the organisation as appropriate, and dissemination of such policies and procedures to all relevant staff;
- ensure the creation of the systems and controls needed to enable staff to make internal *STRs* in compliance with *2010 Act*;
- receive internal *STRs* and make external *STRs* to the *FIU Ireland* and the Revenue Commissioners;
- take remedial action where controls are ineffective;
- draw attention to the areas in which systems and controls are effective and where improvements could be made;
- take reasonable steps to establish and maintain adequate arrangements for awareness and training;
- monitoring the compliance of the *Accountancy firm* with the policy and procedures including reporting to *senior management* on compliance and addressing any identified deficiencies;
- receive the findings of relevant audits and compliance reviews (both internal and external) and communicate these to the board (or equivalent managing body);
- report to the *Accountancy firm's* leadership team (or equivalent managing body) at least annually, providing an assessment of the operations and effectiveness of the *firm's* AML systems and controls. This should take the form of a written report. These written reports should be supplemented with regular ad hoc meetings or comprehensive management information to keep *senior management* engaged with AML compliance and up-to-date with relevant national and international developments in AML, including new areas of risk and regulatory practice. The firm's leadership team (or equivalent managing body) should be able to demonstrate that it has given proper consideration to the reports and ad hoc briefings provided by the *MLRO* and then take appropriate action to remedy any AML deficiencies highlighted.

3.3 What policies, procedures and controls are required?

3.3.1 The *2010 Act* places certain requirements on *Accountancy firms* regarding *CDD* (Chapter three of Part 4 of the *2010 Act*) and 'record keeping, procedures and training' (Chapter six of Part 4 of the *2010 Act*). The following topics, all of which form part of the *MLTF* framework, need to be considered:

- risk based approach, risk assessment and management;
- *CDD*;
- record keeping;
- internal control;
- ongoing *monitoring*;
- reporting procedures;

- compliance management;
- communication;
- training and awareness.

3.3.2 The *2010 Act* provides different amounts of detail about the policies and procedures required in each area. *Accountancy firms* must implement and document policies, controls and procedures that are proportionate to the size and nature of the *firm*. These should be subject to regular review and update, and a written record of this exercise maintained.

Risk assessment and management

3.3.3 Every *Accountancy firm* must have appropriate policies and procedures for assessing and managing *MLTF* risks. To focus resources on the areas of greatest risk, a risk based approach must be adopted. The *firm* must carry out a *firm* risk assessment to identify and assess the risks of money laundering and *terrorist financing* involved in the *firm's* business activities. Such a *firm* risk assessment must at least take account of the risk factors set out in Section 30(A), Schedule 3 and Schedule 4 of the *2010 Act* (Schedule 3 and Schedule 4 of the *2010 Act* are reproduced in Appendix E to this guidance) (e.g. the type of customer, the products and services that are provided etc.) and the *firm* risk assessment must be approved by *senior management*. The *firm* risk assessment, and any related documents, should be kept up to date in accordance with the a*ccountancy firm's* internal policies, controls and procedures with new and changing risks considered as and when they are identified. Resources like the National Risk Assessment for Ireland, the Financial Action Task Force (*FATF*) mutual evaluations and Transparency International's corruption perception index can be useful when determining the *MLTF* risk faced by a firm. Information from the firm's *Competent Authority* must be taken into account. Further information on the risk based approach, types and categories of risk can be found in Section four of this guidance.

Customer Due Diligence (CDD)

3.3.4 *Accountancy firms* are responsible for developing *CDD* policies and procedures. These procedures should ensure that staff are aware of the factors to consider when assessing whether or not to establish a *business relationship* or undertake an *occasional transaction*, in light of the *MLTF* risks associated with the *client* and *transaction*. To ensure that the correct procedures are being followed, staff must be made aware of their obligations under the *2010 Act* and given appropriate training.

3.3.5 *Accountancy firms* already have procedures to help them avoid conflicts of interest and ensure they comply with professional requirements for independence. The requirements of the *2010 Act* can either be integrated into these procedures, to form a consolidated approach to taking on a new *client*, or addressed separately. For more on *CDD* see Section 5 of this guidance.

Reporting

3.3.6 Under *the 2010 Act* the reporting of knowledge or suspicion of money laundering is a legal requirement. It is the responsibility of the *Accountancy firm* to develop and implement internal policies, procedures and systems that are able to satisfy the *2010 Act* reporting requirements. Those policies must set out clearly, (a) what is expected of an *individual* who becomes aware of, or suspects, money laundering, and (b) how they report their concerns to the *MLRO.* All *staff* must be trained in these procedures.

More information on reporting suspicious *transactions* can be found in Section 6 of this guidance.

Record keeping

3.3.7 All records created as part of the *CDD* process, including any non-engagement documents relating to the *client* relationship and ongoing *monitoring* of it, must be retained for five years after the relationship ends. All records related to an *occasional transaction* must be retained for five years after the *transaction* is completed. A disengagement letter could provide documentary evidence that a *business relationship* has terminated, as could other forms of communication such as an unambiguous email making it clear that the *Accountancy firm* does not wish to engage or is ceasing to act.

3.3.8 Although no comparable retention period is specified for information and communications relating to internal and external *STRs*, a firm may wish to retain these securely for at least a period that meets the criteria set out by the Statute of Limitations.

3.3.9 *Accountancy firms* should bear in mind their obligation under the Data Protection Legislation 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 as necessary.

3.3.10 Where directed by a member of the Garda Síochána, not below the rank of Sergeant, the *Accountancy firm* may be required to retain documents and other records for a period up to a maximum of five years, additional to the initial period referred to at 3.3.8, for the purposes of an investigation related to money laundering or *terrorist financing*.

3.3.11 *Senior management* must ensure that all staff are made aware of these retention policies and that they remain alert to the importance of following them. There is more information on record keeping in Section 7 of this guidance.

Training and awareness

3.3.12 The *2010 Act* requires persons involved in the conduct of the *Accountancy firm's* business are made aware of the law relating to *MLTF* and given regular training in how to recognise and deal with suspicious *transactions* which may be related to *MLTF.* Though the *2010 Act* contains no express requirement, it is considered to be best practice for these provisions to be applied to all partners in *Accountancy firms* and to sole practitioners and to train all client-facing staff. In considering a training plan, *accountancy firms* need to keep in mind the objectives they are trying to achieve, which is to create an environment in relation to its business to prevent and detect the commission of money laundering and which thereby helps protect *individuals* and the *accountancy firm*.

3.3.13 The firm/*MLRO* should establish training capable of ensuring that staff:

- Are aware of what money laundering and *terrorist financing* is and how it is undertaken;
- Are aware of their legal and regulatory duties;
- Understand how to put those requirements into practice in their roles; and
- Are continuously updated about changes in
  - (a) the *firm's* AML policies, systems and controls, and
  - (b) the *MLTF* risks faced.

3.3.14 A formal training plan can help make sure that *staff* receive the right training to enable them to comply with their AML obligations.

3.3.15 Training should be tailored to suit the particular role of the *individual*.

3.3.16 Training methods may be selected to suit the size, complexity and culture of the *firm*, and may be delivered in a variety of ways including face to face, self-study, e-learning and video, or a combination of methods. *Accountancy firms* should keep records of attendance at, or completion of, training.

3.3.17 *Accountancy firms* need to make arrangements to ensure new members of staff or other *individuals* are trained as soon as possible after they join.

3.3.18 An *Accountancy firm* that fails to provide training for *staff* could be in breach of the *2010 Act* and at risk of prosecution. It would also risk failing to comply with Section 42 of *the 2010 Act*, which requires *Accountancy firms* to disclose any suspicions of money laundering. Although a 'reasonable excuse' defence against a failure to disclose for the *individual* (note that there is no money laundering case law on this issue and it is anticipated that only relatively extreme circumstances, such as duress and threats to safety, might be accepted) or the *professional privilege reporting exemption* provided under Section 46 of the *2010 Act* may be availed of, the *2010 Act* may still have been breached by the *Accountancy firm* because adequate training was not provided. For further information on training and awareness refer to Section 8 of this guidance.

Monitoring policies and procedures

3.3.19 The *MLRO* and/or appropriate *senior management* should together monitor the effectiveness of policies, procedures and processes so that improvements can be made when inefficiencies are found. Risks should be monitored and any changes must be reflected in changes to policies and procedures; keeping them up-to-date, in line with the risk assessment of the *Accountancy firm.* For more information, see Section 4 of this guidance.

3.3.20 In their efforts to improve AML policies, controls and procedures, and better understand where problems can arise, *senior management* should encourage staff to provide feedback. When changes are made to policies, procedures or processes these should be properly communicated to staff and supported by appropriate training where necessary.

3.3.21 *Accountancy firms* must introduce a system of regular, independent reviews to understand the adequacy and effectiveness of the *MLTF* systems and any weaknesses identified. Independent does not necessarily mean external, as some *firms* will have internal functions (typically audit, compliance or quality functions) that can carry out the reviews. Any recommendations for improvement should be monitored. Existing *monitoring* programmes and their frequency can be extended to include AML. The reviews should be proportionate to the size and nature of the *Accountancy firm.* A sole practitioner with no employees need not implement regular, independent reviews unless required by their *Competent Authority*.

3.3.22 As part of their improvement efforts the *senior manager* responsible for compliance and/or the *MLRO* should monitor publicly-available information on best practice in dealing with *MLTF* risks. For example, thematic reviews by regulators can be useful ways to improve understanding of good and poor practice, while reports on particular enforcement actions can illuminate common areas of weakness in AML policies, controls and procedures.

4 RISK BASED APPROACH

- What is the role of the risk based approach?
- What is the role of *senior management*?
- How should the risk analysis be designed?
- What is the risk profile of the *accountancy firm*?
- How should procedures take account of the risk based approach?
- What are the different types of risk?
- How important is documentation?

4.1 What is the role of the risk based approach?

4.1.1 The risk based approach is fundamental to satisfying the *FATF* recommendations, the *EU Directive* and the overall Irish *MLTF* regime. It requires governments, supervisors and *accountancy firms* alike to analyse the *MLTF* risks they face and make proportionate responses to them. It is the foundation of any *firm's* AML policies, controls and procedures, particularly its *CDD* and staff training procedures.

4.1.2 The risk based approach recognises that the risks posed by *MLTF* activity will not be the same in every case and so it allows the *firm* to tailor its response in proportion to its perceptions of risk. The risk based approach requires evidence-based decision-making to better target risks. No procedure will ever detect and prevent all *MLTF*, but a realistic analysis of actual risks enables a *firm* to concentrate the greatest resources on the greatest threats.

4.1.3 The risk based approach does not exempt low risk *client*s, services and situations from *CDD*, however the appropriate level of *CDD* is likely to be less onerous than for those thought to present a higher level of risk.

4.1.4 This section provides guidance on the analyses the *firm* will need to perform to properly underpin a risk based approach. Guidance on applying the risk based approach to particular AML procedures and controls can be found in the relevant sections of this guidance dedicated to those procedures.

4.2 What is the role of *senior management*?

4.2.1 *Senior management* is responsible for managing all of the risks faced by the *firm*, including *MLTF* risks. *t* should ensure that *MLTF* risks are analysed, and their nature and severity identified and assessed, in order so as to produce a risk profile. *Senior management* should then act to mitigate those risks in proportion to the severity of the threats they pose.

4.2.2 Where a risk is identified, the *firm* must design and implement appropriate procedures to manage it. The reasons for believing these procedures to be appropriate should be supported by evidence, documented and systems created to monitor effectiveness. A *firm's* risk based approach should evolve in response to the findings of the systems monitoring the effectiveness of the AML policies, controls and procedures.

4.2.3 The risk analysis can be conducted by the *MLRO*, but must be approved by *senior management* (see section 30A of the *2010 Act*). This is likely to include formal ratification of the outcomes, including the resulting policies and procedures, but may also include close *senior management* involvement in some or all of the analysis itself.

4.2.4 The risk profile and operating environment of any *firm* changes over time. The risk analysis must be refreshed regularly by periodic reviews, the frequency of which should reflect the *MLTF* risks faced and the stability or otherwise of the business environment. In addition, whenever *senior management* sees that events have affected *MLTF* risks, the risk analysis should also be refreshed by an event-driven review. A fresh analysis may require AML policies, controls and procedures to be amended, with consequential impacts upon, for example, the training programs for relevant employees.

4.3 How should a risk analysis be designed?

4.3.1 One possible first step is to consider the *MLTF* risks faced by each different part of the *firm*. The *firm* may already have general risk analysis processes, and these could form the basis of its *MLTF* risk analysis.

4.3.2 When designing an analysis process the *firm* should look not only at itself but at its *client*s and markets as well. Consider factors that lower risks as well as those that increase them; a *client* subject to an effective *AML regime* may pose a lower risk than one not. *Accountancy firms* should take into account the findings of the most recent National Risk Assessment, together with any guidance issued by the relevant *competent authority,* including Schedules 3 and 4 of the *2010 Act* (as reproduced in Appendix D of this guidance).

4.3.3 *MLTF* risks include the possibility that the *firm* might:

- Be used to launder money (e.g. by holding criminal proceeds in a fund or a *client* money account, or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
- Be used to facilitate *MLTF* by another person (e.g. by creating a corporate vehicle to be used for money laundering or by introducing a money launderer to another regulated entity);
- Suffer consequential legal, regulatory or reputational damage because a *client* (or one or more of its associates) is involved in money laundering;
- Fail to report a suspicion of MLTF.

4.3.4 Risks should be grouped into categories, such as '*client*', 'service' and 'geography'. Some risks will not easily fit under any one heading but that should not prevent them from being considered properly. Nor should a *firm* judge overall risk simply by looking at individual risks in isolation. When two threats are combined they can produce a total risk greater than the sum of the parts. A particular industry and a particular country may each be thought to pose only a moderate risk. But when they are brought together, perhaps by a particular *client* or *transaction*, then the combined risk could possibly be high. *Firms* should avoid taking a 'tick-box' approach to assessing *MLTF* risk in relation to any individual *client* but should, instead, take reasonable steps to assess all information relevant to its consideration of the risk.

4.4 What is the risk profile of the *accountancy firm*?

4.4.1 An *accountancy firm* with a relatively simple *client* base and a limited portfolio of services may have a simple risk profile. In which case, a single set of AML policies, controls and procedures may suffice right across its operations. On the other hand, many *firms* will find that their risk analysis reveals quite different *MLTF* risks in different aspects of the *firm*. *Accountancy services*, for example, may face significantly different risks to insolvency, bankruptcy and recovery services. A risk analysis allows resources to be targeted, and procedures tailored, to address those differences properly.

4.4.2 When a *firm* decides to have different procedures in different parts of its operations, it should consider how to deal with *client*s whose needs straddle departments or functions, such as:

- A new *client* who is to be served by two or more parts of the *firm* with different AML policies, controls and procedures;
- An existing *client* who is to receive new services from a part of the *firm* with its own distinct AML policies, controls and procedures.

4.4.3 The risk based approach can also take into account the *firm's* experience and knowledge of different commercial environments. If, for example, it has no experience of a particular country, it could treat it as a normal or high risk even though other *firms* might consider it low risk. Similarly, if it expects to deal with only Irish individuals and entities, it may treat as high risk any *client* associated with a non-Irish country.

4.5 How should procedures take account of the risk based approach?

4.5.1 Before establishing a *client* relationship or accepting an engagement an *accountancy firm* must have controls in place to address the risks arising from it. The risk profile of the *firm* should show where particular risks are likely to arise, and so where certain procedures will be needed to tackle them.

4.5.2 Risk based approach procedures should be easy to understand and easy to use for all staff who will need them. Sufficient flexibility should be built in to allow the procedures to identify, and adapt to, unusual situations.

4.5.3 The nature and extent of AML policies, controls and procedures depend on:

- The nature, scale, complexity and diversity of the *firm*;

- The geographical spread of *client* operations, including any local AML regimes that apply; and
- The extent to which operations are linked to other organisations (such as networking businesses or agencies).

4.5.4 *Accountancy firms* should have different *client* risk categories such as: low, normal, and high. The procedures used for each category should be suitable for the risks typically found in that category. For example, if it is normal for a *firm* to deal with *client*s from a *high-risk country*, the *firm's* procedures for what they regard as normal *client*s must be designed to address the risks associated with the *high-risk country*. Some low and high risk indicators can be found in APPENDIXD.

4.5.5 Regardless of the risk categorisation, *firms* will still be expected to undertake *monitoring* of the *client* relationship. Such *monitoring* must be done on a risk based approach, with levels of *monitoring* varying depending on the *MLTF* risk associated with individual *client*s.

4.5.6 Taking into account key risk categories, an *accountancy firm* may be able to draw up a simple matrix in order to determine a *client*'s risk profile. Such risk categories may include a *client*'s legal form, the country in which the *client* is established or incorporated, and the industry sector in which the *client* operates. In addition, *firms* should also consider the nature of the service being offered to a *client* and the channels through which the services/*transactions* are being delivered.

4.5.7 Elevated risks could be mitigated by:

- Conducting enhanced levels of due diligence – i.e., increasing the level of *CDD* that is gathered.
- Carrying out periodic *CDD* reviews on a more frequent basis.
- Putting additional controls around particular service offerings or *client*.

4.6 What is *client* risk?

4.6.1 A *firm* should consider the following question, "Does the *client* or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers?"

4.6.2 *Client* risk is the overall *MLTF* risk posed by a *client* based on the key risk categories, as determined by a *firm*.

4.6.3 The *client*'s risk profile may also inform the extent of the checks that need to be performed on other associated parties, such as the *client*'s beneficial owners.

4.6.4 Undue *client* secrecy and unnecessarily complex ownership structures can both point to heightened risk because company structures that disguise ownership and control are particularly attractive to people involved in *MLTF*.

4.6.5 In cases where a *client* (an individual) or beneficial owner of a *client* is identified as a *PEP* (including a domestic *PEP*), an enhanced level of due diligence must be performed on the *PEP*. Further details on the approach to be taken in such circumstances are set out in 5.3.11 - 5.3.22 of this guidance.

4.7 What is service risk?

4.7.1 A *firm* should consider the following question "Do any of our products or services have attributes known to be used by money launderers or terrorist financiers?"

4.7.2 Service risk is the perceived risk that certain products or services present an increased level of vulnerability in being used for *MLTF* purposes.

4.7.3 *Firms* should consider carrying out additional checks when providing a product or service that has an increased level of *MLTF* vulnerability.

4.7.4 Services and products in which there is a serious risk that the *accountancy firm* itself could commit a *money laundering offence* should also be treated as higher risk. For example, wherever the *accountancy firm* may commit an offence under Sections 7 and 10 to 11 or 30A(1)(b) of the *2010 Act* such as the use of the *accountancy firm's client* monies account to inadvertently facilitate money laundering.

4.7.5 Before a *firm* begins to offer a service significantly different from its existing range of products or services, it should assess the associated *MLTF* risks and respond appropriately to any new or increased risks.

4.8 What is geographic risk?

4.8.1 A *firm* should consider the following question "Are our *client*s established in countries that are known to be used by money launderers or terrorist financiers?"

4.8.2 Geographic risk is the increased level of risk that a country poses in respect of *MLTF*.

4.8.3 When determining geographic risk, reference should be made to the EU identification of higher risk jurisdictions (see Appendix D): other factors to consider may include the perceived level of corruption, criminal activity, and the effectiveness of *MLTF* controls within the country.

4.8.4 *Firms* should make use of publicly available information when assessing the levels of *MLTF* of a particular country, e.g. information published by civil society organisations such as Transparency International and public assessments of the *MLTF* framework of individual countries (such as *FATF* mutual evaluations and the EU designation of *high risk financial jurisdictions*).

4.8.5 Although some countries may carry a higher level of *MLTF* risk, those *firms* that have extensive experience within a given country may reach a geographical risk classification that differs to those that that only have a limited exposure (refer to http://www.centralbank.ie/ for a list of countries).

4.9 What is sector risk?

4.9.1 A *firm* should consider the following question "Do our *client*s have substantial operations in sectors that are favoured by money launderers or terrorist financiers?"

4.9.2 Sector risks are the risks associated with certain sectors that are more likely to be exposed to increased levels of *MLTF*.

4.9.3 *Firms* should consider the sectors in which their *client* has significant operations, and take this into account when determining a *client*'s risk profile. When considering what constitutes a high risk sector, *firms* should take into account the findings of the most recent National Risk Assessment (available at www.justice.ie) for Ireland, together with any guidance issued by the relevant *competent authority* for the *designated person*.

4.10 What is delivery channel risk?

4.10.1 A *firm* should consider the following question "Does the fact that I am not dealing with the *client* face to face pose a greater *MLTF* risk?"

4.10.2 Certain delivery channels can increase the *MLTF* risk, because they can make it more difficult to determine the identity and credibility of a *client*, both at the start of a *business relationship* and during its course.

4.10.3 For example, delivery channel risk could be increased where services/products are provided to *client*s who have not been met face-to-face, or where a *business relationship* with a *client* is conducted through an intermediary.

4.10.4 *Firms* should consider the risks posed by a given delivery channel when determining the risk profile of a *client*, and whether an increased level of *CDD* needs to be performed.

4.11 Why is documentation important?

4.11.1 *Accountancy firms* must be able to demonstrate to their relevant *competent authority* how they assess and seek to mitigate *MLTF* risks. This *firm* risk assessment must be documented, and made available to the relevant *competent authority* on request. The documentation should demonstrate how the ***accountancy firm's*** risk assessment informs their policies and procedures. *Accountancy firms'* risk assessments must also be approved by *senior management* and kept up to date in accordance with internal policies, controls and procedures.

5 *CUSTOMER DUE DILIGENCE* (*CDD*)

- What is the purpose of *CDD*?
- When should *CDD* be carried out?
- How should *CDD* be applied?
- What happens if *CDD* cannot be performed?

5.1 What is the purpose of *CDD*?

5.1.1 Criminals often seek to mask their true identity by using complex and opaque ownership structures. The purpose of *CDD* is to know and understand a *client*'s identity and business activities so that any *MLTF* risks can be properly managed. Effective *CDD* is, therefore, a key part of AML defences. By knowing the identity of a *client*, including who owns and controls it, a *firm* not only fulfils its legal and regulatory requirements it equips itself to make informed decisions about the *client*'s standing and acceptability.

5.1.2 *Customer due diligence* measures are a key part of the anti-*money laundering* requirements. They ensure that *accountancy firms* know who their *clients* are, ensure that they do not accept *clients* unknowingly which are outside their normal risk tolerance, or whose business they will not understand with sufficient clarity to be able to form *money laundering* suspicions when appropriate. If an *accountancy firm* does not understand its *client's* regular business pattern of activity it will be very difficult to identify any abnormal business patterns or activities. In addition, *accountancy firms* must be in a position to supply the *client's* identity in the event that the *accountancy firm* is required to submit an *external report* to *FIU Ireland* and the Revenue Commissioners.

5.1.3 Many *accountancy firms* will have other procedures for *client* acceptance, for example to ensure compliance with professional requirements for independence and to avoid conflicts of interest. The requirements of the *2010 Act,* may either be integrated with those procedures or addressed separately. In either case, initial *customer due diligence* information not only assists in acceptance decisions, but also enables the *accountancy firm* to form well-grounded expectations of the *client*'s behaviour which provides some assistance in detecting potentially suspicious behaviour during the *business relationship.*

5.1.4 The processes required for compliance with anti-money laundering initial *customer due diligence* requirements contribute vitally to the overall picture of potential *clients* and appropriate risk assessment of them. However a lack of concern raised during *customer due diligence* does not mean that the *client* and engagement will remain in their initial risk category. Continued alertness for changes in the nature or ownership of the *client*, its business model, or its susceptibility to money laundering – or actual evidence of the latter – must be maintained.

CDD principles

5.1.5 Sections 33 through 39 of the *2010 Act4* the required components of *CDD*. *Accountancy firms* must apply them, (a) at the start of a new *business relationship* (including a company formation), (b) at appropriate points during the lifetime of the relationship and (c) when an *occasional transaction* is to be undertaken. The required components are:

- Identifying the *client* (i.e., knowing who the *client* is) and then verifying their identity (i.e., confirming that identity is valid by obtaining documents or other information from sources which are independent and reliable) (see Appendix B);
- Identifying beneficial owner(s) so that the ownership and control structure can be understood and the identities of any individuals who are the owners or controllers can be known and, on a risk sensitive basis, reasonable measures should be taken to verify their identity; and
- Gathering information, reasonably warranted by the risk of money laundering or *terrorist financing* on the intended purpose and nature of the *business relationship*.

5.1.6 When determining the degree of *CDD* to apply, the *firm* must adopt a risk based approach, taking into account the type of *client*, *business relationship*, product or *transaction*, and ensuring that the appropriate emphasis is given to those areas that pose a higher level of risk (see Section 4 of this guidance). For this reason it is important that risks are assessed at the outset of a *business relationship* so that a proportionate degree of *CDD* can be brought to bear.

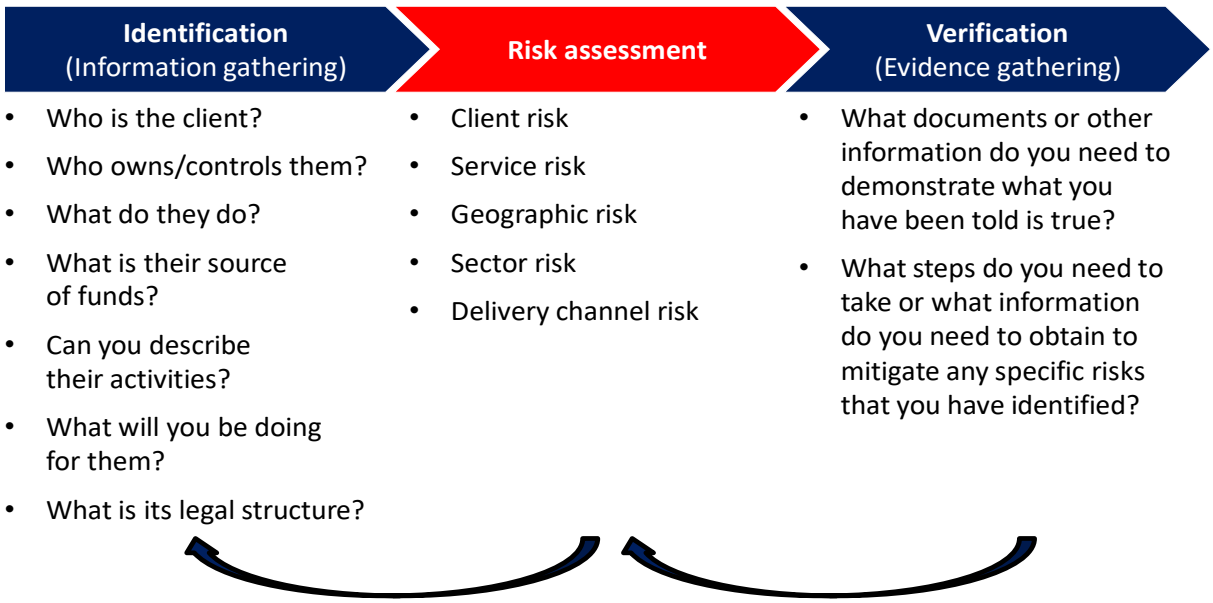
5.1.7 Where the work to be performed falls within the scope of *defined services*, the *firm* must ensure that *CDD* is applied to new and existing *clients* alike. For existing *clients*, *CDD* information gathered previously should be reviewed and updated where it is necessary, timely and risk-appropriate to do so.

5.1.8 The *2010 Act* stipulates that *CDD* must also be performed where there is either a suspicion of *MLTF*, or any doubts about the reliability of the identity information, or documents obtained previously for verification purposes.

5.1.9 Where there is such knowledge or suspicion the *firm* needs to consider not only whether the existing *CDD* information is sufficient and up-to-date, but also whether an external *STR* should be made to *FIU Ireland* and the Revenue Commissioners.

5.1.10 While the *2010 Act* prescribes the level of *CDD* that should be applied in certain situations (i.e. simplified or enhanced – for more on this see section 5.3 of this guidance), it does not describe how to do this on a risk-sensitive basis. Nonetheless, a *firm* is expected to be able to demonstrate to the relevant *competent authority* that the measures it applied were appropriate in accordance with its own risk assessment. Section 4 of this guidance outlines broadly the key areas to be considered when developing a risk based approach including (amongst other factors) the purpose, regularity and duration of the *business relationship*.

Stages of CDD



5.1.11 The arrows in the diagram above represent feedback loops by which an initial risk assessment or verification may highlight a need for more information to be gathered or a fresh risk assessment performed.

5.1.12 The identification phase requires the gathering of information about a *client's* identity and the purpose of the intended *business relationship* before entering into a *business relationship*. This applies to single *transactions* or a series of linked *transactions* valued in excess of €15,000. Appropriate identification information for an individual would include full name, date of birth and residential address. This can be collected from a range of sources, including the client correspondence file. In the case of corporates and other organisations, identification also extends to establishing the identity of anyone who ultimately owns or controls the *client*. These people are the Beneficial Owners, and further detail on how to deal with them can be found in 5.1.16 onwards of this guidance. *A* designated person shall also verify any person purporting to act on behalf of a customer and verify the identity of that person.

5.1.13 The next stage of *CDD* is risk assessment. This should be performed in accordance with the risk based approach guidance contained in Section four of this guidance, and must reflect the purpose, regularity and duration of the *business relationship,* as well as the size of *transactions* to be undertaken by the *client* and the *firm's* own risk assessment. An initial risk assessment is based on the information gathered during stage one (identification), but this may prompt the gathering of additional information as indicated by the left-hand feedback loop. The right-hand feedback loop shows that additional risk assessment may be required in the light of stage three (verification).

5.1.14 Once an initial risk assessment has been carried out, evidence is required to verify the identity information gathered during the first stage. This is called *client* verification. Verification involves validating (with an independent, authoritative source), that the identity is genuine and belongs to the claimed individual or entity. For an individual, verification may require sight of a passport (with a photocopy taken). For corporates and others, in addition to the *client* itself, reasonable verification measures for any individual beneficial owners must also be considered on a risk sensitive basis.

5.1.15 Further guidance on the type of information that should be gathered and the documents that can be used to verify it, can be found in paragraph 5.3.34 onwards.

Beneficial ownership

Definition

5.1.16 A beneficial owner can only be a natural person i.e., an individual (other than in the case of a trust, see below).

5.1.17 Sections 26 through 30 set out in some detail the meaning of beneficial owner in terms of bodies corporate, partnerships, trusts, estates of deceased persons and a catch all provision that, where not otherwise specified, defines the beneficial owner as the person who ultimately owns or

controls the *client* or on whose behalf a service or *transaction* is being conducted. The table below gives a summary of how beneficial ownership could be established for a variety of entities:

***Client* type**	**Voting Rights**	**Shares**	**Capital or profits**	**Other means of ownership/control**
Companies whose securities are listed on a *EEA* regulated investment market or equivalent				No requirement to establish beneficial ownership
Bodies corporate	>25%	>25%		Any individual who ultimately owns or controls whether through direct or indirect ownership or control (including through bearer shareholdings) more than 25% of the shares or voting rights in the body, or who otherwise exercises control over the management of the body
Partnerships	entitled to or controls >25%		entitled to or controls >25%	Any individual who ultimately is entitled to or controls (whether entitlement or control is direct or indirect), more than 25% of the capital or profits of the partnership or more than 25% of the voting rights in the partnership, or who otherwise exercises control over the management of the partnership
Trusts				The beneficiaries (or where some/all have not yet been determined, the class of persons in whose main interest the trust is set up or operates) The settlor , the trustee, the protector Any other individual who has control over the trust (e.g., a protector or trust controller)
Other legal entities				Any individual who benefits from the property of the entity Where no individual beneficiaries are identified, the class of persons in whose main interest the entity or arrangement was set up or operates; Any individual who exercises control over the entity/ arrangement
Estates of deceased individuals				The executor or administrator of the estate
All other cases Where all possible means of identifying the beneficial owner of a body corporate have been				The individual who ultimately owns or controls the *client*, or on whose behalf a *transaction* is being conducted, the senior individual responsible for management (noting the reasons why the business was unable to obtain adequate information on

Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
exhausted and recorded				the beneficial owner, and considering whether it may be appropriate to cease acting, or file a *STR*).

5.1.18 *Accountancy firms*, in accordance with their legal obligations, need to be diligent in their enquiries about beneficial ownership, taking into account that the information they need may not always be readily available from public sources. A flexible approach to information gathering will be needed as it will often involve direct enquiries with *clients* and their advisers as well as searches of public records in Ireland and overseas. There may be situations in which someone is considered to be the beneficial owner by virtue of control even though their ownership share is less than 25%.

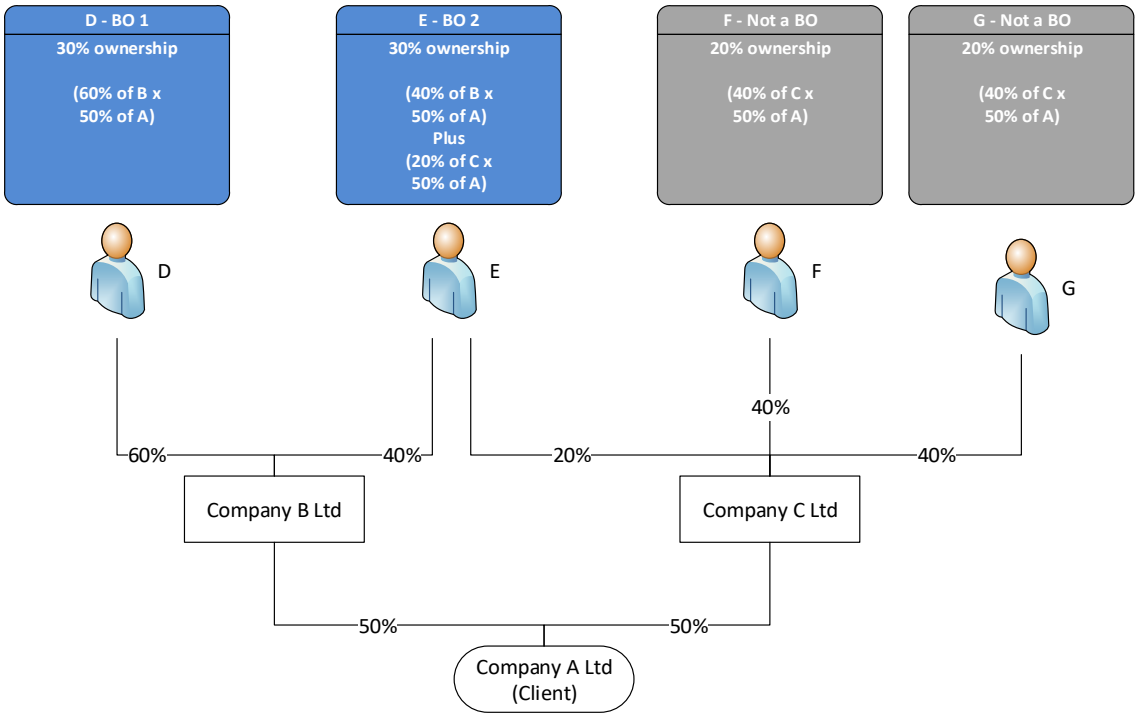
5.1.19 Some possible options of verifying the identity of beneficial owners include:

- Requesting from the customer documentary evidence from an independent source detailing the beneficial owners;
- Searches of the relevant company registry;
- Electronic searches either direct or via a commercial agency for electronic agency for electronic verification;
- The beneficial ownership register maintained by the company.

Determining beneficial owners) in respect of complex structures

5.1.20 In many situations determining beneficial ownership is a straightforward matter. Cases in which the *client* is part of a complex structure will need to be looked at more closely. The diagrams below illustrate types of structures, including indirect ownership and aggregation, which should be taken into account when determining beneficial ownership.

EXAMPLE 1



The *client* is Company A Ltd, a private company. Unless persons F or G exercise the relevant control through other means (such as through 25% voting rights or other means of control) and based on a 25% ownership threshold, the beneficial owners are person D and person E.

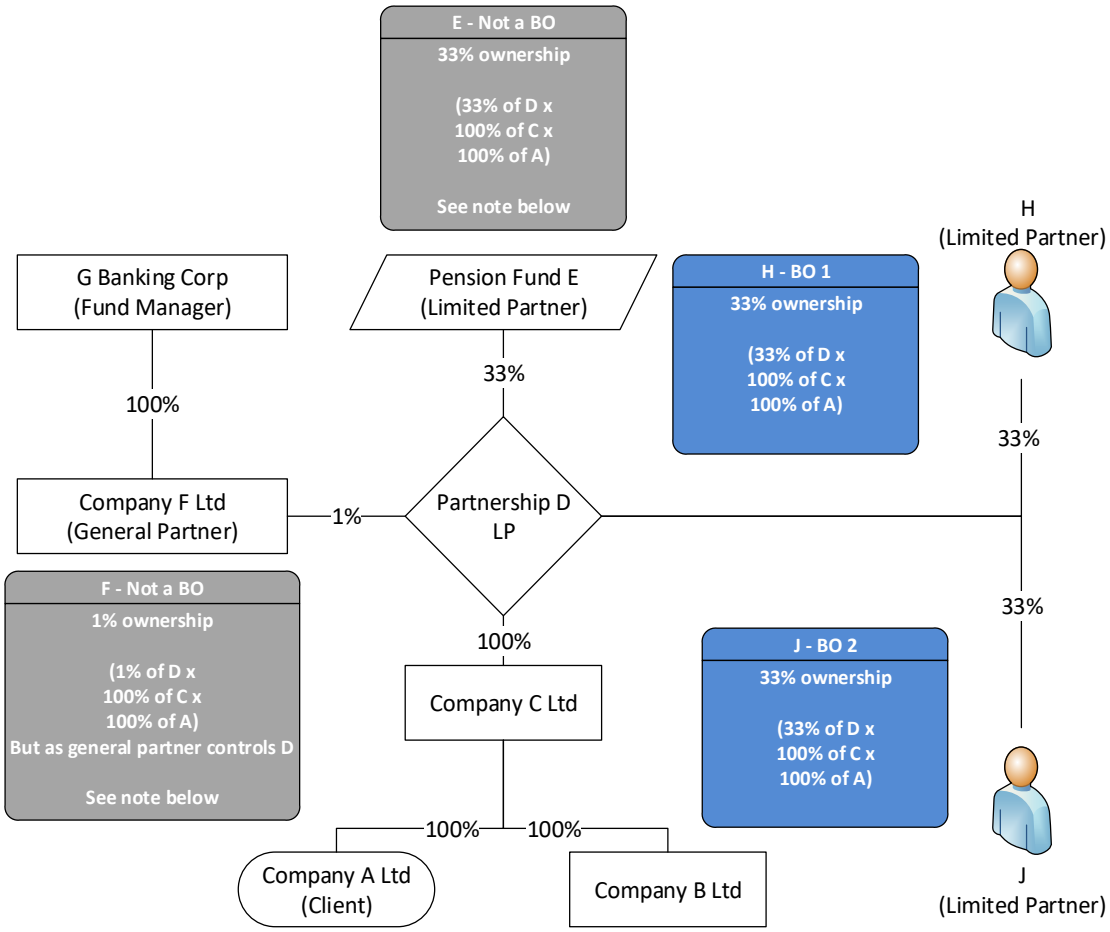
In determining the beneficial owner position, we would need to understand the ownership of Companies B & C (also private companies), but they themselves do not meet the definition of a BO as they are not natural persons.

Person D: is a beneficial owner due to their indirect shareholding of 30% via Company B.

Person E: is a beneficial owner due to their indirect shareholding of 30% via Company B and C.

Persons F & G are not beneficial owners as they only own 20% each via Company C.

EXAMPLE 2



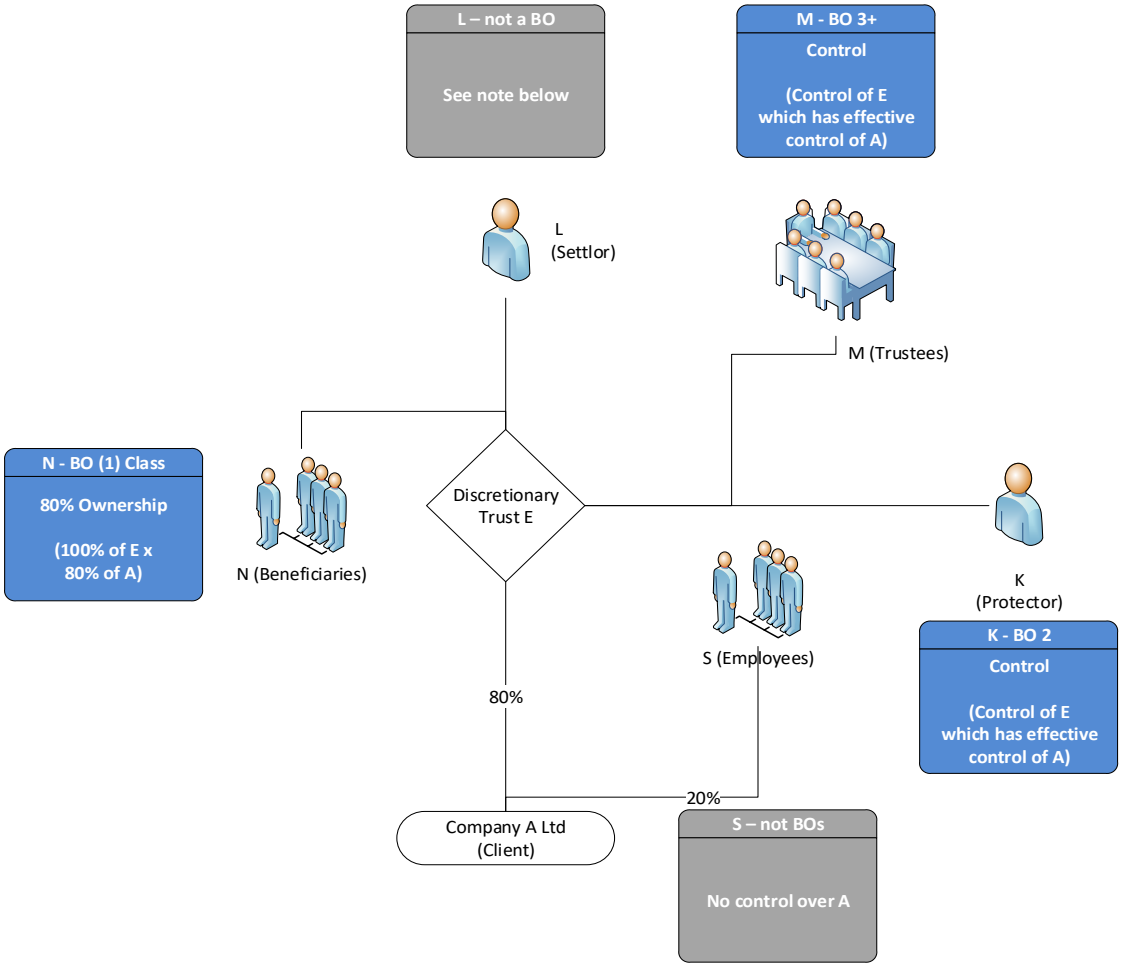
The *client* is Company A Ltd, a private company. Unless E or F control through other means (such as through 25% voting rights or other means of control) and based on a 25% threshold, the beneficial owners are person H and person J.

In determining the beneficial owner position, we would need to understand the structure of Company C, Partnership D, Pension Fund E, Company F and G Banking Corp but they themselves do not meet the definition of a beneficial owner as they are not natural persons.

Persons H & J: are beneficial owners based on a 25% threshold due to their indirect shareholding of 33% each via Partnership D.

Whilst not beneficial owners in their own right, Pension Fund E and Company F present avenues of ownership and control which should be considered further. Pension Fund E has a 33% ownership interest in Company A. Company F, as General Partner, controls the operations of Partnership D (which owns 100% of Company A). Company F is ultimately owned by G Banking Corp. In some situations, if risk is low, pension schemes and banks may qualify for Simplified Due Diligence (SDD), in which case consideration will stop at the point that we can confirm they are eligible for such treatment. Depending on the risk assessment we may need to further investigate the ownership and control structure to ensure there are no further beneficial owners.

EXAMPLE 3



The *client* (Company A Ltd) is a body corporate, therefore:

- Its beneficial owners are the natural persons who: (a) is entitled to a *vested interest* in possession, remainder or reversion, whether or not the interest is defeasible; (b) in the case of a trust other than one that is set up or operates entirely for the benefit of individuals referred to in paragraph (a), the class of individuals in whose main interest the trust is set up or; (c) any individual who has control over the trust; or (d) the settlor; (e) the trustee; (f) the protector.
- There is no need to use the beneficial owner rules related to other types of *client*, such as trusts.

In our case, all of the shares in Company A have equal voting rights. 80% of them are owned by Discretionary Trust E, which allows Discretionary trust E to control the activities of Company A. The remaining shares are owned by employees of Company A, none of whom have any connection to anyone else in the ownership and control structure.

Discretionary trust E is not a natural person, so it cannot be a beneficial owner.

The activities of Discretionary trust E are controlled by its trustees (M). Thus, each trustee is a beneficial owner of Company A.

In our case the trust's protector (K) acts as a check on the powers of the trustees and is also responsible for appointing new trustees. They are therefore regarded as having significant influence and control over E. Protector K is a beneficial owner of Company A.

In our case the settlor (L) has no involvement following settlement of assets into the trust, nor do they exercise significant influence or control over the trustees or the protector. L has no other connection to A. L is not a beneficial owner of Company A, since they will not be exercising significant influence or control over E.

The employee-shareholders do not have enough votes, acting either individually or together, to control Company A, none of them is a beneficial owner of Company A.

Although the trustees and the protector must act in the interest of the beneficiaries, they (N) have no authority over the trustees or protector. Thus, the beneficiaries will not be beneficial owners of Company A, unless they exercise significant influence or control over E or A.

Notes:

- There may be situations where it is appropriate to know the identity of person L, for example to understand the source of Company A's capital. The *MLRO* should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- There may be situations where it is appropriate to identify the class of beneficiaries of trust E or even individuals receiving distributions from the trust, for example where distributions from Company A appear excessive it may be appropriate to establish that the beneficiary or beneficiaries require substantial funds. This may occur where a beneficiary is paying for a wedding or for large medical bills. The *MLRO* should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- If the trust E becomes a *client*, the settlor and the class of beneficiaries will need to be identified, in line with the rules for a discretionary trust.

5.2 When should *CDD* be carried out?

When establishing a business relationship

5.2.1 *CDD* should normally be completed before entering into a *business relationship* or undertaking an *occasional transaction*. For guidance on the situation when *CDD* cannot be performed before the commencement of a *business relationship*, see 5.4 of this guidance.

5.2.2 A *business relationship* is defined by Section 24 of the *2010 Act* as:

'in relation to a *designated person* and a customer of the person, means a business, professional or commercial relationship between the person and the customer that the person expects to be ongoing.'

Thus generic advice, provided with no expectation of any *client* follow-up or continuing relationship (such as generic reports provided free of charge or available for purchase by anyone), is unlikely to constitute a *business relationship*, although may potentially be an *occasional transaction*.

5.2.3 Under Section 24 of the *2010 Act*, for a *transaction* to be 'occasional' it must occur outside of a *business relationship* and have a value more than €10,000. Such a thing is not common in *accountancy services*, but should it occur then the *firm* must,

(a) understand why the *client* requires the service,

(b) consider any other parties involved, and

(c) establish whether or not there is any potential for *MLTF*. If the *client* returns for another *transaction* the *firm* should consider whether this establishes an ongoing relationship.

5.2.4 In addition, section 33A of the *2010 Act* provides for an *electronic money* derogation, provided certain criteria are met (including that the payment instrument concerned is not reloadable and has a maximum monthly payment *transaction* limit not exceeding €250).

5.2.5 *CDD* procedures must also be carried out at certain other times, such as when there is a suspicion of *MLTF*, or where there are doubts about the available identity information, perhaps following a change in ownership/control or through the participation of a *PEP* (see section 5.3.11 of this guidance).

Ongoing monitoring of the client relationship

5.2.6 Established *business relationships* should be subject to *CDD* procedures throughout their duration. This ongoing *monitoring* involves the scrutiny of *client* activities (including enquiries into sources of funds if necessary) to make sure they are consistent with the *firm's* knowledge and understanding of the *client* and its operations, and the associated risks.

Event-driven reviews

5.2.7 *Accountancy firms* need to make sure that documentation, data and information obtained for *CDD* purposes is kept up-to-date. Events prompting a *CDD* information update must include:

- a change in the *client's* identity
- a change in beneficial ownership of the *client*
- a change in the service provided to the *client*
- information that is inconsistent with the *firm's* knowledge of the *client*

An event driven review may also be triggered by:

- the start of a new engagement;
- planning for recurring engagements;
- a previously stalled engagement restarting;
- a significant change to key office holders;
- the participation of a *PEP* (see section 5.3.12 of this guidance)
- a significant change in the *client's* business activity (this would include new operations in new countries); and

- there is knowledge, suspicion or cause for concern (for example where you doubt the veracity of information provided). If a *STR* has been made, care must also be taken to avoid making any disclosures which could constitute *tipping off*.

Periodic reviews

5.2.8 *Accountancy firms* should use routine periodic reviews to update their *CDD*. The frequency of up-dating should be risk based, making use of the *firm's* risk assessment covered in Section 4 of this guidance, and reflecting the *firm's* knowledge of the *client* and any changes in its circumstances or the services it requires.

Ongoing procedures

5.2.9 The *CDD* procedures required for either event-driven or periodic reviews may not be the same as when first establishing a new *business relationship*. Given how much existing information could already be held, ongoing *CDD* may require the collection of less new information than was required at the very outset.

5.3 How should *CDD* be applied?

Applying CDD by taking a risk based approach

5.3.1 Sections 33 and 35 of the *2010 Act* require *customer due diligence* measures to be carried out on a risk-sensitive basis. This means that *accountancy firms* need to consider how their risk assessment and management procedures (see Section 4 of this guidance) flow through into their *client* acceptance and ID procedures, to give sufficient information and evidence, in the way most appropriate to the business concerned. In addition, there are certain circumstances where Sections 33 through 39 of the *2010 Act* lay down categories where simplified due diligence or *enhanced due diligence* is appropriate, according to national and international assessments of the risk of money laundering. A non-exhaustive list of risk factors can be found in APPENDIX D.

5.3.2 For information on client verification documents for the more frequently encountered entity types see APPENDIX B.

Simplified due diligence (SDD)

5.3.3 'Simplified due diligence', whilst not being explicitly referred to as such in the *2010 Act*, is covered in Sections 34 and 36 of the *2010 Act*. It is a phrase which means that an *accountancy firm* is not required to apply the *customer due diligence* measures laid out in Sections 33 (both in relation to a customer and to beneficial owners) and 35 of the *2010 Act*, where the accountancy firm has reasonable grounds for believing that *client* falls into the relevant categories.

5.3.4 *Accountancy firms* who may be permitted to apply the simplified due diligence exemptions but who perceive other than a low risk of money laundering in a specific case, should consider applying their standard or *enhanced due diligence* processes. In any case, where a *client* or potential *client* has been subject to simplified due diligence and a suspicion or money laundering or *terrorist financing* arises in relation to that *client*, the simplified due diligence provisions may no longer be applicable and the *customer due diligence* requirements of Sections 33 and 35 of the *2010 Act* may need to be applied, subject to any issues regarding the potential to prejudice an investigation through a prohibited disclosure under Section 49.

5.3.5 The *firm's* internal procedures should set out clearly what constitutes reasonable grounds for a *client* to qualify for SDD and must take into account at least the risk factors in APPENDIX D (taken from Schedule 3 of the *2010 Act*) and relevant information made available by its *competent authority*. Where a firm applies CDD measures, it shall:

(a) keep a record of the reasons for its determination and the evidence on which it was based, and

(b) carry out sufficient *monitoring* of the *transactions* and *business relationships* to enable the firm to detect unusual or suspicious *transactions*.

5.3.6 In any case, when a *client* or potential *client* has been subjected to SDD, and a suspicion of *MLTF* arises nonetheless, the SDD provisions must be set aside and the appropriate due diligence procedures applied instead (with due regard given to any risk of *tipping off*).

Enhanced due diligence (EDD)

5.3.7 A risk based approach to *CDD* will identify situations in which there is a higher risk of *MLTF*. Section 38A of the *2010 Act* specifies that 'enhanced' due diligence must be applied to manage and mitigate the risk of money laundering and *terrorist financing*....when dealing with a customer established or residing in a *high-risk third country*.

5.3.8 Examples of scenarios requiring the application of *enhanced due diligence* might include:

- where there is a high risk of *MLTF*;
- in any *occasional transaction* or *business relationship* with a person established in a *high-risk third country*;
- if a *firm* has determined that a *client* or potential *client* is a *PEP*, or *an immediate family member* or *close associate* of a *PEP;*
- in any case where a *client* has provided false or stolen identification documentation or information on establishing a *business relationship*;
- in any case where a *transaction* is complex and unusually large, there is an unusual pattern of *transactions* which have no apparent economic or legal purpose;
- in any other case which by its nature can present a higher risk of *MLTF.*

5.3.9 The *firm's* internal procedures should set out clearly what constitutes reasonable grounds for a *client* to qualify for EDD and must take into account at least the high risk factors in APPENDIX D (taken from Schedule 4 of the *2010 Act*).

5.3.10 EDD procedures must include:

- as far as reasonably possible, examining the background and purpose of the engagement; and
- Increasing the degree and nature of *monitoring* of the *business relationship* in which the *transaction* is made to determine whether that *transaction* or that relationship appear to be suspicious.

5.3.11 EDD measures may also include one or more of the following measures:

- seeking additional independent, reliable sources to verify information, including identity information, provided to the *firm*;
- taking additional measures to understand better the background, ownership and financial situation of the *client*, and other parties relevant to the engagement concerned;
- taking further steps to be satisfied that the *transaction* is consistent with the purpose and intended nature of the *business relationship*;
- Increasing the *monitoring* of the *business relationship*, including greater scrutiny of *transactions*.

Politically exposed person (PEP)

5.3.12 As set out above, section 37 of the *2010 Act* specifies that *PEPs* (as well as certain *immediate family members* and *close associates*) must undergo EDD. The nature, and extent of, such EDD measures will need to vary depending on the extent of any heightened *MLTF* risk associated with individual *PEPs* (including domestics *PEPs*). *Accountancy firms* must treat *PEPs* on a case-by-case basis, and apply EDD on the basis of their assessment of the *MLTF* risk associated with any individual *PEPs*.

5.3.13 Section 37 defines a *PEP* as an individual '…who is or has, at any time in the preceding 12 months, been entrusted with a prominent public function', including either a "specified official" or a member of the administrative, management or supervisory body of a state-owned enterprise or an *immediate family member* or *close associate* of such a person. Specified official is defined as any of the following officials (including any such officials in an institution of the European Communities or an international body):

- a head of state, head of government, government minister or deputy or assistant government minister;
- a member of parliament or of a similar legislative body;

- a member of a supreme court, constitutional court or other high level judicial body whose decisions, other than in exceptional circumstances, are not subject to further appeal;
- a member of a court of auditors or of the board of a central bank;
- an ambassador, charge d'affairs or high ranking officer in the armed forces; or
- a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation.

For risk management and reputational risk reasons, *accountancy firms* may wish to treat as *PEPs* persons who held such positions more than a year ago.

'*Immediate family member*' of a *PEP* includes: parents, spouses and equivalent, children, spouses of children and equivalent, and any other family member of a class prescribed by the Minister (none at the time of publication). '*Close associate*' includes any person who

(i) has joint beneficial ownership of a legal entity or arrangement, or any other close business relations with a *PEP* or

(ii) has sole beneficial ownership of a legal entity or arrangement set up for the actual benefit of a *PEP*.

5.3.14 An individual identified as a *PEP* solely because of their public function must still be treated as a *PEP*. However if the *firm* is not aware of any factors that would place the individual in a higher risk category, the individual may be categorised as a low risk *PEP*. The risk factors guidance produced by the European Supervisory Authorities set out factors that might point to potential higher risk. Such factors might also include, for example:

- known involvement in publicised scandals e.g., regarding expenses;
- undeclared business interests;
- previous prosecution for criminal offences;
- the acceptance of inducements to influence policy.

5.3.15 In lower-risk situations a *firm* should apply less onerous EDD requirements (such as, for example, making fewer enquiries of a *PEP's immediate family members* or *close associates;* and taking less intrusive and less exhaustive steps to establish the sources of wealth/funds of *PEPs*). Conversely, and in higher-risk situations, *firms* should apply more stringent EDD measures. This represents part of the risk based approach that *firm's* should take to *MLTF* compliance, as described more fully elsewhere in this section.

5.3.16 *Accountancy firms* must treat individuals as *PEPs* for at least 12 months after they cease to hold a prominent public function. This requirement does not apply to *immediate family members* or *close associates. Immediate family members* and *close associates* of *PEPs* should be treated as ordinary *clients* (and subject only to *CDD* obligations) from the point that the *PEP* ceases to discharge a prominent public function. *Firms* need only apply EDD measures to *PEPs* for more than 12 months after they have ceased to hold a prominent public function when the *firm* has determined that they present a higher risk of *MLTF*.

5.3.17 An *accountancy firm* is deemed to know or have reasonable grounds to know that a person is a *PEP*, an immediate *family member* of a *PEP* or a *close associate* of a *PEP* on the basis of information in the possession of the *accountancy firm* or in the public domain. The *2010 Act* provides that the definition of immediate *family member* must include the spouses/civil partners of *PEPs*, the children of *PEPs* (and their spouse or civil partner) and the parents of *PEPs*. This is not an exhaustive list – in determining whether other immediate *family members* should be subject to EDD, *accountancy firms* should consider the levels of *MLTF* risk associated with the relevant *PEP*. In lower-risk situations, a *firm* should not apply EDD to additional immediate *family members* other than those contained within the definition set out in the *2010 Act*.

5.3.18 As regards international organisations, the *2010 Act* states that only directors, deputy directors and board members (or equivalent) should be treated as *PEPs*. Middle-ranking and junior officials do not fall within the definition of a *PEP*.

5.3.19 'International organisation' is not defined, and due consideration should be given to the type, reputation and constitution of the body before excluding it or its representatives from *enhanced due diligence*. However, bodies such as the United Nations, NATO and *FATF* may reasonably be included within the definition of an international body for this purpose. The context of the *engagement* and role of the *PEP* in respect of it should also be considered.

5.3.20 *Accountancy firms* are required to have risk sensitive measures in place to recognise *PEPs* (Sections 37(1) to 37(3)). This can be a simple check conducted by enquiring of the *client* and perhaps using an internet search engine. *Accountancy firms* that are likely to regularly undertake services for *PEPs* may need to subscribe to a specialist database. *Firms* that use such databases must understand how they are populated and will need to ensure that those flagged by the database fall within the definition of a *PEP*, *immediate family member* or *close associate* as set out in Section 37 of the *2010 Act*. During the life of a relationship, and to the extent that it is practical, attempts should be made to keep abreast of developments that could transform an existing *client* into a *PEP*.

5.3.21 *Firms* wanting to enter into, or continue, a *business relationship* with a *PEP* must carry out EDD, which includes:

- *senior management* approval for the relationship;
- adequate measures to establish sources of wealth and funds; and
- enhanced *monitoring* of the ongoing relationship.

As set out above, the nature and extent of EDD measures must vary depending on the levels of *MLTF* risk associated with individual *PEPs*.

5.3.22 The Anti Money Laundering Compliance Unit (AMLCU) of the Department of Justice has published guidance on how businesses that it supervises for MLTF purposes should identify and treat *PEPs*. *Accountancy firms* may find this guidance useful in determining the approach that they should take to identifying and applying EDD to *PEPs*.

5.3.23 The preamble to the *EU Directive* (which the *2018 Act* brought into Irish law makes it clear that refusing a *business relationship* with a person solely on the basis that they are a *PEP* is contrary to the spirit and letter of the *EU Directive*, and of the *FATF* standards. *Firms* should instead mitigate and manage any identified *MLTF* risks, and should refuse *business relationships* only when such risk assessments indicate that they cannot effectively mitigate and manage these risks.

Financial sanctions and other prohibited relationships

5.3.24 The *2010 Act* sets out circumstances which constitute prohibited relationships. In Section 59, correspondent banking relationships with *shell banks*, or a bank known to permit use of its accounts by a *shell bank* are prohibited. In addition, Section 58 prohibits the setting up of anonymous accounts, and *customer due diligence* must be applied to any existing accounts continuing in existence after commencement of the *2010 Act* before such an account is used. In addition, *accountancy firms* must comply with any prohibition issued by the Department of Finance in respect of any person, or State to which financial sanctions apply. These are published regularly in Iris Oifiguil.

5.3.25 Financial sanctions can be a complex and changeable area. Detailed discussion of it is beyond the scope of this guidance. *Accountancy firms* should refer to the Department of Finance. *Firms* unsure of their legal obligations should seek legal advice.

Reliance on other parties

5.3.26 Section 40 of the *2010 Act* provides that *accountancy firms* may rely on certain third parties, referred to as 'relevant third parties', to complete all or part of *customer due diligence*, subject to there being an arrangement between the *firm* and the relevant third party. The *firm* proposing to rely on a relevant third party must satisfy themselves that, on the basis of the arrangement in place, the relevant third party will forward any documents or information relating to the *client* in question that has been obtained by the relevant third party in identifying that *client*, as soon as practicable after the *firm* makes the request. *Accountancy firms* should, however, be cautious in relying on third parties as the firm will remain liable for any failure to comply with *customer due diligence* measures notwithstanding their reliance on a third party (Section 40(5)). *Accountancy firms* should consider requiring copies of relevant information and documentation from the third parties, in order that they may satisfy themselves the information is sufficient. 'Relevant third parties' on whom reliance may be placed are:

- *credit* or *financial institutions* (excluding undertakings solely providing foreign exchange or money services)
    - in Ireland; or

- authorised to operate under the laws of another Member State or of a designated place (under Section 31)

- *external accountants*, auditors, *tax advisers* and *relevant independent legal professionals*
  - who are members of a Designated Accountancy Body, the Irish Taxation Institute or the Law Society of Ireland respectively; or
  - who are subject to mandatory professional registration or mandatory professional supervision under the laws of another Member State or in a designated place (under Section 31);

- *trust or company service providers*
  - who are members of a Designated Accountancy Body, or the Law Society of Ireland, or are authorised to carry on business by the Central Bank of Ireland; or
  - who are subject to mandatory professional registration or mandatory professional supervision under the laws of another Member State or in a designated place (under Section 31);

The relevant third parties in the abovementioned 'designated place' under Section 31 must be supervised or monitored in the place for compliance with requirements equivalent to those specified in the Fourth Money Laundering Directive. *Accountancy firms* may outsource their *customer due diligence* measures but remain liable for any failure in the *customer due diligence*.

5.3.27 Outsourcing is permitted only if the other party is required to apply the requirements of the Directive (e.g. a *designated person* in Ireland) or subject, in an *EEA* or non-*EEA* state, to an equivalent regulatory regime which includes compliance supervision requirements equivalent to the *EU Directive.*

5.3.28 *Firms* should note that where one party places reliance on another they should enter into an agreement (that should be in writing) to ensure that the other party will provide the *CDD* documentation as soon as practicable after a request. An arrangement of this kind can be useful and efficient when the two parties are able to build a relationship of trust, but it should not be entered into lightly. Liability for inadequate *CDD* remains with the relying party. *Firms* placing reliance on another should satisfy themselves with the level of *CDD* being undertaken.

Parties seeking reliance

5.3.29 A *firm* relying on a third party in this way is not required to apply standard *CDD*, but it must still carry out a risk assessment and perform ongoing *monitoring*. That means it should still obtain a sufficient quantity and quality of *CDD* information to enable it to meet its *monitoring* obligations.

5.3.30 If relying on a third party, *firms* should obtain from that party copies of all relevant information to satisfy *CDD* requirements. They should also enter into a written arrangement that confirms that the party being relied on will provide copies of identification and verification documentation as soon as practicable after a request.

Parties granting reliance

5.3.31 An *accountancy firm* is not obliged to act as a relevant third party for another *designated person*. *Accountancy firms* agreeing an arrangement to act as a relevant third party in relation to the *customer due diligence* obligations of another *designated person* should take great care to ensure they have adequate systems in place to keep proper records and to respond to any request for these. Where an *accountancy firm* agrees to be part of an arrangement whereby another *designated person* relies on him in meeting their obligations under the *2010 Act* with regard to *customer due diligence* must, if requested, make available to the person relying as soon as is reasonably practicable:

- any information obtained about the *client* (and any beneficial owner) when applying *customer due diligence* measures; and/or;
- copies of any identification and verification data and other documents on the identity of the *client* (and any beneficial owner) obtained when applying *customer due diligence* measures.

Other *designated persons* who rely on an *accountancy firm* to carry out *customer due diligence* measures, as part of an arrangement between both parties, remain ultimately responsible under the *2010 Act* for any failure to apply the measures

Subcontracting

5.3.32 Where a relevant *firm*, A, is engaged by another *firm*, B, to help with work for one of its *clients* or some other underlying party, C, then A should consider whether its *client* is in fact B, not C. For example, where there is no *business relationship* formed, nor is there an engagement letter between A and C, it may be that *CDD* on C is not required but should instead be completed for B.

5.3.33 On the other hand, where there is significant contact with the underlying party, or where a *business relationship* with it is believed to have been established, then C may also be deemed a *client* and *CDD* may be required for both C and B. In this situation, A may wish to take into account information provided by B and the relationship it has with C when determining what *CDD* is required under its risk based approach. It should be noted that the same considerations are relevant in networked arrangements, where work is referred between member firms.

Evidence gathering

5.3.34 The purpose of verification of identity is to confirm and prove the information collected in so far as it relates to the identity of the *client*. Recourse to documents from independent sources is important. The amount of reliance that can be placed upon, and thus the strength of, particular forms of evidence varies. The following are illustrative of a different of strength of various forms of documentary evidence starting with the highest:

- documents issued by a government department or agency or a Court (including documents filed at the Companies Registration Office or overseas equivalent);
- documents issued by other public-sector bodies or local authorities;
- documents issued by *designated persons* regulated by the Central Bank of Ireland or overseas equivalent;
- documents issued by *relevant professional advisers* and *relevant independent legal professionals* regulated for anti-money laundering purposes by the Designated Accountancy Bodies or the Law Society of Ireland and overseas equivalents;
- documents issued by other bodies.

In the case of *clients* who are persons, documents from highly rated sources that contain photo identification as well as written details are a particularly strong source of verification of identity. Consideration should also be given to conducting a general internet search of the company and the directors and beneficial owners.

5.3.35 In higher risk cases *firms* must consider whether they need to take extra steps to increase the depth of their *CDD* knowledge. These might include more extensive internet and media searches covering the *client*, key counterparties, the business sectors and countries and requests for additional identity evidence. Subscription databases can be a quick way to access this kind of public domain information, and they will often reveal links to known associates (companies and individuals) as well.

5.3.36 *Client* verification means to verify on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified. Documents issued or made available by an official body can be regarded as being independent.

5.3.37 It is important that verification procedures are undertaken on a risk-sensitive basis.

Refer to APPENDIX B for a non-exhaustive list of documents that can be used for verification purposes.

Validation of documents

Certification of documents by a third party

5.3.38 *Accountancy firms* may consider it appropriate, in the case of documents originating from or provided by a third party, to request certification as to their accuracy. In such cases, *firms* are advised to have regard to the standing of the person certifying and may wish to consider specifying from whom certification may be accepted. For instance, *firms* may decide to accept those documents certified by a person in the permitted categories for reliance (Section 40) which are broadly a *credit* or *financial institution* authorised by the Central Bank of Ireland, a professionally qualified auditor, *external accountant*, insolvency practitioner or *tax adviser*, or *relevant independent legal professional*, or their equivalent in other Member States or other designated places under Section 31, which have equivalent law and provided in all cases that the person is subject to supervision as to his compliance with those requirements.

Annotation of sources of validation

5.3.39 This should be used when the document is as good as an original but is not the original itself. This particularly applies to printouts from the Internet, such as downloads from the Companies Registration Office, regulator, stock exchange or government websites, or similar trustworthy business information sources. Each document so obtained should bear written evidence showing who printed it, when, from where and should be signed by the relevant person. Where necessary and taking a risk based approach, such documents (whether downloaded or otherwise) should be validated with an authoritative source such as a government agency.

Use of electronic data

5.3.40 There are now a number of subscription services that give access to databases of information on identity. Many of these services can be accessed on-line and are often used by *accountancy firms* to replace or supplement paper verification checks. This means *firms* may use on-line verification as a substitute for paper verification checks for *clients* considered normal risk, supplemented by additional paper verification checks for higher risk *clients*, or vice versa.

5.3.41 Before using electronic databases, however, *firms* should question whether the information supplied is sufficiently reliable, comprehensive and accurate. Consider the following points:

- **Does the system draw on multiple sources?** A single source (e.g., the Electoral Register) is usually not sufficient. A system which uses negative and positive data sources is generally more robust than one that does not.
- **Are the sources checked and reviewed regularly?** Systems that do not regularly update their data regularly are generally prone to more inaccuracies than those that do.
- **Are there control mechanisms to ensure data quality and reliability?** Systems should have built-in data integrity checks which, ideally, are sufficiently transparent to prove their effectiveness.
- **Is the information accessible?** Systems need to allow a *firm* either to download and store the results of searches in appropriate electronic form, or to print off a hardcopy record containing all necessary details as to name of provider, source, date etc.
- **Does the system provide adequate evidence that the *client* is who they claim to be?** Consideration should be given as to whether the evidence provided by the system has been obtained from an official source, e.g., certificate of incorporation from the official company registry.

5.4 What happens if *CDD* cannot be performed?

When delays occur

5.4.1 In forming new *business relationships*, there are some cases where delay **may** be acceptable, such as in urgent insolvency appointments, and urgent appointments that involve ascertaining the legal position of a *client* or defending the *client* in legal proceedings.

5.4.2 In such cases, *accountancy firms* should still gather enough information to allow them to at least form a basic assessment of the identity of the *client* and money laundering risk and to complete other acceptance formalities such as considering the potential for conflicts of interest.

5.4.3 In other cases, where the majority of information required has been collected before entering a *business relationship*, short time extensions to complete collection of remaining information may be acceptable, provided this is caused only by administrative or logistical issues, and not by any reluctance of the *client* to provide the information and is necessary not to interrupt the normal course of business. Such extensions should be exceptional, rather than the norm. It is recommended that such extensions of time are considered and agreed by a member of *senior management* or the *MLRO*, where appointed in accordance with the *firm's* procedures, to ensure the reasons for the extension are valid and do not give rise to concern over the risk category of the *client* or the potential for money laundering suspicion.

5.4.4 Provided that *CDD* is completed as soon as practicable, verification procedures may be completed during the establishment of a *business relationship* if it is necessary not to interrupt the normal course of business and there is little risk of *MLTF*. In some situations it may be necessary to carry out *CDD* while commencing work because it is urgent. Such situations could include:

- some insolvency appointments;
- appointments that involve ascertaining the *client's* legal position or defending them in legal proceedings;
- response to an urgent cyber incident; or
- when it is critically important to preserve or extract data or other assets without delay.

5.4.5 If evidence is delayed (rather than refused), *accountancy firms* should consider;

- the credibility of the *client's* explanation;
- the length of delay;
- whether the delay is in itself reasonable grounds for suspicion of a *money laundering* offence requiring a report to *FIU Ireland* and the Revenue Commissioners and/or a factor indicating against acceptance of the *client* and engagement; and
- documenting the reasons for delay and steps taken.

5.4.6 No client engagement (including transfers of *client* money or assets) should be completed until *CDD* has been completed in accordance with the *firm's* own procedures.

Cessation of work and suspicious transactions reporting

5.4.7 If a prospective *client* refuses to provide evidence of identity or other information properly requested as part of *customer due diligence*, the *business relationship* should be discontinued and/or the *transaction*/series of linked *transactions* amounting to in excess of €15,000 sought by the *client* must not be provided, for so long as the failure continues (but see paragraphs 5.4.10 to 5.4.12 below regarding particular circumstances affecting insolvency cases). Consideration must be given as to whether a report needs to be made to *FIU Ireland* and the Revenue Commissioners, in accordance with Section 42(4).

5.4.8 Where the appointment is of either a lawyer or *relevant professional advisor* in the course of ascertaining the legal position for the *client*, or performing the task of defending or representing the *client* in or concerning legal proceedings (including advice on instigating or avoiding proceedings) the requirement to cease acting and consider reporting to the FIU Ireland and the Revenue Commissioners does not apply although *customer due diligence* information will still need to be collected within the time constraints in Sections 33 and 35 of the *2010 Act*. *Accountancy firms* are advised to consider the position very carefully before applying this exception to ensure that the type of work and their professional status fall within the definition of *relevant professional adviser* set out in Section 24 of the *2010 Act*.

Insolvency cases

5.4.9 An insolvency practitioner should obtain verification of the identity of the person or entity over which he is appointed. Acceptable evidence of verification may include a court order, a court endorsed appointment, or an appointment made by a debenture holder or creditors meeting supported by a company search or similar. It is not always possible or necessary to obtain identification evidence direct from persons or individual shareholders or directors in an appointment in respect of a company as their co-operation may not be forthcoming.

5.4.10 It is important for an officeholder to be sure about the identity of the person or entity over which he is taking appointment given the urgency of the situation and the necessity not to delay when this might risk dissipation of assets and erosion of value. Initial contact with the company would include, for example accepting instructions from directors to take steps to place a company into liquidation or to accept appointment as independent expert under section 504 of the Companies Act 2014. . However, completion of other elements of customer due diligence may not be possible prior to appointment and should be completed as soon as practicable after appointment (if possible, usually within 5 working days).

5.4.11 Insolvency practitioners post appointment have a very different relationship with the insolvent client than that with an audit or advisory client and have access to a very wide range of information which alters the need for traditional pre-appointment CDD. However, particular focus is needed before, and immediately after, appointment on considering the way the business has been operated and assessing the risk of assets being tainted by crime. In such cases it may well be necessary, but not as a matter of routine in every case, to make an external report prior to performing the normal range of duties of collection, realisation and distribution of assets.

5.4.12 Where the insolvency practitioner is appointed by Court order without any prior involvement with the insolvent company, reliance on the order of appointment or winding-up order is considered to be sufficient evidence of identity. This would apply in the following cases:

• Appointment as provisional liquidator by order of the Court;

• Appointment as liquidator in a winding up by the Court (including by order following an examination); or

• Appointment as examiner by order of the Court.

An insolvency practitioner appointed to a company which is itself a *designated person* under the *2010 Act*, and becoming responsible for the company's operation, will need to be satisfied that the company has appropriate procedures in place to ensure its compliance with the requirements of the *2010 Act* and that the procedures continue to function during the term of the his appointment.

6 SUSPICIOUS TRANSACTION REPORTING (*STR*)

- What must be reported?
- Offences
- When and how should a report be made?
- Reporting and the privileged circumstances exception?
- Determining whether to proceed with or withdraw from a *transaction* or service
- Requests for further information
- What should happen after an external *STR* has been made?

6.1 What must be reported?

The reporting regime

6.1.1 The obligation to make a Suspicious Transaction Report (*STR*) is set out in section 42 of the *2010 Act* and arises when:

- an *accountancy firm* or an *individual* connected with the firm knows or suspects, or has reasonable grounds to suspect, that another person has been, or is, engaged in money laundering or *terrorist financing (*see below*);*
- the information on which the above is based came to the *firm* or the *individual* in the course of carrying on the business of an *accountancy firm* or accountant;
- the *firm* or *individual* has scrutinised the information in the course of reasonable business practice.

Money laundering

6.1.2 Section 2 of the guidance defines the *money laundering offences* (see paragraph 2.2.1). A person commits a *money laundering offence* if he, knowing or believing that property is or 'probably comprises' the *proceeds of criminal conduct* or being reckless as to whether the property is or 'probably comprises' such proceeds, engages in any of the following acts in relation to the property:

- concealing or disguising the true nature, source, location, disposition, movement or ownership or the property, or any rights relating to the property;
- converting, transferring, handling, acquiring, possessing or using the property;
- removing the property from, or bringing the property into, the State.

6.1.3 Money laundering can be carried out in respect of the proceeds of both conduct that is an offence in Ireland and, in certain circumstances, conduct occurring elsewhere. These circumstances are set out in section 8 of the *2010 Act* and include actions by an Irish citizen in another jurisdiction or that take place on an Irish ship or an aircraft registered in Ireland.

6.1.4 For a matter to be money laundering, there must not only be *criminal conduct*, but also *proceeds of criminal conduct*.

Terrorist financing

6.1.5 '*Terrorist financing'* means an offence under Section 13 of the Criminal Justice (Terrorist Offences) Act 2005 and involves the provision, collection or receipt of funds with the intent or knowledge they will be used to carry out an act of terrorism or any act intended to cause death or serious injury.

6.1.6 The offence is committed by any person, in or outside the State, who directly or indirectly, unlawfully and wilfully, provides, collects or receives funds intending that they will be used or knowing that they will be used to carry out an act of terrorism. Terrorism is taken to be the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

6.1.7 **Materiality or 'de minimis' exceptions do not exist in relation to either *money laundering* or *terrorist financing* offences**

6.1.8 In relation to reporting obligations, references to *accountancy firms* are to be read as including references to a director or other officer, employee or (in the case of a partnership) principal of the *accountancy firm*. Section 41 also captures agents of the *accountancy firm* or other persons 'engaged under a contract for services' within the definition of *designated persons* for the purposes of the reporting obligation.

6.1.9 Disclosure is ordinarily made internally to the *MLRO* or other nominated person in accordance with procedures established by the *accountancy firm* in accordance with s54(3)(g) or, if appropriate in the circumstances, may be made directly to *FIU Ireland* and the Revenue Commissioners.

6.1.10 The procedures implemented by the *accountancy firm* should also provide a mechanism to ensure that the *STR* to *FIU Ireland* and Revenue Commissioners is made where there is knowledge, suspicion or reasonable grounds to suspect money laundering or *terrorist financing* as a consequence of the *internal report*.

6.1.11 The key elements required for a *STR* (knowledge, suspicion, crime, proceeds) are set out below.

Knowledge and Suspicion

6.1.12 An *accountancy firm* or *individual* is required to make an *STR* where that *firm* or *individual* has knowledge, suspicion or reasonable grounds for suspicion of money laundering or *terrorist financing* arising from the *firm's/individual's* normal course of business.

6.1.13 Having knowledge means actually knowing that something is the case. There is very little guidance on what constitutes 'suspicion' so the concept remains subjective. Some pointers can be found in case law, where the following observations have been made. Suspicion is:

- a state of mind more definite than speculation but falling short of evidence-based knowledge;
- a positive feeling of actual apprehension or mistrust;
- an opinion, based on indicative but not conclusive evidence.

Suspicion is not

- a mere idle wondering;
- a vague feeling of unease.

6.1.14 An *STR* must be made where there is knowledge or suspicion of money laundering *terrorist financing*, but there is no requirement to make speculative *STRs*. If, for example, a suspicion is formed that someone has failed to declare all of their income for the last tax year, to assume that they had done the same thing in previous years would be speculation in the absence of specific supporting information. Similarly, the purchase of a brand new Ferrari by a *client's* financial controller is not, in itself, a suspicious *transaction*. However, inconsistencies in accounts for which the financial controller is responsible could raise speculation to the level of suspicion.

6.1.15 An *STR* is also required when there are 'reasonable grounds' to suspect money laundering or *terrorist financing (*section *42(3) of the 2010 Act)*. While suspicion is, by its nature, subjective, the term "reasonable grounds to suspect" is an objective test i.e., the standard of behaviour expected of a reasonable person in the same position. Claims of ignorance or naivety are no defence.

6.1.16 'Reasonable grounds' should not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. For example, cash-based businesses or complex overseas trust and company structures may be capable of being used to launder money, but this capability of itself is not considered to constitute ''reasonable grounds'.

6.1.17 Existence of higher than normal risk factors require increased attention to gathering and evaluation of *CDD* information, and heightened awareness of the risk of money laundering in performing professional work, but do not of themselves require a report of suspicion to be made. For 'reasonable grounds' to come into existence, there needs to be sufficient information to advance beyond speculation that it is merely possible someone is laundering money, or a higher than normal incidence of some types of crime in particular sectors.

6.1.18 It is important for *individuals* to make enquiries that would reasonably be expected of someone with their qualifications, experience and expertise, and such enquiries fall within the normal scope of the engagement or *business relationship*. In other words, they should exercise a healthy level of professional scepticism and judgement and, if unsure about what to do, consult their

MLRO or other nominated officer (or similar) in accordance with the *firm's* own procedures. If in doubt, it is advisable to err on the side of caution and report to the *MLRO*.

6.1.19 The information or knowledge that gave rise to the suspicions must have come to the *individual* in the course of business a as *designated person* (section 42 of the *2010 Act*). .

Crime and proceeds

6.1.20 *Criminal conduct* is behaviour which constitutes an offence in Ireland or, in certain circumstances, occurring elsewhere (see Section 2 above). *Criminal conduct* is defined under Section 6 in terms of the commission of "an offence". This definition captures not only criminal offences, but all other offences which result in proceeds. As such, *criminal conduct* is defined very broadly. It goes beyond the common understanding of money laundering, being the conversion and concealment of funds derived from illegal activity, to incorporate the mere possession, acquisition or use of the illicit proceeds. Any offence, therefore, whether indictable or otherwise, which results in proceeds, represents a *money laundering offence* and falls to be reported under the legislation.

6.1.21 Since Irish law defines *money laundering offences* so widely, any *criminal conduct* which has resulted in any form of *proceeds of criminal conduct* will also constitute *money laundering*. It is not expected that *individuals* will become expert in the very wide range of underlying or predicate criminal offences which lead to *money laundering* but they will be expected to recognise those that fall within the professional competence of their role and should use professional scepticism, judgement and independence as appropriate to identify offences.

6.1.22 The *2010 Act*'s definition of *money laundering offences* (section 2 of the Act) requires that an offender must know or suspect, or be reckless as to whether or not, that property is the *proceeds of criminal conduct*. An innocent error or mistake would not normally give rise to criminal proceeds (unless a strict liability offence).

6.1.23 If an *accountancy firm* or *individual* knows or believes that a *client* is acting in error, the *individual* may approach the *client* and explain the situation and legal risks to him. However, once the criminality of the conduct is explained to the *client*, that *client* must bring the conduct (including past conduct) promptly within the law to avoid a *money laundering offence* being committed. Where there is uncertainty about the legal issues, outside the competence of the *accountancy firm, clients* should be referred to an appropriate specialist or professional legal adviser.

6.1.24 As noted above, the reporting obligations arise where offences are committed which give rise to proceeds. These *predicate offences* may be under any legislation – for example, including inducements offered in contravention of the Criminal Justice (Corruption Offences) Act 2018. *Accountancy firms* are most likely to encounter possible offences under the Companies Acts, the Criminal Justice (Theft and Fraud Offences) Act 2001 and tax legislation. However, they should be aware that if they receive information during the normal course of their work which gives rise to knowledge, suspicion or reasonable grounds for suspicion that an offence has been, or is being, committed under other legislation, they have a reporting obligation in such circumstances (except where the *professional privilege reporting exemption* applies – see section 6.4 below). *CCAB-I* / professional guidance has been issued dealing with indictable offences under the Companies Acts which are reportable to the Office of the Director of Corporate Enforcement, and reporting of theft and fraud offences, which at date of issue are as follows:

- Technical Release 04/2015 – Companies Act 2014 A *statutory auditor's* duty to report to the Director of Corporate Enforcement;
- Technical Release 03/2016 – Companies Act 2014 Reporting Company Law Offences: Information for *Statutory Auditors*;
- *CCAB-I* memo – Section 59 Criminal Justice (Theft and Fraud Offences) Act 2001;
- Information Sheet 01/2013 – Criminal Justice Act 2011, Reporting implications for Members in Practice and in Business.

6.1.25 In most cases of suspicious *transactions* the reporter will have a particular type of *criminal conduct* in mind, but this is not always the case. Some *transactions* or activities so lack a commercial rationale or business purpose that they give rise to a general suspicion of *MLTF*. As noted in paragraph 6.1.21, Irish law defines money laundering widely: *individuals* are not required to become experts in the wide range of criminal offences that lead to money laundering, but they are expected to recognise any that fall within the scope of their work. Exercise professional scepticism and judgement at all times.

Proceeds

6.1.26 *Proceeds of criminal conduct* means any property that is derived from or obtained through *criminal conduct*, directly or indirectly, in whole or in part. Criminal proceeds can take many forms. Cost savings (as a result of tax evasion or ignoring legal requirements) and other less obvious benefits can be proceeds of crime. Where criminal property is used to acquire more assets, these too become criminal property. It is important to note that there is no question of a de minimis value.

6.1.27 If someone knowingly engages in criminal activity with no benefit, then they may have committed some offence other than money laundering (it will often be fraud) and there is no obligation to make an *STR*. However, the duty to report under other legislation (including company law and the Criminal Justice (Theft and Fraud Offences) Act 2001) should be assessed and where appropriate a report made as required by that legislation.

6.1.28 Examples of unlawful behaviour which may be observed, and may well result in advice to a *client* to correct an issue, but which are not reportable as *money laundering offences* are given below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *accountancy firms* and *individuals* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position.
- misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due.
- attempted frauds where the attempt has failed and so no benefit has accrued (although this may still be reportable under other legislation.

A checklist for the *STR* reporting process can be found in APPENDIX C.

Examples of reportable matters

Example 1 – Overpaid invoices	
Some customers of your *client* have overpaid their invoices. The *client* retains overpayments and credits them to the profit and loss account.	

Report	If you:
	• know or suspect that the *client* intends to dishonestly retain the overpayments. Reasons for such a belief may include:
	  ○ The *client* omits overpayments from statements of account.
	  ○ The *client* credits the profit and loss account without making any attempt to contact the overpaying party.

Do not report	If you:
	• believe that the *client* has no dishonest intent to permanently deprive the overpaying party. Reasons for such a belief may include:
	  ○ Systems operated by the *client* to notify the customer of overpayments.
	  ○ Evidence that requested repayments are processed promptly.
	  ○ Evidence that the *client* has attempted to contact the overpaying party.
	  ○ The *client* has sought and is following legal advice in respect of the overpayments.

Example 2 – Illegal dividends
Your *client* has paid a dividend based on draft accounts. Subsequent adjustments reduce distributable reserves to the extent that the dividend is now illegal.

Report	If there is suspicion of fraud.
Do not report	If there is no such suspicion. The payment of an illegal dividend is not a criminal offence under the Companies Act.

Example 3 – Invoices lacking commercial rationale	
Your *client* plans to expand its operations into a new country of operation. They have engaged a consultancy firm to oversee the implementation although it is not clear what the firm's role is. Payments made to the consultancy firm are large in comparison to the services provided and some of the expenses claimed are for significant sums to meet government officials' expenses. The country is one where corruption and facilitation payments are known to be widespread. You ask the Finance Director about the matter and he thought that such payments were acceptable in the country in question.	
Report	If you suspect that bribes have been paid.
Do not report	If you do not suspect illegal payments.
Money laundering offences include, in certain circumstances, conduct occurring overseas which would constitute an offence if it had occurred in Ireland.	

Example 4 – Concerted price rises	
Your *client's* overseas subsidiary is one of three key suppliers of goods to a particular market in Europe. The subsidiary has recently significantly increased its prices and margins and its principal competitors have done the same. There has been press speculation that the suppliers acted in concert, but publicly they have cited increased costs of production as driving the increase. Whilst this explains part of the reason for the increase, it is not the only reason because of the increase in margins. On reviewing the accounting records, you see significant payments for consultancy services and seek an explanation. Apparently, they relate to an assessment of the impact of the price increase on the market as well as some compensation for any losses the competitors suffered on their business outside of Europe. Some of the increased profits have flowed back to the Irish parent company. There is not a criminal cartel offence under local law but there is under Irish law.	
Report	If you suspect a price fixing cartel.
Do not report	If you do not suspect criminal activity.

6.2 Offences relating to reporting

Failure to disclose

6.2.1 Persons involved in the conduct of the designated activity e.g. employees of an accountancy firm ("relevant employees") should make sure that any information in their possession which is part of the required disclosure is passed to the MLRO as soon as practicably possible.

6.2.2 Where, as a result of an *internal report*, or otherwise, the MLRO obtains knowledge or forms a suspicion of *MLTF*, they must as soon as practicable make an external *STR* to *FIU Ireland* and the Revenue Commissioners. The *MLRO* may commit an offence if they fail to do so.

Defences and exemptions

6.2.3 There are defences to the offence of failing to report as follows:

- the *professional privilege reporting exemption* (see section 6.4 below) applies; or
- the *relevant employee* did not actually know or suspect *money laundering* has occurred and had not been provided by his employer with the training required by the *2010 Act*. If the employer has failed to provide the training, this is an offence on the part of the employer. In these circumstances, it may not be reasonable for relevant employees to be held liable for failing to make a report; or

- it is known, or believed on reasonable grounds, that the *money laundering* is occurring outside Ireland, and is not unlawful under the criminal law of the country where it is occurring.

6.2.2.1 In determining whether a failure to disclose offence has been committed under Section 42(9), the Courts may have regard to the content of this Guidance when applied to an *individual,* delivering *defined services,* or to an *MLRO* or other nominated officer, where one is appointed under the *accountancy firm's* procedures.

Prejudicing an investigation ('tipping off')

6.2.4 A person who knows or suspects, on the basis of information obtained in the course of carrying on business as a designated person, that a report concerning money laundering or terrorist financing has been, or is required to be made, commits an offence if they make any disclosure that is likely to prejudice an investigation that may be conducted following the making of the report (section 49 of the *2010 Act*).

6.2.5 This offence is committed when an *individual* in the *designated sector* discloses that:

- an *STR* has been, or is required to be, made and this disclosure is likely to prejudice any subsequent investigation; or
- an investigation into allegations of *MLTF* is underway (or being contemplated) and this disclosure is likely to prejudice that investigation.

6.2.6 Considerable care must be taken when communicating with *client*s or third parties if any form of *STR* has been made or is required to be made. Before disclosing any of the matters reported, or to be reported, it is important to consider carefully whether to do so is likely to constitute an offence of *prejudicing an investigation*. It is suggested that *accountancy firms* keep records of these deliberations and the conclusions reached.

6.2.7 No *tipping off* offence is committed under Section 53(1)(c) of the *2010 Act*, if the person did not know or suspect that their disclosure was likely to prejudice any subsequent investigation.

Permitted Disclosures

6.2.8 There are a number of exceptions to this prohibition on revealing the existence of or requirement to make a report or an actual or contemplated investigation which are as follows:

- **Section 50 - Disclosure to customer in case of direction or order to suspend service or *transaction***: it is a defence for *accountancy firms* to prove that the disclosure was to a customer/*client*, who was the subject of an order or direction given to the *accountancy firm* not to carry out any specified service or *transaction* (by a member of *FIU Ireland* of the rank of superintendent or above and/or on application by the Garda Síochána to the District Court), in accordance with Section 17, and the disclosure made was solely that the effect that the *accountancy firm* had been so ordered/directed.
- **Section 51(1) - Disclosures within an undertaking:** it is a defence to prove that the disclosures in question were between agents, employees, partners, directors or other officers of the same undertaking.
- **Section 51(2) - Disclosures between *credit* or *financial institutions, or a* majority owned subsidiary or branch of such institution, belonging to the same group**: a person does not commit an offence where disclosure is made between two or more institutions, belonging to the same *group* (as defined in Section 52(2) of the *2010 Act*, and the institution receiving the disclosure is from a Member State or from a country other than a *high-risk third country*.
- **Section 51(3) - Disclosures between legal advisers or *relevant professional advisers* within different undertakings that share common ownership, management or control**: it is a defence for a legal adviser or a *relevant professional adviser* to prove that the disclosure was made to another legal adviser or a *relevant professional adviser* where both the person making the disclosure and the person to whom it was made are in either a Member State or from a country, other than a *high-risk third country*, as imposing equivalent anti-*money laundering* requirements and both undertakings share common ownership, management or control.

- **Section 52 - Other permitted disclosures between institutions or professionals**: it a defence for a *credit institution*, a *financial institution*, a legal adviser or a *relevant professional adviser* to prove that the disclosure was
    - to another institution of the same type (e.g. one *credit institution* to another) or professional of the same kind from a different undertaking but of the same professional standing (including being subject to equivalent duties of professional confidentiality and the protection of personal data within the meaning of the Data Protection Legislation);
    - related to the same *client* or former *client* of both institutions or advisers or involves a *transaction* or provision of a service that involved them both;
    - was made only for the purpose of preventing a *money laundering* or *terrorist financing* offence; and
    - was made to a person in an EU Member State or a State imposing an equivalent anti-money laundering requirements.

    This means that, for example, an accountant may only disclose to another accountant, and not to a lawyer or another kind of *relevant professional advisor*.

- **Section 53 - Other permitted disclosures (general)**: a defence is available if the accountancy firm or individual is able to prove that disclosure is made:
    - to a *competent authority* by virtue of the *2010 Act*, or
    - for the purpose of the detection, investigation or prosecution of a criminal offence in the Ireland or elsewhere, or
    - because the person did not know or suspect, at the time of the disclosure, that the disclosure was likely to prejudice an investigation into whether a *money laundering* or *terrorist financing offence* had been committed, or
    - by an *accountancy firm* ('a *relevant professional adviser*' per the legislation) to its *client* solely to the effect that the *accountancy firm* would no longer provide the particular service in question to the *client*, provided that the *accountancy firm* ceased providing the service thereafter and made any *external report* required in accordance with the *2010 Act.*

- Agents of, and other persons 'engaged under a contract for services' with, *accountancy firms* are required, under sections 41 and 42 of the *2010 Act*, to make a report to *FIU Ireland* and the Revenue Commissioners where they have knowledge, suspicion or reasonable grounds for suspicion that another person "has been or is engaged in an offence of *money laundering* or *terrorist financing"*. Such reporting is required, independently of the *accountancy firm* and unlike the approach of the *2010 Act* with regard to employees being permitted to report by way of an internal reporting procedure, agents do not fulfil their obligations by reporting up to the *accountancy firm* to which they are contracted by way of an agreed reporting procedure. Section 52 would, however, permit agents, who are themselves *external accountants*, to report their knowledge and suspicions also to the *accountancy firm* to which they are contracted without committing the offence of prejudicing an investigation if such disclosure was for the purpose of preventing money laundering or terrorist financing.

6.2.9 A prohibited disclosure under section 49 of the *2010 Act (tipping off)* may be made in writing or verbally, and either directly or indirectly – including through inclusion of relevant information in published information. Considerable care is required in carrying out any communications with *clients* or third parties whilst considering whether to make a report as well as following any such report. Before any disclosure is made relating to matters referred to in an *internal report* or *an external report*, it is important to consider carefully whether or not it is likely to constitute an offence of *prejudicing an investigation*. It is suggested that *accountancy firms* keep records of these deliberations and the conclusions reached.

6.2.10 However, *individuals* and *accountancy firms* will frequently need to continue to deliver their professional services and a way needs to be found to achieve this without falling foul of the offence of *prejudicing an investigation*. More guidance on acting for a *client* after a *money laundering* suspicion has been formed is given in paragraph 6.5.3.

6.2.11 *Accountancy firms* should ensure they have sufficient document retention policies in place to meet their needs in this regard and in meeting their obligations under the *2010 Act*, as well as their legal and professional obligations more generally.

6.2.12 Falsification, concealment or destruction of documents relevant to an investigation (or causing the same) can also fall within this offence. Again, there is a defence if it was not known or suspected that the documents were relevant, or there was no intention to conceal facts.

6.3 When and how should a report be made?

Is a report required?

6.3.1 There are no hard and fast rules for recognising *MLTF*. It is important for everyone to remain alert to the risks and to apply their professional judgement, experience and scepticism.

6.3.2 All *individuals* involved in the conduct of the ***accountancy firm's*** business must, where concerned that criminal conduct may have occurred, ask themselves whether something they have observed in the course of business has the characteristics of *MLTF* and, therefore, warrants a *STR*. Most *firms* include in their standard anti-money laundering systems and controls arrangements to enable such individuals to discuss, with suitable people, whether their concerns amount to reportable knowledge or reasonable grounds for suspicion. *Individuals* should take advantage of these arrangements, where appropriate, to clarify reporting responsibilities

6.3.3 Once there is the requisite knowledge or suspicion, or reasonable grounds for either, then the staff member concerned must submit an *internal report* to their *MLRO* promptly. In exceptional circumstances, a report straight to *FIU Ireland and the Revenue Commissioners* may be appropriate. Sole practitioners make a report directly to *FIU Ireland* and the Revenue Commissioners.

6.3.4 There are no legal or other external requirements for the format of an *internal report* and accountancy firms may design their systems for internal reporting as they wish. *Internal reports* may be made orally or in writing, and may refer to *client* files or contain all the requisite information in a standard form, provided that all the information as required by Section 42(6) of the *2010 Act* and other information which the accountancy firm requires under its procedures for the reporting of money laundering are reliably provided and recorded.

6.3.5 Deciding whether or not something is suspicious may require further enquiries to be made with the *client* or their records (all within the normal scope of the assignment or *business relationship*). The Irish anti-money laundering regime does not prohibit normal commercial enquiries to fulfil *client* duties, and these may help establish whether or not something is properly a cause for suspicion.

6.3.6 Investigations into suspected *MLTF* should not be conducted unless to do so would be within the scope of the *engagement*. Any information sought should be in keeping with the normal conduct of business. Normal business activities should continue (subject to the *firm's* consideration of the risks involved), with any relevant information or other matters that flow from those activities included in an *STR*. To perform additional investigations is not only unnecessary, it is undesirable since it would risk *tipping off* a money launderer.

6.3.7 *Individuals* may wish to consider the following questions to assist their decision:

Step	Question
1	• Do I have knowledge or suspicion, or reasonable grounds for suspicion, of criminal activity? Or • Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion or reasonable grounds for suspicion of *MLTF*?
2	• Do I know or suspect, or have reasonable grounds to suspect, that a benefit arose from the activity in 1?
3	• Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
4	• Can I identify the person (or persons) in possession of the benefit? Or • Do I know the location of the benefit? Or • Do I have information that will help identify the person (or persons)? Or • Do I have information that will help locate the benefits?

6.3.8 Note that the reporting requirement may relate to any information coming to an *accountancy firm* in the course of carrying on business as an *accountancy firm*, and not just information relating to *clients* and their affairs. This means that reports may be required on the basis of information not only about *clients*, but about potential *clients*, associates and counterparties of *clients*, acquisition targets and even employees of *accountancy firms.*

6.3.9 If in doubt, always report concerns to the *MLRO*.

***Internal reports to the MLRO or other* nominated officer**

6.3.10 Only sole practitioners, who employ no employees, or who themselves undertake the role of the *MLRO* (see section 3.2 of this guidance),.have a duty to submit *STRs* straight to *FIU Ireland* and the Revenue Commissioners.

6.3.11 Section 44 of *the 2010 Act* provides for *individuals* undertaking work for an *accountancy firm* to make an *internal report* to their *MLRO* in accordance with an internal reporting procedure – reporting to a line manager or colleague is not enough to comply with the legislation. In making an *internal report* to their *MLRO,* the *individual* has a defence against accusations of failing to report under Sections 42 and 43 of the *2010 Act*. It is vital that all principals and staff of an *accountancy firm* clearly understand the communication lines for reporting suspicions of money laundering with the *accountancy firm's* procedures, and the importance of complying with those procedures in meeting the obligation both of *individuals* and of the *accountancy firm* under the legislation. Someone seeking reassurance that their conclusions are reasonable can discuss their suspicions with managers or other colleagues, in line with the *firm's* procedures.

6.3.12 When more than one member of staff is aware of the same reportable matter a single *internal report* can be submitted to the *MLRO*, but it should contain the names of all those making the report. No *internal report* should be made in the name of an individual who is unaware of the existence of the *internal report*. There is no prescribed format for internal *STRs* to be made to an *MLRO* or other nominated person.

6.3.13 The role of the *MLRO* should be undertaken by an appropriately experienced *individual*. One of the principals of an accountancy firm, or similar in other *accountancy firms*, is likely to be suitable, or another senior and skilled person with sufficient authority to enable decisions to be taken independently. Fulfilling that role in relation to STRs involves:

- considering *internal reports* of money laundering;
- deciding if there are sufficient grounds for suspicion to pass those reports on to *FIU Ireland* and the Revenue Commissioners in the form of an *external report*, and, if so, to make that report;
- acting as the key liaison point with *FIU Ireland* and the Revenue Commissioners;
- advising on how to proceed with work once an *internal report* and/or *external report* has been made in order to guard against risks of *prejudicing an investigation.*

6.3.14 If these responsibilities are not undertaken by the *MLRO*), they should be taken on by another sufficiently senior and skilled person within the *accountancy firm*. This person should work closely with the MRLO.

6.3.15 Depending on the size and complexity of an *accountancy firm*, it may establish procedures such that the functions of an *MLRO* can be delegated, although it would be advisable that the *MLRO* maintain close supervision of such delegated functions. It would also be advisable for *accountancy firms* to have contingency arrangements for discharging the duties of a *MLRO*, where appointed, during periods of absence or unavailability. *Accountancy firms* may consider appointing an alternate or deputy *MLRO* for these situations and ensure that the reporting channels are well known to all relevant employees.

6.3.16 Like all *individuals*, *MLROs*, where appointed, can commit the money laundering and *terrorist financing* offences as well as the related offences of failure to disclose and *prejudicing an investigation*.

Onward reports by the MLRO to FIU Ireland and the Revenue Commissioners

6.3.17 It is the *MLRO's* responsibility to decide whether the information reported internally needs to be reported to *FIU Ireland* and the Revenue Commissioners. When an *internal report* is submitted, there are two matters which need to be dealt with immediately. Rapid consideration of the *internal report* is needed as section 42(7) of the *2010 Act* requires, with only limited exceptions, that where a report is deemed necessary, it must be submitted before the *accountancy firm*

proceeds with the *transaction* or service in question (see section 6.5). In addition, the *accountancy firm* should first establish by discussion and review whether or not the *professional privilege reporting exemption* may apply, as this exemption significantly affects not only whether an *external report* must be made under the legislation, but also whether it may be made.

6.3.18 External STRs to *FIU Ireland* are required to be made using the GoAML Online System. Guidance on registration and use of the system has been issued by the Department of Justice and Equality, and is available at *GoAML*.

6.3.19 Following acceptance of a report to *FIU Ireland* via GoAML*, a* printed copy of the online report should be forwarded to the Revenue Commissioners.

6.3.20 The *accountancy firm's* procedures should also address the process for considering whether or not to proceed with a *transaction* or service in circumstances where a report is deemed necessary but has not yet been submitted.

6.3.21 *MLROs* should approach external reporting with caution. When deciding what to do they should consider the following questions:

Step	Question
1	• Do I know or suspect (or have reasonable grounds for either) that someone is engaged in MLTF?
2	• Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
3	• From the contents of the internal *STR,* can I identify the suspect or the whereabouts of any laundered property if this information is available through normal conduct of business?
4	• Can I provide the information essential to an external *STR* without disclosing information acquired in privileged circumstances? The professional privilege reporting exemption is limits to *relevant professional advisers* as defined by the *2010 Act*. Further guidance on the privilege reporting exemption can be found in section 6.4 of this guidance.

6.3.22 The MLRO may want to make reasonable enquiries of within the *firm*. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for an external *STR.*

6.3.23 The disclosure of information in accordance with the requirements of the *2010 Act* shall not be treated, for any purpose, as a breach of any other enactment or rule of law e.g. Data Protection Legislation (Section 47 of the *2010 Act*) or the *accounting firm*'s duty of client confidentiality

Timing of Reporting

6.3.24 Knowledge, suspicions or reasonable grounds for suspicion are deemed only to arise where the *accountancy firm* has scrutinised the information "in the course of reasonable business practice" (Section 42(3) of the *2010 Act*). *CCAB-I* understands this provision to emphasise that the information must come to the *accountancy firm* "in the course of carrying on business" of an *accountancy firm* (Section 42(1) of the *2010 Act*) and there is no obligation to complete an assessment of that information on a timescale which is different to that on which the *firm* normally conducts its business.

6.3.25 Care is advised in applying this provision, however, as information might come to an *accountancy firm* in circumstances where normal business practice might be that such information would typically not be scrutinised until a later date, which might be some time after the information is received. Section 42(2) requires a report "as soon as practicable after acquiring that knowledge or forming that suspicion". For example, audit conclusions are made at the end of the audit process and this may have an impact on the timing of the auditor's judgement that an issue is reportable under Section 42. In certain circumstances, an auditor may only be able to conclude at audit completion and sign off that he has reasonable grounds for suspecting that an offence resulting in proceeds has taken place. Also, information may be received during the course of an interim audit, which may take place some months before the planned audit completion and sign off, and such information might not normally be considered until a much later stage in the audit process.

6.3.26 An *accountancy firm* which does not deal with information for an extended period of time after receiving the information or forming the suspicion could expose itself to an accusation of a breach of Section 42(2) on timely reporting. Where doubt exists, it would be advisable to seek legal advice.

What information should be included in an external STR?

6.3.27 An *external report* to *FIU Ireland* is made by completing an *STR* on the GoAML website. Following the acceptance of that report by *FIU Ireland*, a copy of the accepted *STR* is sent to the Revenue Commissioners. Guidance can be found at http://www.antimoneylaundering.gov.ie/en/AMLCU/Pages/GoAML_and_Suspicious_Transaction_Reports_STRs. The following details are required by the *STR* report to be completed should be regarded as essential information:

- Name of reporter;
- Date of report;
- The name of the suspect or information that may help identify them, if this information is available. As many details as possible should be provided to *FIU Ireland* to assist with the identification of the suspect;
- Details of who else is involved, associated, and how, if this information is available;
- Clarification of the role of each subject/person, as far as it is known, in the matter, clearly identifying whether or not each subject/person is suspected of being involved in the commission of the alleged money laundering or *terrorist financing* offence;
- Information regarding bank account/*transaction* details, where available and relevant;
- The facts regarding what is suspected or the grounds for suspicion and why. The 'why' should be explained clearly so that it can be understood without professional or specialist knowledge;
- The whereabouts of any criminal property, or information that may help locate it, if this information is available;
- Section 42(6) requires that the *accountancy firm* include "any relevant information" in the *external report*. This could, for example, include the names of victims or other persons associated with the activity. If such persons are not suspected by the *accountancy firm* to be involved in the alleged *money laundering* of *terrorist financing* offence, the report should clearly state this.

6.3.28 All external *STRs* should be free of jargon and written in plain English.

6.3.29 It is recommended that in making an external STR the reporters:

- do not include confidential information not required by AML legislation;
- show the name of the *accountancy firm*, *individual* or *MLRO* submitting the report only once, in the source ID field and nowhere else;
- do not include the names of those who made the internal *STRs* to the *MLRO*;
- include other parties as 'subjects' only when the information is necessary for an understanding of the external *STR* or to meet *required disclosure* standards; and
- highlight clearly any particular concerns the reporter might have about safety (whether physical, reputational or other). This information should be included in the 'reasons for suspicion/disclosure' field.

Confidentiality

6.3.30 A correctly made external *STR* provides full immunity from action for any form of breach of confidentiality, whether it arises out of professional ethical requirements or a legal duty created by contract (e.g., a non-disclosure agreement).

6.3.31 There will be no such immunity if the external *STR* is not based on knowledge or suspicion or reasonable grounds for suspicion, or if it is intended to be 'defensive' i.e., for the purposes of regulatory compliance rather than because of a genuine suspicion.

Documenting reporting decisions

6.3.32 In order to control legal risks it is important that adequate records of internal *STRs* are kept. This is usually done by the *MLRO* or person nominated by the *MLRO* and would normally include details of:

- all internal *STRs* made;
- how the *MLRO* handled matters, including any requests for further information;
- assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information;
- the rationale for deciding whether or not to make an external *STR*;
- any advice given to engagement teams about continued working.

These records can be simple or sophisticated, depending on the size of the *firm* and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. They are important because they may be needed later if the *MLRO* is required to justify and defend their actions.

6.3.33 For the *MLRO's* efficiency and ease of reference, a reporting index may be kept and each internal *STR* given a unique reference number.

6.4 Reporting and the privileged circumstances exemption

6.4.1 Section 46(1) of the *2010 Act* states that disclosure of information which is subject to legal privilege is not required. *Accountancy firms* and *individuals* may, in the course of their work, receive information documentation subject to legal privilege, for example when engaged by a legal professional to carry out work on behalf of a *client*.

6.4.2 Apart from legal privilege, Section 46(2) of the 2010 Act, as quoted below, also establishes that *relevant professional advisers* are not required to submit an *external report* in certain circumstances.

> "Nothing in this Chapter requires a relevant professional adviser to disclose information that he or she has received from or obtained in relation to a client in the course of ascertaining the legal position of the client."

6.4.3 *Relevant professional advisers* who know about or suspect *MLTF* (or have reasonable grounds for either) are not required to submit an external *STR* if the information came to them in privileged circumstances, defined in section 46(2) as being when ascertaining the legal position of the *client*. In these circumstances, and as long as the information was not provided with the intention of advancing a crime, then the information need not be reported. The *privileged reporting exemption* only covers *STRs* and should not be confused with legal professional privilege (see paragraph 6.4.2 above), which also extends to other documentation and advice.

6.4.4 In Section 24 of the *2010 Act*, *relevant professional adviser* is defined as an accountant, auditor or *tax adviser* who is a member of a designated accountancy body or of the Irish Institute of Taxation.

6.4.5 Whether or not the privilege reporting exemption applies to a given situation is a matter for careful consideration. The *firm* may have been providing the *client* with a variety of services, not all of which would create the circumstances required for the exemption. Consequently, it is strongly recommended that careful records are kept about the provenance of the information under consideration when decisions of this kind are being made. Legal advice may be needed.

6.4.6 Audit work, book-keeping, preparation of accounts or tax compliance assignments are unlikely to take place in privileged circumstances.

Discussion with the MLRO

6.4.7 Given the complexity of these matters – as well as the need for a considered and consistent approach to all decisions, supported by adequate documentation – it is recommended that they are always discussed with the *MLRO*.

6.4.8 Where the purpose of these discussions is to obtain advice on making a disclosure under Section 43 of the *2010 Act* they do not affect the applicability of the privilege reporting exemption.

The crime/fraud exception

6.4.9 Information received from or obtained in relation to a client that would otherwise qualify for the privilege reporting exemption are excluded from it when they are intended to facilitate or guide anyone in the furtherance of a criminal purpose. An example of this might be where tax advice was sought ostensibly to enable the affairs of a tax evader to be regularised but in reality was sought to aid continued evasion by improving the evader's understanding of the relevant issues. This is usually the *client* but could be a third party.

6.4.10 The criminal purpose exception does not apply where the adviser is approached to advise on the consequences of a crime or fraud or similar conduct that has already taken place and where the *client* has no intention, in seeking advice, to further that crime or fraud. This means that a person who is concerned that he may be guilty of tax evasion can approach a *tax adviser* for legal advice in this regard without fear of the exception being invoked. This remains the case even if the potential *client* declines a *client* relationship having received the advice, and the adviser does not know whether the person will proceed to rectify his affairs. However, if the person behaves in a way that makes the adviser suspicious that the intended use of the advice is to further continued evasion, then an *external report* could be required.

6.4.11 In summary, the following issues need to be considered before deciding whether to apply the professional privilege reporting exemption:

(a) Are those who received the information or other matter which gave rise to knowledge or suspicion of *money laundering or terrorist financing offences relevant professional advisers* (Section 24 of the *2010 Act*)?

(b) Was the information or other matter which gave rise to knowledge or suspicion of money laundering/*terrorist financing* received by the *relevant professional adviser* in privileged circumstances (Section 46(2) of the *2010 Act*) and not in some other communication or situation?

(c) Was the information or other matter received or communicated with the intention of furthering a criminal purpose (i.e., does the criminal purpose exception apply (Section 46(3) of the *2010 Act*)?

If the answers to (a) and (b) are yes, and the answer to (c) is no, the professional privilege reporting exemption must be applied. If the answer to (a) and (b) are yes and the answer to (c) is yes, the criminal purpose exception applies and an *external report* must be made. Further advice should be sought from the relevant professional body or a lawyer in cases of doubt. This issue may be vital in balancing legal and professional requirements for confidentiality and for serving the public interest and the interests of *clients*. If doubts cannot be resolved through internal discussion, through access to normal sources of professional advice, *accountancy firms* are strongly recommended to seek advice from a professional legal adviser with experience of these matters.

6.5 Determining whether to proceed with or withdraw from a *transaction* or service

6.5.1 As noted above, *external reports* must be made as soon as practicable. Section 42(7) of the *2010 Act* requires an *accountancy firm*, obliged to make an *external STR,* to do so before proceeding with any suspicious *transaction* or service that is connected with, or the subject of, the report. There are two exceptions to this requirement, namely:

- where it is not practicable to delay or stop the *transaction* or service from proceeding; or
- where the *accountancy firm* reasonably believes that a failure to proceed with the *transaction* would alert the other person to the possibility that a report may have been or will be made, or that an investigation is being contemplated or is on-going.

6.5.2 These exceptions do not apply to situations where the *accountancy firm* has received a valid direction from the Garda Síochána or an order from a judge of the District Court not to proceed with the *transaction* or service (see section 42(8) of the *2010 Act*).

6.5.3 When preparing to make an external *STR* the *MLRO* must consider carefully whether the *firm* would commit a *money laundering offence* if it continued to act as it intends (usually as instructed by the *client*).

Proceeding with a transaction or service

6.5.4 Examples of scenarios which may constitute a "*transaction* or service connected with, or the subject of, the report", requiring the *external STR* to be made prior to proceeding might include:

- acting as an insolvency officeholder when there is knowledge or a suspicion that either:
  - all or some assets in the insolvency are criminal property; or
  - the insolvent entity may enter into, or become concerned in, an arrangement which facilitates the “converting, transferring, handling, acquiring, possessing or using” the *proceeds of criminal conduct* (under section 7 of the *2010 Act*);
- designing and implementing trust or company structures (including acting as trustee or company officer) when there is knowledge or suspicion arises that the *client* is, or will, or may be about to, use these to launder money or finance terrorism;
- acting as an agent of a *client* in the negotiation or implementation of a *transaction* (such as a corporate acquisition) in which there is an element of criminal property being bought or sold by the *client*;
- handling through *client* accounts money that is suspected of being criminal in origin;
- providing outsourced business processing services to *client*s when the money is suspected of having criminal origins.

Typically, the issuing of an opinion on whether a set of financial statements give a true and fair view of the performance and financial position of the reporting entity is unlikely to be relevant to, or connected with, an *external STR* to *FIU Ireland* and the Revenue Commissioners regarding knowledge or suspicions of the commission of a *money laundering* or *terrorist financing offence*. However, if the auditor suspects that the audit report is necessary in order for financial statements to be issued in connection with a *transaction* involving the proceeds of crime, or if the auditor is due to sign off an auditor's report on financial statements for a company that he suspects to be a front for illegal activity, the auditor might be involved in an arrangement which facilitates the "converting, transferring, handing, acquiring possessing or using" the *proceeds of criminal conduct*.

Instructions not to proceed with a transaction or service

6.5.5 Under Section 17(1), a member of the Garda Síochána, who has a rank "not below the rank of superintendent", may direct a person, in writing, not to proceed with a particular service or *transaction* for the period specified in the direction, not to exceed seven days. A District Court Judge may also issue and order not to proceed with a specified service or transaction. For further details, see Appendix F.

6.6 What should happen after an external *STR* has been made?

Client relationships

6.6.1 *Accountancy firms* do not have to stop working after submission of an *external STR* unless a direction of an appropriate member of the Garda Síochána (rank of superintendent or above) or an order from a judge of the District Court is received (Appendix E), in which case all or part of *client* work may well need to be suspended until the relevant period of the direction/order lapses or notice is received in writing that the direction/order ceases to have effect.

6.6.2 Where an *external STR* involves a *client* as a suspect, *accountancy firms* may wish to consider whether the behaviour observed is such that for professional reasons the *accountancy firm* no longer wishes to act.

6.6.3 Generally, if following a report of suspicion, an *accountancy firm* wishes for its own commercial or ethical reasons to exit a relationship, there is nothing to prevent this provided the way the exit is communicated does not constitute an offence of *prejudicing an investigation* under section 49 of the *2010 Act*.

6.6.4 If a decision is made to terminate a *client* relationship, an *accountancy firm* should follow its normal procedures in this regard, whilst always bearing in mind the need to avoid *prejudicing an*

investigation. Section 53(2) of the *2010 Act* provides a defence for a legal adviser or *relevant professional adviser* (see Section 24 of the *2010 Act*) in exiting a *client* relationship, as long as:

- the disclosure was solely to the effect that the legal adviser or *relevant professional adviser* would no longer provide the particular service concerned to the *client;*
- the service duly ceases once the *client* has been informed; and
- the *relevant professional adviser* made any report required in accordance with *the 2010 Act*.

Balancing professional work and the requirements of the 2010 Act

6.6.5 Normal commercial enquiries to understand a *transaction* carried out in the course of an engagement will not generally lead to *prejudicing an investigation*, although care should be exercised to avoid either making a disclosure prohibited under section 49 of the *2010 Act* (see paragraphs 6.2.4 to 6.2.12) or making accusations or suggesting that any person is guilty of an offence. It is important to confine enquiries to those required in the ordinary course of business and not attempt to investigate a matter unless that is within the scope of the professional work commissioned.

6.6.6 Continuation of work may require discussion with *client senior management* of matters relating to suspicions formed. This may be of particular importance in audit relationships. Care must be taken to select appropriate, and non-complicit, members of *senior management* for such discussion whilst always bearing in mind the need to avoid *prejudicing an investigation.*

6.6.7 In more complex circumstances, consultation with the Garda Síochána may be necessary before enquiries are continued, but in most cases a common sense approach will resolve the issue.

6.6.8 *Accountancy firms* may wish to consult the *MLRO*, where appointed, or other *individual(s)* in accordance with the *accountancy firm's* procedures, or other suitable specialist (for example a solicitor) regularly if there are concerns with regard to *prejudicing an investigation*, and, in particular, it is important that before any document referring to the subject matter of a report is released to a third party the *MLRO,* if appointed, is consulted and, in extreme cases, the Garda Síochána. Some typical examples of documents released to third parties are shown below as an aide memoire:

- public audit or other attest reports;
- public record reports to regulators;
- confidential reports to regulators (e.g. to the Central Bank of Ireland);
- provision of information to sponsors or other statements in connection with the Irish Stock Exchange Listing Rules;
- reports by a liquidator to the Director of Corporate Enforcement on the conduct of directors under Section 682 of the Companies Act 2014;
- statements on resignation as auditors in accordance with Section 400 and 403 of the Companies Act 2014;
- professional clearance/etiquette letters;
- communications to *clients* of intention to resign.

6.6.9 In particular, Section 400 of the Companies Act 2014 ('2014 Act') requires notice of auditor resignations to be filed at the Companies Registration Office and such notice to include statements of any circumstances "connected with the resignation to which it relates that the auditor concerned considers should be brought to the notice of the members or creditors of the company". Furthermore, Section 403 of the 2014 Act requires notification to the Irish Auditing and Accounting Supervisory Authority ('IAASA') where an auditor resigns in accordance with Section 400 of the 2014 Act, or is removed in accordance with Section 399 of the 2014 Act, during the period between the conclusion of the last annual general meeting and the conclusion of the next annual general meeting. Notice of resignation to IAASA is to be accompanied by the resignation notice served under Section 400(3) of the 2014 Act (or, in the case of removal, by a copy of any representations made by the auditor to the company in accordance with Section 399(3) of the 2014 Act – except where they were not sent out to the members in accordance with Section 399(4)). The contents of such statements require careful consideration to ensure that statutory and professional duties are met, without including such information as may constitute an offence of *prejudicing an investigation*. There are no provisions in the *2010 Act* in this regard. However, *accountancy firms* may well wish, in cases of complexity, to discuss the matter with the Garda Síochána in order to understand their perspective and document such discussion.

6.6.10 Such a discussion with the Garda Síochána may well be valuable, but *accountancy firms* and *individuals* should bear in mind these authorities are not able to advise, and nor are they entitled to dictate how professional relationships should be conducted. It may be possible to arrive at an agreed wording, such that the *firm's* obligations are adequately addressed whilst the relevant law enforcement agency is satisfied that the wording would not *prejudice an investigation*. In such circumstances, it is unlikely that the *firm* will know or suspect that the report will *prejudice an investigation*. If the wording cannot be agreed, the *firm* or *individual* should seek legal advice and potentially the directions of the Court to protect itself.

6.6.11 *Accountancy firms* may on occasion need advice to assist them in considering such reporting issues. Legal advice may be sought from a suitably skilled and knowledgeable professional legal adviser, and recourse may also be had to helplines and support services provided by professional bodies.

6.7 Requests for further information

Requests from FIU Ireland and/or the Revenue Commissioners

6.7.1 *FIU Ireland* is responsible for receiving and analysing *STRs* and other information for the purpose of prevention, detection and investigation of possible MLTF offences. According to section 40C(3) of the *2010 Act* a member of the Garda Síochána, who is a member of *FIU Ireland*, may request, in writing, a *designated person* to provide any financial, administrative or law enforcement information that *FIU Ireland* requires to assist it in its functions. Additionally s42(6A) of the *2010 Act* requires a *designated person* who is required to make a *STR* to respond to any request for additional information by *FIU Ireland* or the Revenue Commissioners as soon as practicable after receiving the request and to take all reasonable steps to provide any information specified in the request.

6.7.2 Before responding, it is recommended that a verification process is undertaken to ensure the person making contact is a bona fide member of the Garda Síochána / the Revenue Commissioners. This may be most simply achieved by taking a caller's name and organisation details, and then calling the main switchboard of the organisation to be put through to the person.

6.7.3 To the extent that the request is simply aimed at clarifying the content of an *external report*, *accountancy firms/individuals* may respond without the need for any further process.

6.7.4 However, if the request is for production of documents or provision of information additional to the *external report*, it is recommended that *accountancy firms/individuals* require the relevant agency to use its powers of compulsion before they respond to requests by *FIU Ireland* or the Revenue Commissioners. This is not intended to be non co-operative, and indeed *accountancy firms/individuals* are recommended to engage in constructive dialogue with *FIU Ireland* / Revenue Commissioners, including as to the content and drafting of the request, but is intended to protect *accountancy firms/individuals* from allegations that they breached confidentiality. *Client* or other third party consent is not required in cases of compulsion, and nor should it be sought due to the risk of *prejudicing an investigation.*

6.7.5 Before providing information to a member of *FIU Ireland* or the Revenue Commissioners, *accountancy firms/individuals* should require evidence of the person's identity, for example, by showing official identification and a copy of the relevant order, or *accountancy firms* may attend the premises of the relevant agency to hand over the information.

6.7.6 Before responding to requests for further information, *accountancy firms/individuals* should ensure they understand

- the authority under which the request is made;
- the extent of the information requested;
- the required timing and manner of the production of information; and
- what information should be excluded *e.g.,* that subject to legal privilege.

If in any doubt, *accountancy firms/individuals* should seek legal advice. *Accountancy firms* should document their consideration of the issues.

6.7.7 Information or documentation that is subject to legal privilege or legal professional reporting privilege should not be provided. If *individuals* or *accountancy firms* are unsure as to whether certain documents fall within the privileged category or not, they should not include these documents in response to enquiries and seek legal advice.

Requests arising from a change of professional appointment (professional enquiries)

Requests regarding client identification or information regarding suspicious transactions

6.7.8 In general, it is recommended that such requests are declined as the offence of *prejudicing an investigation* greatly restricts the ability to make such disclosures. It is recommended that *accountancy firms* do not respond to questions in professional enquiry letters concerning either their satisfaction as to the identity of an entity or natural person or as to whether any *external report* has been made or contemplated. *Accountancy firms* may wish to consider a standard wording in such responses to the effect that the legislation precludes them from responding to such queries.

Data protection - including subject access requests

6.7.9 Under the Data Protection Legislation *accountancy firms* need not comply with data subject access requests that are likely to prejudice the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties. Similarly, personal data that relates to knowledge or suspicion of *MLTF* (i.e., data that has been processed to help prevent or detect crime) should not be disclosed under a subject access request especially as to do so could constitute *tipping off*. Both of these exceptions apply to the personal data likely to be contained in records relating to internal *MLTF* reports and *STRs*.

6.7.10 Personal data exempt from one subject access request may no longer be exempt at the time of a subsequent request (perhaps because the original suspicion has by then been proved false). When a *firm* receives a data subject access request covering personal data in its possession, it should always consider whether the exception applies to that specific request regardless of any history of previous requests relating to the same data. These deliberations will usually involve the *MLRO,* or other designated person, and the data protection officer. It is recommended that the thinking behind any decision to grant or refuse access is documented.

7 RECORD KEEPING

- Why may existing document retention policies need to be changed?
- What should be considered regarding retention policies?
- What considerations apply to *STRs* and directions, orders and authorisations relating to investigations?
- What considerations apply to training records?
- Where should reporting records be located?
- What do *accountancy firms* need to do regarding third-party arrangements?
- What are the requirements regarding the deletion of personal data?

7.1 Why may existing document retention policies need to be changed?

7.1.1 Records relating to *CDD*, the *business relationship* and *occasional transactions* must be kept for five years from the end of the *client* relationship. More specifically, records must be kept of *clients'* identity, the supporting evidence of verification of identity (in each case including the original and any updated records), the firm's *business relationships* with them (i.e. including any non- engagement related documents relating to the *client* relationship) and details of any *occasional transactions* and details of *monitoring* of the relationship.

7.1.2 All records related to an *occasional transaction* must be retained for five years after the date of the *transaction*.

7.1.3 The *2010 Act* does not specify the medium in which records should be kept, but they must be readily retrievable.

7.2 What should be considered regarding retention policies?

7.2.1 *Accountancy firms* must be aware of the interaction between of *MLTF* laws with the requirements of the GDPR. The Data Protection Regime requires that personal information be subject to appropriate security measures and retained for no longer than necessary for the purpose for which it was originally acquired.

7.3 What considerations apply to *STRs* and directions, orders and authorisations relating to investigations?

7.3.1 No retention period is officially specified for records relating to:

- *internal reports*;
- the *MLRO's* consideration of *internal reports*;
- any subsequent reporting decisions;
- issues connected to directions, orders and authorisations relating to investigations (sections 17-23 of the *2010 Act*), production of documents and similar matters;
- suspicious transaction reports;
- requests received for additional information in accordance with Section 42(6A) of the *2010 Act* sent to the Garda Síochána and Revenue Commissioners, or its responses to such requests;
- Copies of requests received from *FIU Ireland* or Revenue Commissioners in accordance with Section 41(1) of the *2010 Act*, copies of the relevant orders, evidence of agent's identity and resulting consideration of the matter by the firm;
- Requests from "relevant third parties" in accordance with Section 40 of the *2010 Act* and related considerations and responses.

7.3.2 Since these records can form the basis of a defence against accusations of MLTF and related offences, *firms* will determine an appropriate retention period for them, taking into account the Statute of Limitations and potential gravity of the underlying matter.

7.4 Where should reporting records be located?

7.4.1 Records related to internal and external *STRs* of suspicious *transactions* are not part of the working papers relating to *client* assignments. They should be stored separately and securely as a safeguard against *tipping off* and inadvertent disclosure to someone making routine use of *client* working papers.

7.5 What considerations apply to training records?

7.5.1 *Accountancy firms* must demonstrate their compliance with *2010 Act* that place a legal obligation on them to make sure that certain of their relevant employees are

(a) aware of the law relating to *MLTF*, and

(b) trained regularly in how to recognise and deal with *transactions* and other events which may be related to *MLTF*.

7.5.2 These records should show the training that was given, the dates on which it was given, which *individuals* received the training and the results from any assessments.

7.6 What do *accountancy firms* need to do regarding third-party arrangements?

7.6.1 An *accountancy firm* may arrange for another organisation to perform some of its AML related activities – *CDD* or training, for example. In which case, it must also ensure that the other party's record keeping procedures are good enough to demonstrate compliance with the *MLTF* obligations, or else it must obtain and store copies of the records for itself. It must also consider how it would obtain its records from the other party should they be needed, as well as what would happen to them if the other party ceased trading.

8 TRAINING AND AWARENESS

- Who should be trained and who is responsible for it?
- What should be included in the training?
- When should training be completed?

8.1 Who should be trained and who is responsible for it?

8.1.1 The *2010 Act* requires that all *individuals* involved in providing *defined services* (including partners are made aware of MLTF law and trained regularly to recognise and deal with activities which may be related to MLTF, as well as to identify and report anything that gives grounds for suspicion (see Section 6 of this guidance).

8.1.2 Thought should also be given to who else might need AML training. When identifying which staff may be considered relevant, *accountancy firms* should consider not only those who have involvement in *client* work, but also, where appropriate, those who deal with the *firm's* finances, and those who deal with procuring services on behalf of the *firm* and who manage those services. Accordingly, it is likely that all client-facing staff will be considered relevant and at least the senior support staff. *Firms* may decide to provide comprehensive training to all relevant staff members, or may choose to tailor their provision to match more closely the role of the employees concerned. In particular, *MLROs*, where appointed, or other individual(s) given significant responsibilities in relation to compliance with the firm's obligations under the *2010 Act,* may require supplementary training, and members of *senior management* may also benefit from a customised approach or some supplementary training.

8.1.3 The *MLRO* (or another member of senior management) should be made responsible for ensuring that appropriate AML training is delivered. There should be a mechanism to ensure that *individuals* complete their AML training promptly.

8.1.4 Someone accused of a failure-to-disclose offence has a defence if:

- they did not know or suspect that someone was engaged in money laundering even though they should have; but
- their employer had failed to provide them with the appropriate training.

8.1.5 This defence – that an *individual* did not receive the required AML training – is likely to put the *accountancy firm* at risk of prosecution for a regulatory breach.

8.2 What should be included in the training?

8.2.1 Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them.

8.2.2 The programme itself should include:

- an explanation of the law within the context of the *firm's* own commercial activities;
- so-called 'red flags' of which *individuals* should be aware when conducting business, which would cover all aspects of the MLTF procedures, including CDD (for example those that might prompt doubts over the veracity of evidence provided) and *STRs* (for example what might prompt suspicion); and
- how to deal with activities that might be related to *MLTF* (including how to use internal reporting systems), the *firm's* expectations of confidentiality, and how to avoid *tipping off* (see Section six of this guidance).

8.2.3 Training programmes should be tailored to each business area and cover the *firm's* procedures so that *individuals* understand the *MLTF* risks posed by the specific services they provide and types of *client* they deal with, and so are able to appreciate, on a case-by-case basis, the approach they should be taking. Furthermore, *firm's* should aim to create an AML culture in which employees are always alert to the risks of *MLTF* and habitually adopt a risk based approach to *CDD*.

8.2.4 Records should be kept showing who has received training, the training received and when training took place (see 7.4 of this guidance). These records should be used so as to inform when additional training is needed – e.g. when the *MLTF* risk of a specific business area changes, or when the role of an *individual* changes.

8.2.5 The effectiveness of the training, should be considered on an ongoing basis.

8.2.6 The overall objective of training is not for employees and partners to develop a specialist knowledge of criminal law. However, they should be able to apply a level of legal and business knowledge that would reasonably be expected of someone in their role and with their experience, particularly when deciding whether to make an internal *STR* to the *MLRO* or other designated person.

8.3 When should training be completed?

8.3.1 *Accountancy firms* need to make sure that new employees are trained promptly.

8.3.2 The frequency of training events can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), the *firm's* risk profile, procedures, and service lines.

8.3.3 It may not be necessary to repeat a complete training programme regularly, but it may be appropriate to provide employees and partners with concise updates to help refresh and expand their knowledge and to remind them how important effective anti-money laundering work is.

8.3.4 In addition to training, *firms* are encouraged to mount periodic *MLTF* awareness campaigns to maintain alertness to individual and firm-wide responsibilities.

GLOSSARY

2005 Act Criminal Justice (Terrorist Offences) Act 2005

2010 Act Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

2018 Act Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

Accountancy firm(s)/Firm(s) A firm, sole practitioner, company, partnership or other organisation undertaking *defined services*. This includes accountancy practices, whether structured as partnerships, sole practitioners or corporate practices.

Accountancy services For the purpose of this guidance this includes any service provided under a contract for services (i.e. not under a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.

Business relationship a business, professional or commercial relationship between a *designated person* and a customer, which is expected by the *designated person*, at the time when contact is established, to have an element of duration.

Business risk assessment has the meaning given by section 30A of the *2010 Act* and shall take into account

- the type of clients that the firm has;
- the products and services that the designated person provides;
- the countries or geographical areas in which the firm or its clients operate (taking into account those jurisdictions identified as high risk by FATF and the EU);
- the type of services that the firm provides;
- the delivery channels used for those service;
- other prescribed additional risk factors.

Capital Requirements Regulations means Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for *credit institutions* and investment firms and amending Regulation (EU) No 648/2012.

CCAB-I the Consultative Committee of Accountancy Bodies in Ireland, which represents Chartered Accountants Ireland, the Association of Chartered Certified Accountants, the Chartered Institute of Management Accountants; and the Institute of Certified Public Accountants in Ireland.

CDD Client due diligence.

Client A person or entity in a *business relationship*, or carrying out an *occasional transaction*, with an *accountancy firm*.

Close associate of a *politically exposed person* means any individual has joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a *politically exposed person*; any individual who has sole beneficial ownership of a legal entity or a legal arrangement set up for the actual benefit of a *politically exposed person* (Section 37(10) of the *2010 Act*).

Collective investment undertaking means (a) an undertaking for collective investment in transferable securities authorised in accordance with the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 (S.I. No. 352 of 2011) or otherwise in accordance with the Directive of 2009, (b) an alternative investment fund within the meaning of the European Union (Alternative Investment Fund Managers) Regulations 2013
(S.I. No. 257 of 2013), (c) a management company authorised in accordance with the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 or otherwise in accordance with the Directive of 2009, or (d) an alternative investment fund manager within the meaning of the European Union (Alternative Investment Fund Managers) Regulations 2013.

Competent Authority bodies identified by Sections 60 and 61 of the *2010 Act* as being empowered to supervise the compliance of *individuals* and *accountancy firms* with the *2010 Act*. [or in the case of an *Accountancy firm* the relevant designated accountancy body (e.g. the Institute of Chartered Accountants in Ireland)].

Correspondent relationship (a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services, or (b) the relationships between and among *credit institutions* and *financial institutions* including where

similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

Credit Institution (a) a credit institution within the meaning of point (1) of Article 4(1) of the *Capital Requirements Regulation*, or (b) An Post in respect of any activity that it carries out, whether as principal or agent, that would render it, or a principal for whom it is an agent, a credit institution as a result of the application of paragraph (a).

Criminal conduct conduct that constitutes an offence in Ireland as well as, in certain circumstances, conduct occurring elsewhere that (a) constitutes an offence under the law of that place and would have been an offence if it had taken place in Ireland or (b) would constitute an offence under section 5(1) or 6 (1) of the Criminal Justice (Corruption Offences) Act 2018 if it were to occur in Ireland and the person or official concerned doing the act, or making the omission, concerned in relation to their office, employment, position or business is a foreign official within the meaning of that Act (Section 6 of the *2010 Act*).

Customer Due Diligence (CDD) The process by which information regarding the *or* is gathered, and the identity of a *client* is established and verified, for both new and existing *clients*.

Data Protection Legislation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as implemented in Ireland by the Data Protection Act 2018.

Defined services Activities carried on, in the course of business carried on by *accountancy firms firms* or *individuals* as an auditor, *external accountant*, insolvency practitioner or *tax adviser* or as *trust or company service providers* (eg company secretarial services).

Designated person has the meaning given by section 25 of the *2010 Act* as amended by the *2018 Act*.

EEA European Economic Area. Countries which form the combined membership of the European Union (EU) and the European Free Trade Association (EFTA).

Electronic money means electronic money within the meaning of the European Communities (Electronic Money) Regulations 2011 (S.I. No. 183 of 2011).

Enhanced Due Diligence Additional due diligence steps that must be applied in situations where there is a higher risk of money laundering or *terrorist financing* and in a number of specific situations (Sections 37 and 39 of the *2010 Act*).

EU Directive Refers in this document to the Forth Money Laundering Directive.

External accountant Means a person (an *accountancy firm* or sole practitioner) who by way of business provides *accountancy services* (other than when providing such services to the employer of the person) whether or not the person holds accountancy qualifications or is a member of a designated accountancy body (Section 24 of the *2010 Act*).

External report Report made under Section 42 or 43 of the *2010 Act* to the *FIU Ireland* and the Revenue Commissioners.

FATF Financial Action Task Force. Created by G7 nations to fight money laundering.

Financial institution has the meaning given by Section 24 of the *2010 Act* as amended by Section 4 of the *2018 Act*.

FIU Ireland means those members of the Garda Síochána, or members of the civilian staff of the Garda Síochána, appointed by the Commissioners of the Garda Síochána who may carry out all the functions of an EU Financial Intelligence Unit under the Fourth Money Laundering Directive (Section 40A of the *2010 Act*).

Group means a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.

High-risk third country those jurisdictions identified by FATF, EU law or by other authoritative sources. Such jurisdictions identified by the EU as at February 2019 consist of the following:

- Afghanistan
- American Samoa
- The Bahamas
- Botswana
- Democratic People's Republic of Korea
- Ethiopia
- Ghana
- Guam
- Iran
- Iraq
- Libya
- Nigeria
- Pakistan
- Panama
- Puerto Rico
- Samoa
- Saudi Arabia
- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- US Virgin Islands
- Yemen

Immediate family member of a politically exposed person includes any of the following persons:

(a) any spouse of the politically exposed person;

(b) any person who is considered to be equivalent to a spouse of the politically exposed person under the national or other law of the place where the person or politically exposed person resides;

(c) any child of the politically exposed person;

(d) any spouse of a child of the politically exposed person;

(e) any person considered to be equivalent to a spouse of a child of the politically exposed person under the national or other law of the place where the person or child resides;

(f) any parent of the politically exposed person;

(g) any other family member of the politically exposed person who is of a prescribed class.

Individuals Includes the partners, directors, subcontractors, consultants and employees of *accountancy firms*.

Internal report A report made internally by an *individual* in accordance with procedures established by the *accountancy firm*.

Money laundering offences As defined in Section 7 of the *2010 Act,* a person commits a *money laundering offence* by:

- concealing or disguising the true nature, source, location, disposition, movement or ownership of criminal property, or any rights relating to the property;
- converting, transferring, handling, acquiring, possessing or using the criminal property; or
- removing the criminal property from, or bringing the property into, the State.

Other offences involve money laundering outside the State in certain circumstances (Section 8), attempts outside the State to commit offences in the State (Section 9) and aiding, abetting, counselling or procuring outside the State commission of offence in the State (Section 10).

Irish AML Regime Irish anti-money laundering and *terrorist financing* regime.

MLRO Money *laundering reporting officer*: an individual designated as having responsibility for oversight of an *accountancy firm's* anti-money laundering and reporting procedures.

MLTF (money laundering and terrorist financing) Defined for the purposes of this document to include those offences relating to terrorist financing as defined under section 13 of the Criminal Justice (Terrorist Offences) Act 2005 as well as the money laundering offences defined by sections 6 to 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

Money laundering reporting officer See *MLRO*, above.

Monitoring in relation to a *business relationship* between a *designated person* and a customer, means the *designated person*, on an ongoing basis (a) scrutinising transactions, and the source of wealth or of funds for those transactions, undertaken during the relationship in order to determine if the transactions are consistent with the *designated person's* knowledge of (i) the customer,
(ii) the customer's business and pattern of transactions, and (iii) the customer's risk profile (as determined under section 30B), and (b) ensuring that documents, data and information on customers are kept up to date in accordance with its internal policies, controls and procedures adopted in accordance with section 54.

Occasional transaction means, in relation to a customer of a *designated person* where the *designated person* does not have a *business relationship* with the customer, a single transaction, or a series of transactions that are or appear to be linked to each other, and

(a) in a case where the *designated person* concerned is a person referred to in section 25(1)(h), that the amount of money or the monetary value concerned (i) paid to the *designated person* by the customer, or (ii) paid to the customer by the *designated person*, is in aggregate not less than €1,000,

(b) in a case where the transaction concerned consists of a transfer of funds (within the meaning of Regulation (EU) No. 2015/847 of the European Parliament and of the Council of 20 May 2015) that the amount of money to be transferred is in aggregate not less than €1,000,

(bb) in a case where the *designated person* concerned is a person referred to in section 25(l)(i), that the amount concerned (i) paid to the *designated person* by the customer, or (ii) paid to the customer by the *designated person*, is in aggregate not less than €10,000, and

(c) in a case other than one referred to in paragraphs (a), (b), or (bb), that the amount or aggregate of amounts concerned is not less than €10,000.

PEPs Politically exposed persons. As defined in section 37 of the *2010 Act* as amended by the *2018 Act* to include domestic PEPs and immediate family members of a PEP.

Predicate offence means the underlying offence or any offence as a result of which *criminal property* has been generated.

Prejudicing an investigation A 'related' *money laundering offence*, defined under section 49 of the *2010 Act*. It involves the making of any disclosure that is likely to prejudice an investigation.

Proceeds of criminal conduct Any property that is derived from or obtained through *criminal conduct* whether directly or indirectly, or in whole or in part (section 6 of *2010 Act*).

Professional privilege reporting exemption an exemption from reporting suspicions formed on the basis of information received in privileged circumstances (see section 6.4 of this Guidance).

Public body means an FOI body within the meaning of the Freedom of Information Act 2014.

Regulated market (a) A regulated market with the meaning of point (21) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, located within the *EEA*, or (b) a regulated market that subjects companies whose securities are admitted to trading to disclosure obligations which are equivalent to the following: (i) disclosure obligations set out in Articles 17 and 19 of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, (ii) disclosure obligations consistent with Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectuses to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC, (iii) disclosure obligations consistent with Articles 4 to 6, 14, 16 to
19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, and (iv) disclosure requirements consistent with EU legislation made under the provisions mentioned in subparagraphs (i) to (iii).

Relevant independent legal professional A relevant independent legal professional shall be a *designated person* only as respects the carrying out of the services specified in the definition of 'relevant independent legal professional' in section 24(1).

Relevant professional adviser Defined in Section 24 of the *2010 Act* as an accountant, auditor or *tax adviser* who is a member of a designated accountancy body or of the Irish Taxation Institute.

Required disclosures The requirement under Section 42(6) of the *2010 Act* to disclose (a) information on which the knowledge, suspicion or reasonable grounds are based; (b) the identity, if known, of the person known or suspected to be or have been engaged in an offence of *money laundering* or *terrorist financing*; (c) the whereabouts, if known, of the criminal property; and (d) any other relevant information. Section 42(6A) requires a *designated person* who is required to make a report under this section to respond to any request for additional information by *FIU Ireland* or the Revenue Commissioners as soon as practicable after receiving the request and to take all reasonable steps to provide any information specified in the request.

STR Suspicious transaction report (see below).

Senior management means an officer or employee with sufficient knowledge of the institution's money laundering and *terrorist financing* risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a partner of the firm concerned or a member of the management board.

Shell bank means a *credit institution* or *financial institution* (or a body corporate that is engaged in activities equivalent to those of a *credit institution* or *financial institution*) that— (a) does not have a physical presence, involving meaningful decision making and management, in the jurisdiction in which it is incorporated, (b) is not authorised to operate, and is not subject to supervision, as a *credit institution*, or as a *financial institution*, (or equivalent) in the jurisdiction in which it is incorporated, and (c) is not affiliated with another body corporate that— (i) has a physical presence, involving meaningful decision-making and management, in the jurisdiction in which it is incorporated, And (ii) is authorised to operate, and is subject to supervision, as a *credit institution*, a *financial institution* or an insurance undertaking, in the jurisdiction in which it is incorporated.

Suspicious transaction report: a report concerning suspicions of money laundering or terrorist financing made in accordance with section 42 of the *2010 Act* (also referred to as a *STR* (see above).

Statutory Auditor means an individual or firm who is approved in accordance with the Companies Act 2014, as amended by the Companies (Amendment) Act 2018.

Tax adviser means a person who by way of business provides advice about the tax affairs of other persons (Section 24 of *2010 Act*).

Terrorist financing means an offence under Section 13 of the *2005 Act*, which states:

"…a person is guilty of an offence if, in or outside the State, the person by any means, directly or indirectly, unlawfully and wilfully provides, collects or receives funds intending that they be used or knowing that they will be used, in whole or in part in order to carry out—

(a) An act constitutes an offence under the law of the State and within the scope of, and as defined in, any treaty that is listed in the annex to the Terrorist Financing Convention, or

(b) An act (other than one referred to in paragraph (a) —

  i. That is intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, and

  ii. The purpose of which is, by its nature or context, to intimidate a population or to compel a government or an international organisation to do, or abstain from doing, any act.

The offence also encompasses providing, collecting or receiving funds whilst knowing or intending that they will be used for the benefit or purposes of a terrorist group or to carry out other *terrorist offences* under Section 6 of the *2005 Act*. Attempting to commit the above offences is also an offence.

Terrorist offences Section 6 of the *2005 Act* defines *terrorist offences*, incorporating:

- terrorist activity (defined as an act that is committed in or, in certain circumstances, outside the State and that (a) if committed in the State, would constitute an offence specified in Part 1 of Schedule 2 [of the 2005 Act], and (b) is committed with the intention of (i) seriously intimidating a population, (ii) unduly compelling a government or an international organisation to perform or abstain from performing an act, or (iii) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a state or an international organisation); and

- terrorist-linked activity (defined as (a) an act that is committed in or, in certain circumstances, outside the State and that (i) if committed in the State, would constitute an offence specified in Part 2 of Schedule 2, and (ii) is committed with a view to engaging in a terrorist activity, (b) an act that is committed in or, in certain circumstances, outside the State and that (i) if committed in the State, would constitute an offence specified in Part 3 of Schedule 2, and (ii) is committed with a view to engaging in a terrorist activity or with a view to committing an act that, if committed in the State, would constitute an offence under section 21

or 21A of the Act of 1939, (c) public provocation to commit a *terrorist offence*, (d) recruitment for terrorism, or (e) training for terrorism.

Tipping off See *prejudicing an investigation.*

Transaction The provision of any service by an *accountancy firm* or *individual* to a *client* by way of business, or the handling of *client's* finances by way of business. Section 24 of the *2010 Act* defines transactions in the context of different '*designated persons*', including:

"(a) in relation to a professional service provider, any transaction that is carried out in connection with a customer of the provider and that is –

(i) in the case of a provider acting as an auditor, the subject of an audit carried out by the provider in respect of the accounts of the customer,

(ii) in the case of a provider acting as an *external accountant* or *tax adviser*, or as a *trust or company service provider*, the subject of a service carried out by the provider for the customer, or

(iii) in the case of a provider acting as a *relevant independent legal professional*, the subject of a service carried out by the professional for the customer of a kind referred to in paragraph (a) or (b) of the definition of "*relevant independent legal professional*" in this subsection;

and

(b) in relation to a casino or private members' club, a transaction, such as the purchase or exchange of tokens or chips, or the placing of a bet, carried out in connection with gambling activities carried out on the premises of the casino or club by a customer of the casino or club."

Trust or company service provider means any person whose business it is to provide any of the following services as defined under Section 24 of *2010 Act*.

Vested interest Is an interest to which an entitlement already exists (whether immediately – 'in possession'; or in the future, following the ending of another interest – 'in remainder' or 'in reversion'). It is in contrast to an interest which is merely 'contingent'; a contingent interest is an interest which will only arise on the happening of a particular event, such as surviving to a particular date or surviving a particular person. Determining whether an interest is vested or contingent requires careful analysis. For example, if a trust provides that A has a life interest, and that B has an interest which takes effect on A's death, both A and B will have vested interests and, if B does not survive A, B's interest will devolve as part of B's estate; however, if B's interest is expressed to take effect on A's death only if he (B) is then living, B's interest (which will fail if he predeceases A) is merely contingent.

A *defeasible interest* is one which may be defeated, generally by the exercise of a power under the trust deed; an indefeasible interest is one which cannot be defeated. In the examples given above, A and B both have indefeasible interests. It is important that a defeasible vested interest is not mistaken for contingent interest. A defeasible vested interest will take effect unless and until it is defeated; a contingent interest on the other hand will not take effect unless and until the event on which it is contingent arises.

APPENDIX A: OUTSOURCING, SUBCONTRACTING AND SECONDMENTS

A.1 Outsourcing and subcontracting arrangements

A.1.1 Where an *accountancy firm* chooses to outsource or subcontract work to a third party it is still obliged to maintain appropriate risk management procedures to prevent *MLTF*. This also requires the *firm* to consider whether the outsourcing or subcontracting increases the risk that it will be involved in, or used for, *MLTF*, in which case appropriate controls to address that risk should be put in place.

A.1.2 Where a *firm* contracts with a *client*, it remains responsible for ensuring that it undertakes *CDD* to Irish standards, including maintaining the appropriate records even if execution of all or part of the *client* work is outsourced or sub-contracted out. Some aspects of *CDD,* such as collecting documentary evidence, can also be delegated to an outsourcer or sub-contractor, but the *firm* remains responsible for compliance with Irish legislation.

A.1.3 Regardless of any outsourcing or subcontracting arrangement, a *firm* remains responsible for reporting any knowledge or suspicion of *MLTF* that comes to it in the course of its own activities. However a *firm* is not responsible for reporting knowledge or suspicion that comes to the attention of the outsourcer or sub-contractor, where such knowledge or suspicion has not been passed on to the *firm*. Subcontractors are subject to the reporting requirements of the *2010 Act* by virtue of section 41: however there is no legal obligation for an outsourcer or subcontractor to report knowledge or suspicion of *MLTF* to a *firm. Firms* may wish to establish a *MLTF* reporting protocol in the terms of engagement agreed with the subcontractor concerned. If an *STR* is made by the sub-contractor, the *firm* should consider its own reporting obligations. When a sub-contractor is integrated into an Irish business it may be appropriate for its staff to be trained in the *MLTF* procedures adopted by that *firm* so that common standards can be observed.

A.2 Secondees and those temporarily working outside of Ireland

A.2.1 A secondee is an individual legally employed by one organisation (the seconder) but acting as an employee of another. The formal terms of all secondments should make clear to all concerned how the secondee's legal obligations will be applied.

A.2.2 The position of a secondee working temporarily outside of Ireland or on foreign secondments but still within an Irish *firm* is difficult. For example the duty to report *MLTF* suspicions may be influenced by the terms of the secondment. Issues to consider include:

- If the work outside of Ireland is part of an Irish *defined service* then in some circumstances the *MLTF* suspicion will be reportable;
- an *individual* should be particularly cautious about any decision not to make a *STR* in accordance with the secondee's legal employer's procedures if the information relates to work that they are undertaking in Ireland or to an entity incorporated, or an individual resident, in Ireland.

A.2.3 Arrangements must be considered on their own facts to determine which policies and procedures the secondee should follow. *Accountancy firms* may wish to take legal advice in relation to the need for their relevant employees to comply with the Ireland's money laundering reporting regime as well as any local legal requirements, and in relation to the drafting of appropriate secondment agreements.

A.3 Reporting requirements for subcontractors

A.3.1 Where all or part of a piece of work is contracted-out to a subcontractor there is no legal requirement for the subcontractor to report suspicious *transactions* to the referring *firm's MLRO*, although this may be addressed in the engagement terms agreed by the *firm* with the subcontractor concerned. Whether or not such reporting is agreed between the parties, where the subcontractor notifies the referring *firm* of information which gives rise to a *MLTF* suspicion, the referring *firm* must consider its own reporting obligations.

APPENDIX B: *CLIENT* VERIFICATION

As discussed in section 5 of this guidance, documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the *2010 Act*, or to equivalent legislation; then
- those issued by other organisations.

B.1 Individuals

***Client* identification:**

B.1.1 The full name, date of birth and residential address should be obtained.

***Client* Verification:**

B.1.2 A document issued by an official (e.g., government) body is deemed to be independent and reliable source even if provided by the *client*. Documents should be valid and recent. Documents sourced online should not be accepted if there is any suspicion regarding the provenance of the documents. The following is a suggested non-exhaustive list of sources of evidence.

Risk profile	Verification
Normal risk	The original, or an acceptably certified copy, of one of the following documents or similar should be seen and a copy retained: • valid passport • valid photo card driving licence • national Identity card
Higher risk	The original of a second document should be seen and a copy retained. This should be one of the following: • Recent evidence of entitlement to a state- or local authority-funded benefit (including housing benefit, council tax benefit, tax credits, state pension, educational or other grant). • Instrument of a court appointment (such as a grant of probate). • Documents issued by the Revenue Commissioners, such as PAYE coding notices and statements of account (NB: employer issued documents such as P60s are not acceptable). • End of year tax deduction certificates. • Current (within last 3 months) bank statements or credit/debit card statements issued by a regulated financial sector firm in Ireland, EU or designated place under Section 31. • Current utility bills. • An electoral register search showing residence in the current or most recent electoral year (can be done via http://www.checktheregister.ie/. • A solicitor's letter confirming recent house purchase or land registry confirmation (you should also verify the previous address).

Source of wealth and source of funds

B.1.3 Where appropriate, evidence can be obtained from searching public information sources like the internet, company registers and land registers.

B.1.4 If the *client*'s funds/wealth have been derived from, say, employment, property sales, investment sales, inheritance or divorce settlements, then it may be appropriate to obtain documentary proof.

B.2 Private companies

Client identification

B.2.1 The following information must be obtained and verified:

- full name of company
- registered number
- registered office address and, if different, principal place of business
- any shareholders/members who ultimately own or control more than 25% of the shares or voting rights (directly or indirectly including bearer shares), or any individual who otherwise exercises control over management must be identified (and verified on a risk sensitive basis).
- The identity of any agent or intermediary purporting to act on behalf of the entity and their authorisation to act e.g., where a lawyer engages on behalf of an underlying *client*.

Unless the entity is listed on a *regulated market*, reasonable steps should be taken to determine and verify:

- the law to which it is subject
- its constitution (for example via governing documents)
- the full names of all directors (or equivalent) and senior persons responsible for the operations of the company.

Company registers of beneficial ownership may be used but not solely relied upon.

B.3 Listed or regulated entity

Client identification

B.3.1 The following information should be gathered:

- full name
- membership or registration number
- address

Client verification

Risk Profile	Recommended verification
Normal/ high risk	One of the following documents should be seen and a copy retained: • a printout from the web-site of the relevant regulator or exchange (which should be annotated); • written confirmation of the entity's regulatory or listing status from the regulator or exchange.

B4. Government or similar bodies

Client identification

B.4.1 The following information should be gathered:

- full name of the body
- main place of operation
- government or supra-national agency which controls it

Client verification

Risk Profile	Recommended verification
Normal/ high risk	The following information should be obtained and reviewed, and a copy retained: • a printout from the web-site of the relevant body (which should be annotated). Additionally for housing associations:

	• the printout must contain its registered number, registered company number (where appropriate) and registered address.

APPENDIX C: *STR* REPORTING PROCESS CHECKLIST

Should I report to the MLRO?		**As the MLRO, should I report externally?**
• Do I have knowledge or suspicion of criminal activity resulting in someone benefitting? • Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of money laundering? • Do I know or suspect a person or persons of being involved in crime? • Do I think that the person(s) involved in the activity knew or suspected that the activity was criminal? • Can I explain my suspicions coherently? In making a report to the MLRO, consider whether you are aware of information as to who might have received the benefit of the criminal activity, or where the criminal property might be located, based on information obtained in the conduct of firm's business.		• Do I know, suspect or have reasonable grounds to know or suspect that another person is or was engaged in money laundering; **and** • Did the information or other matter giving rise to the knowledge or suspicion come to me in an internal STR? • Was the information scrutinised in the course of reasonable business practice? • Does the privileged circumstances exemption apply (see section 6.4)?

CHECKLIST: Essential elements of an external SAR – to be submitted using GoAML and copied to the Revenue Commissioners in hard copy

- Name of reporter;
- Date of report;
- Who is suspected or any information available to the *accountancy firm* or individual making the report that may assist in ascertaining the identity of the suspect (which may simply be details of the victim and the fact that the victim knows the identity but this is not information to which the firm is privy in the ordinary course of its work). The reporter should provide as many details as possible to allow *FIU Ireland* to identify the main subject; together with (*continued overleaf)*
- Who is otherwise involved in or associated with the matter and in what way.
- The facts;
- What is suspected and why;
- Any information available to the *accountancy firm* or individual regarding the whereabouts of any criminal property or information that may assist in ascertaining it.
- Reports should generally be jargon free and written in plain English.

APPENDIX D: RISK FACTORS

High risk factors

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY HIGHER RISK

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in subparagraph (3);

(c) non-resident customers;

(d) legal persons or arrangements that are personal asset-holding vehicles;

(e) companies that have nominee shareholders or shares in bearer form;

(f) businesses that are cash intensive;

(g) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

(3) Geographical risk factors:

(a) countries identified by the EU as having strategic deficiencies in their regime for countering money-laundering and terrorist financing. As of 13 February 2019, 23 jurisdictions had been identified by the EU process, which takes into account *FATF* assessments: the list and commentary is available on the Europeans Commission website here

(b) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to combat *MLTF*;

(c) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(d) countries subject to sanctions, embargos or similar measures issued by organisations such as, for example, the European Union or the United Nations;

(e) countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country."

Low risk factors

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY LOWER RISK

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises;

(c) customers that are resident in geographical areas of lower risk as set out in subparagraph (3).

(2) Product, service, transaction or delivery channel risk factors:

(a) life assurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

APPENDIX E: DIRECTIONS FROM GARDA SIOCHAN OR COURT REGARDING PROCEEDING WITH A TRANSACTION OR SERVICE

E1 Directions not to proceed

E1.1 Under Section 17(1), a member of the Garda Síochána, who has a rank "not below the rank of superintendent", may direct a person, in writing, not to proceed with a particular service or *transaction* for the period specified in the direction, not to exceed seven days.

E1.2 An order to proceed may also be made by the District Court. Details of relevant circumstances and processes to be followed in relation to such orders are set out in

E1.3 The direction:

- may, but is not required to be, issued on foot of a report made by an *accountancy firm* under Section 42 of the *2010 Act*;
- is made on the basis that the member of the Garda Síochána is satisfied that the direction is reasonably necessary to allow preliminary investigations to be carried out to establish whether or not there are reasonable grounds to suspect that the service or *transaction* would comprise or assist in money laundering or *terrorist financing.*

E2 Order from a judge of the District Court not to proceed

E2.1 Section 17(2) of the *2010 Act* also provides for an order from a District Court Judge not to proceed with a specified service or *transaction* for the period specified in the order, not to exceed 28 days. However, such orders may be made on more than one occasion, in accordance with Section 17(3) of the *2010 Act*.

E.2.2 In making such an order, the District Court Judge is satisfied by information provided on oath by a member of the Garda Síochána that:

- There are reasonable grounds to suspect that the service or *transaction* would comprise or assist *money laundering* or *terrorist financing*, and
- An investigation of a person for that *money laundering* or *terrorist financing* is taking place.

E.2.3 Applications for an order by a District Court Judge are made to a judge of the District Court in the district where the order is to be served (Section 17(4) of the *2010 Act*).

E3 Directions and orders - compliance; notice

E.3.1 Failure to comply with a direction of the Garda Síochána or an order from a judge of the District Court is an offence. Any person acting in compliance with a direction or order will not be treated as having breached any requirement or restriction imposed by any other enactment or rule of law.

E.3.2 Section 18(1) of the *2010 Act* obliges the member of the Garda Síochána, who issues the direction or applies to the District Court for the order, to give notice in writing to any person, whom he knows to be affected by the direction or order, as soon as practicable after the direction is given or order is made, unless:

- it is not reasonably practicable to ascertain the whereabouts of the person; or
- there are reasonable grounds for believing that disclosure would prejudice the investigation.

E3.3 If the member of the Garda Síochána becomes aware that a person who is affected by the direction or order is aware of the direction or order, then the member of the Garda Síochána is obliged to inform him in writing as soon as practicable thereafter of the direction or order, notwithstanding the above provision about *prejudicing the investigation* (Section 18(2)) of the *2010 Act*.

E3.4 The notice in writing shall include the reasons for the direction or order and advise the person of their rights to apply the District Court:

- (under Section 19 of the *2010 Act*) for a revocation of the direction or order; or
- (under Section 20of the *2010 Act*) for an order to in relation to any of the property concerned (a) to discharge reasonable living expenses and other necessary expenses of the person and/or the person's dependents or (b) to carry on a business, trade, profession or other occupation to which any of the property relates.

E3.5 Under Section 19 of the *2010 Act*, a judge of the District Court may revoke a direction or order on application by a person affected by the direction/order, if satisfied that the grounds for the direction/order do not, or no longer, apply.

E3.6 The direction or order ceases to have effect on the cessation of the investigation. As soon as practicable thereafter, a member of Garda Síochána is obliged to inform, in writing, both the person who received the direction or order and any other person whom the member is aware is affected by the direction or order.

E4 Authorisation from the Garda Síochána to proceed

E4.1 A member of the Garda Síochána, not below rank of superintendent, may authorise, in writing, a person to proceed with a service or *transaction*, which would otherwise comprise or assist *money laundering*, if the member is satisfied that to do so is necessary for the purposes of the investigation (Section 23 of the *2010 Act*).

E5 Suspension of Activity

E5.1 Once a direction or order has been received, the process must be adhered to and the activity that would otherwise be a *money laundering* or *terrorist financing* offence refrained from until the notice period has expired or notice in writing has been received that the direction or order has ceased to have effect. Failure to do so risks prosecution either for a *money laundering* or *terrorist financing* offence, which is punishable by imprisonment and/or a fine.

E5.2 Section 50 of the *2010 Act* provides a defence against the offence of making a disclosure which prejudices an investigation where disclosure is made to a *client* that the defendant (the *accountancy firm*) was directed by the Garda Síochána or ordered by a judge of the District Court not to carry out any specified service or *transaction* in respect of the *client*. Disclosure must be made only to the *client* and must be solely to the effect that the *accountancy firm* has been so directed / ordered.