TR 01 2019

Anti-Money Laundering Guidance

(Updated March 2022 and July 2026)

Guidance only and Disclaimer

Chartered Accountants Ireland is the operating name of the Institute of Chartered Accountants in Ireland, and the operating name Chartered Accountants Ireland is used hereafter throughout the disclaimer and the guidance.

Readers are advised that anti-money laundering obligations of designated persons derive from law. This guidance signposts obligations of accountants in this area but should not be regarded as a definitive legal interpretation. The law is complex and open to different interpretations and in some instances not particularly well drafted. It also changes fast and is ever evolving. This publication is guidance only and does not purport to provide definitive legal interpretation(s) or opinion(s) on the applicable legislation or other legal matters referred to in the guidance or relevant to anti-money laundering. If the reader is in doubt on any matter in this complex area, they should consider obtaining legal advice. Any examples, diagrams, infograms or charts provided are illustrative only and provided in good faith to guide and assist the reader in understanding the obligations in this area but do not purport to be and must not be relied upon by the reader as a definitive legal interpretation.

This publication is designed to provide accurate and authoritative information and guidance on the subject matter covered. It is provided on the understanding that neither Chartered Accountants Ireland or the Association of Chartered Certified Accountants is engaged in rendering professional services and each disclaims all liability for any reliance placed on the information contained within this publication and recommends that if professional advice or other expert assistance is required, the services of a competent professional should be sought.

The content of this publication is provided as a guide only and does not purport to give professional advice or a legal interpretation. 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 Chartered Accountants Ireland and the Association of Chartered Certified Accountants 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. Chartered Accountants Ireland and the Association of Chartered Certified Accountants 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, Chartered Accountants Ireland and the Association of Chartered Certified Accountants 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 Chartered Accountants Ireland and the Association of Chartered Certified Accountants, 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, Chartered Accountants Ireland and the Association of Chartered Certified Accountants 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 Chartered Accountants Ireland and the Association of Chartered Certified Accountants in respect of any inaccurate, mistaken or negligent misstatement or omission contained in this publication.

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.

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 working party comprising staff and volunteer practitioners of the Chartered Accountants Ireland and the Association of Chartered Certified Accountants.

This guidance is based on the law as of **31 January 2026.** 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 (if regulated for this service by an accounting body) in the Republic of Ireland.

Contents

1. ABOUT THIS GUIDANCE

2026 Updates of Anti-Money Laundering Guidance

This guidance has been updated in 2026 and some of the main changes are described below.

Sanctions

Since the last publication of the guidance in 2022, the area of sanctions has increased in importance. This is at least partly because of the sanctions imposed since the Russian invasion of Ukraine and partly since the adoption of AMLD 6 by the European Union. The sanctions provisions in the AML Regulation passed under AMLD 6 effectively brings sanctions compliance into firms' AML framework. Readers can read more about sanctions, including sanctions internal controls in Chapters 5 and 11 of the guidance.

Proliferation financing

Proliferation financing is a concept that is not yet firmly established Irish law. While detailed advice on the area is outside the scope of the guidance, there is some coverage included to heighten members awareness of proliferation financing and the risks associated with it.

Outsourcing and reliance

The guidance contains a **r**efreshed and expanded chapter (10) on outsourcing and reliance. This content was previously covered (to a lesser extent) in Chapter 5. The updated guidance highlights differences between reliance on relevant third parties and outsourcing to a third-party service provider and procedures and controls to be put in place to manage outsourcing and reliance arrangements. Controls include the establishment of a written agreement between the designated entity and the relevant third party (in the case of reliance) or the third-party service provider (in the case of outsourcing).

The updated guidance also includes details of points to consider when managing suspicious transaction reporting where reliance and/or outsourcing arrangements are established. Subcontracting considerations are also included at the end of chapter 10 given subcontracting arrangements are frequently used by member firms.

Verification, electronic solutions, meaning of "non-face to face"

Methods of client verification continue to develop in a digital age. The updated guidance considers automated compliance solutions, electronic identification, and non-face-to-face situations. The guidance offers a description of what non-face-to-face means and additional checks which might be done in non-face-to-face situations.

The guidance also now contains a link to PRADO. This site allows review of the formats of identification documents from most jurisdictions in the world, for the purposes of customer due diligence. This will be useful for any practitioner who needs to do customer due diligence on a potential foreign client.

Appendix B of the guidance on client verification has been refreshed. It considers when it might be useful depending on the circumstances to get details of nationality, place of birth or country of residence of a client. It also contains some narrative on listed entities and new content is included on verification when onboarding charities.

Trust or Company Service Providers

TCSPs is an area that has come under increased scrutiny in recent years. A short section has been included in the guidance on TCSPs. Readers can also refer to the Irish Trust or Company Service Providers Risk Assessment published in 2022 for further information.

Europe's AMLD 6 Regime

Probably the biggest single change since the last update of the guidance in 2022 is the adoption by the European Union of the 6th Anti Money laundering package (AMLD 6). This entered into force in July 2024. Most of the provisions of AMLD 6 commence in 2027. The regulation 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing will be directly effective in Ireland. The provisions of Directive 2024/1640 must be transposed into Irish law by July 2027.

The guidance deals with aspects of the future of the Irish regime from 2027. The Institute published a technical alert in December 2025 TA 05/2025, which contained an outline of selected changes under the European Union 6th Anti-Money Laundering Package. This is replicated and integrated into chapter 11 of the guidance.

Some of the changes to take note of include:

- More detailed requirements for customer due diligence (CDD) procedures.
- EU Ban on cash payments over €10,000.
- More closely defined AML roles, governance structures, and internal control framework.
- An independent audit function within entities or the possibility to outsource this to an external expert.
- New outsourcing rules and outsourcing prohibitions.
- Wider definition of a Politically Exposed Person (e.g. to include the siblings of PEPs in certain cases).
- More detailed beneficial ownership provisions.

Other

More content is added by way of guidance on firms' policies and procedures. This includes annual review and refresh of AML policies and procedures. It also makes clear that business-wide risk assessments (BWRAs) should be done at least annually. Some content has been added concerning risks in fragmentation of services (where a client uses different firms for different services), suspicious transaction reporting in group audit situations, and updates are made in section 8 in relation to training.

Updates regarding monitoring the adequacy and effectiveness of AML policies, procedures, and processes are also included, highlighting that effectiveness

reviews should be performed via an annual Money Laundering Compliance Review (MLCR). Other more minor updates include updates to the non-exhaustive listing of relevant anti money laundering legislation, both primary legislation and statutory instruments and some new definitions added into the glossary particularly due to AMLD 6 and proliferation financing.

The following paragraphs consider:

- What is the purpose of this guidance?
- Who is this 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 subsequent legislation including the Criminal Justice Act 2013, 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) and the Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2021 and related statutory instruments which give effect to the provisions of the Fifth Money Laundering Directive (Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018) and to provide for related matters.

1.1.2 In this document, the '2010 Act' has the meaning given to it in the Glossary.

1.1.3 Key changes introduced by the amending Acts of 2018 and 2021 include greater emphasis on identification of beneficial owners of businesses, expanding the definition of *tax adviser* in the definition of "designated person" and providing a wider definition of politically exposed persons (PEP). The 2021 Act expands the definition of a PEP to include any individual performing a prescribed function (see further on *PEPs* at 5.3.13 below), introduces a requirement to apply procedures based on an enhanced risk-based approach to assess and respond to potential money laundering or *terrorist financing*, and introduces enhanced requirements relating to client identification. While the 2018 Act removes 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, the 2021 Act now includes a specific list of *enhanced due diligence* measures that the designated person is required to apply when dealing with a customer established, or residing, in a *High-risk third country*. In addition, since the last update of this guidance, the area of sanctions regulations and associated compliance has increased in importance given the sanctions regime introduced by the EU against Russia. Subject to our "Guidance only and Disclaimer "provisions, 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 2010 (see paragraph 1.2.1) to fulfil their obligations under the updated Irish legislation to prevent, recognise and report money

laundering and *terrorist financing*. Compliance with it will assist compliance with the relevant legislation (including that related to counter *terrorist financing*) and professional requirements.

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

1.1.5 The term 'must' is used throughout to indicate a mandatory legal or regulatory requirement.

1.1.6 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.

1.1.7 The Irish anti-money laundering regime applies only to *defined services* carried out by designated *persons*. 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*.

1.1.8 This guidance takes account, where relevant, of guidance issued by bodies other than Chartered Accountants Ireland and the Association of Chartered Certified Accountants. When those bodies revise or replace their guidance, the references in this document should be assumed to refer to the latest versions.

1.1.9 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 1.1.6 of this guidance) be in a position to explain this reliance to their *competent authority*. The law which comprises the Irish AML regime is largely contained in the following legislation and relevant statutory instruments (S.I.s). The listing of legislation below is provided as a guide for readers but does not purport to be definitive or exhaustive:

1.1.10

Legislation:

- Criminal Justice (*Terrorist Offences*) Act 2005 (as amended)
- Criminal Justice (*Terrorist Offences*) Amendment Act 2015
- Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010
- Criminal Justice Act 2011
- Criminal Justice Act 2013, Part 2;
- Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2018
- Criminal Justice (Corruption Offences) Act 2018

- Investment Limited Partnerships (Amendment) Act 2020
- Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2021 ("2021 Act")
- Criminal Justice (Theft and Fraud Offences) (Amendment) Act 2021

Statutory Instruments:

- Commencement orders
- S.I. No. 342 of 2010 Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (Commencement) Order 2010
- S.I. 486 of 2018 Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2018 (Commencement) Order 2018
- S.I. 298 of 2018 Criminal Justice (Corruption Offences) Act 2018 (Commencement) Order 2018
- S.I. 188/2021 Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2021 (Commencement) Order 2021
- Other statutory instruments
- S.I. No. 348 of 2010 *Trust or Company Service Provider* (Authorisation) (Fees) Regulations 2010
- S.I. No. 347 of 2012 Criminal Justice (Money Laundering and *Terrorist Financing*) (Section 31) Order 2012
- S.I. No. 79 of 2014 Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (*Competent authority*) Regulations 2014
- S.I. No. 453 of 2016 Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (*Competent authority* and State *Competent authority*) Regulations 2016
- S.I. No 474/2018 Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2018
- S.I. 487 of 2018 Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018;(added gambling services)
- S.I No 110 of 2019 European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019
- S.I. 578/2019 European Union (Money Laundering and *Terrorist Financing*) Regulations 2019
- S.I.233/2020 European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of *Certain Financial Vehicles*) Regulations 2020
- S.I.194/2021 European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) Regulations 2021 ("Trust Regulations 2021")

- S.I. 321/2021 European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of *Certain Financial Vehicles*) (Amendment) Regulations 2021
- S.I. 387/2021 European Union (Access to Anti-money Laundering Information by Tax Authorities) Regulations 2021
- S.I. No. 46 of 2022 European Union (Anti-Money Laundering: Central Mechanism for Information on Safe-Deposit Boxes and Bank and Payment Accounts) Regulations 2022
- S.I. No. 445/2022 - European Union (Anti - Money Laundering: Central Mechanism for Information on Safe - Deposit Boxes and Bank and Payment Accounts) (Amendment) Regulations 2022
- S.I. No. 704/2022 - European Union (Access to Anti - Money Laundering Information by Tax Authorities) (Amendment) Regulations 2022
- S.I. No. 22/2023 - European Union (Money Laundering and *Terrorist Financing*) (Use of Financial and Other Information) Regulations 2023
- S.I. No. 308/2023 - European Union (Anti - Money Laundering: Beneficial Ownership of Corporate Entities) (Amendment) Regulations 2023
- S.I. No. 607/2024 - European Union (Markets in Crypto-Assets) Regulations 2024
- S.I. No. 724/2024 - Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (Sections 25 and 60) (Prescribed Class and *Competent authority*) Regulations 2024
- S.I. 310/2025 European Union (Information Accompanying Transfers of Funds) Regulations 2025
- S.I. No. 311 of 2025 European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) (Amendment) Regulations 2025
- S.I. 318/2025 European Union (Controls of Cash Entering or Leaving the Union) Regulations 2025
- S.I. 440/2025 European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) (Amendment) (No. 2) Regulations 2025

1.1.11 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.

1.1.12 References to a section in this guidance, unless otherwise stated is to the 2010 Act (as defined in the Glossary).

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 Chartered Accountants Ireland and the Association of Chartered Certified Accountants, 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 or any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance, or advice on tax matters*,*
- and those who act in the course of business as *trust or company service provider*s if regulated for this service by an accounting body in the Republic of Ireland.
- 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.
- 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, *Accountancy Service* is defined in the Glossary.

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

1.2.3 Guidance related to secondees and subcontractors can be found within the guidance.

1.3 What is the legal status of this guidance?

1.3.1 Readers are referred to the "Guidance only and disclaimer" notice at the beginning of this document. This guidance has been prepared to assist accountants fulfil their legal obligations under legislation in force at the time of issue. Since the 2018 Act, persons carrying out a *business risk assessment* must have regard to any guidance on risk issued by the *competent authority* for the designated person. 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 Home Affairs and

Migration for information purposes, and 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?

2.1.1 What is money laundering?

2.1.2 Money laundering is defined in section 7 of the 2010 Act.

A person commits an offence if:

(a) the person engages in any of the following acts in relation to property that is the *proceeds of criminal conduct*:

(i) concealing or disguising the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;

(ii) converting, transferring, handling, acquiring, possessing or using the property;

(iii) removing the property from, or bringing the property into, the State, and

(b) the person knows or believes (or is reckless as to whether or not) the property is the *proceeds of criminal conduct*.

2.1.3 A person who attempts to commit an offence under the above subsection commits an offence.

2.1.4 Money laundering is defined very widely in Irish law. It includes all forms of handling, disguising, layering, transferring, or possessing the *proceeds of criminal conduct*. i.e. for the matter to be money laundering there must not only be criminal conduct but also *proceeds of criminal conduct*. See also paragraphs 7.1.18–7.1.20 below on "criminal conduct".

2.1.5 The '*proceeds of criminal conduct*' is defined in section 6 of the 2010 Act and means any property that is derived from or obtained through criminal conduct, whether directly or indirectly, or in whole or in part, and whether that criminal conduct occurs before, on or after the commencement of the 2010 Act.

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

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

2.1.7 Money laundering can involve the proceeds of offences committed in Ireland but also, in certain circumstances, of conduct overseas. These circumstances

are set out in section 8 of the 2010 Act and include actions that: (i) are an offence in the place where the conduct takes place; and (ii) would have been an offence had it taken place in Ireland or that take place on an Irish ship or an aircraft registered in Ireland. It should also be noted that there is no need for the proceeds to pass through Ireland. Other offences involve attempts outside the State to commit offences in the State (Section 9 of 2010 Act) and aiding, abetting, counselling, or procuring outside the State commission of offence in the State (Section 10 of 2010 Act).

2.1.8 For the purposes of this guidance, except where otherwise stated, money laundering also includes *terrorist financing (*see further at 7.1 below*)*. There are no materiality or 'de minimis' exceptions to *money laundering* or *terrorist financing* (*MLTF*) *offences*.

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

- *Clients*;
- Suppliers;
- Employees; and
- The customers, suppliers, employees and associates (including beneficial owners) of *clients*.

2.1.10 Neither the *firm* nor its *client* needs to have been party to money laundering for a reporting obligation to arise (see Section 7 of this guidance).

2.2 What is the legal and regulatory framework?

2.2.1 Sections 6 to 11 of 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 are 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* (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 an investigation* or *tipping off*, (Section 49 of the *2010 Act*), see Section 7 of this guidance.

2.2.4 In addition, there are reportable offences under 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 9 of this guidance: Training and awareness) 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 and controls 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 *clients*, 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.

3.1.8 The relevant *senior management* responsibilities should be clearly defined.

3.1.9 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 section 54 of the 2010 Act.

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/seniority, 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 directed 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 *clients*
- 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 directed 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 a *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. Where a difficult or contentious AML matter arises in the *Accountancy firm* and this matter cannot be resolved by the firm, the MLRO should ensure that the firm obtains support from a suitable external party to assist the firm in appropriately addressing the matter.

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 (e.g., national risk assessments, supranational risk assessments at European level and *FATF* annual reports) 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, including annual review and refresh of AML policies and procedures
- 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
- monitor 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

AMLD 6 will bring changes to the current provisions in relation to MLROs. Further details of the changes, and additional information required under AMLD 6 are found in Chapter 11 of this guidance document.

3.3 What policies, procedures and controls are required?

3.3.1 The *2010 Act* and regulations including the ones listed in section 1 above place 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*). For information on beneficial ownership registration see section 6 below. The following topics, all of which form part of the *MLTF* framework, need to be considered:

- Risk-based approach, risk assessment and management
- *CDD*
- Non face to face *clients* (see further below)
- record keeping
- internal control
- ongoing *monitoring*
- reporting procedures
- compliance management
- communication
- training and awareness
- confirming beneficial ownership details (Maintenance of an *Internal Register* as well as confirming beneficial ownership details with the relevant Central Register -see section 6 below)

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, at least annually, and updated where necessary, and a written record of this exercise maintained. Where the practice chooses to use a standard policy and procedures template, it is important that this is tailored to the specific circumstances of the firm.

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* wide 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 D to this

guidance.) (e.g. the type of customer, the products and services that are provided etc.). The *AML Regulation* will effect some changes to the "Higher Risk Factors" Annex. 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. The firm-wide risk assessment should at a minimum be reviewed annually (and updated as needed) and that review documented. Following the update of the firm's risk assessment, the firm should consider if any changes to AML policies, procedures, and associated AML internal controls are needed. Resources like the National Risk Assessment for Ireland, (readers should note that a new Money Laundering, *Terrorist Financing*, and *Proliferation Financing* National Risk Assessment 2026 was published in June 2026), 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. See also Guidance for a Risk-Based Approach for the Accounting Profession, non-binding guidance from *FATF*. 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.

3.3.4 Firms must have a policy or procedure in place about verifying *clients* in non-face-to-face situations. Firms should consider an electronic verification/identification method, approved or accepted by the firm and/or the MLRO if it has more than a few non-face-to-face *clients*.

Customer Due Diligence (CDD)

3.3.5 *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*. *CDD* policies and procedures should also include details regarding the firm's client risk scoring methodology in terms of detailing what factors make a customer high, moderate, or low risk, from an AML perspective. 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.

3.3.6 *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

3.3.7 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 7 of this guidance.

Record keeping

3.3.8 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.

3.3.9 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.

3.3.10 *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.

3.3.11 Where directed by a member of An 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*.

3.3.12 *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 8 of this guidance.

Training and awareness

3.3.13 The 2010 Act requires that persons involved in the conduct of the Accountancy firm's business are instructed on the law relating to MLTF and given regular training in how to recognise and deal with suspicious transactions which may be related to MLTF. These provisions should 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. In determining this training plan, current developments in anti-money laundering and associated risks should be considered.

3.3.14 The firm/*MLRO* should establish training capable of ensuring that staff are instructed on the law relating to MLTF as required by the 2010 Act. Staff should:

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

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

3.3.16 Training should be tailored to suit the particular role of the *individual* with an enhanced training requirement for the firm's MLRO.

3.3.17 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.

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

3.3.19 An *Accountancy firm* that fails to provide training for *staff* could be in breach of the *2010 Act* and at risk of prosecution. Failure to provide adequate staff training could mean the firm 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 9 of this guidance.

Monitoring policies and procedures

3.3.20 The *MLRO* and/or appropriate *senior management* should together monitor the adequacy and effectiveness of AML policies, procedures, and processes so that improvements can be made when inefficiencies are found. Effectiveness reviews should be performed via an annual Money Laundering Compliance Review (MLCR). The MLCR should be performed by the MLRO. The annual MLCR should be documented and signed/dated by the MLRO. The MLRO will monitor compliance with any recommendations and corrective measures arising from the annual MLCR. The MLRO will also consider if AML policies and procedures require updating in light of the MLCR findings in addition to communicating results of the annual MLCR to staff. In addition, risks should be monitored and any changes must also be reflected in the firm's AML 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.

3.3.21 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.

Reporting procedures

3.3.22 There are two types of reporting procedures or "whistleblowing" mechanisms - internal within the designated person /firm and externally to the *competent authority*. (This is separate to reporting of suspicious *transactions* or activity dealt with at Section 7 below.)

(a) Internal reporting procedure

The European Union (Money Laundering and *Terrorist Financing*) Regulations 2019 (578/2019) has a requirement that an accounting firm has an internal reporting procedure to allow staff to report a contravention of the anti-money laundering regulations internally through a specific, independent, and anonymous channel, proportionate to the nature and size of the designated person concerned. This should serve to improve AML policies, controls, and procedures, and better understand where problems can arise. When changes are made to policies, procedures, or processes these should be

properly communicated to staff and supported by appropriate training where necessary.

*Accountancy firm*s should consider how this requirement is best achieved in the firm. In making such considerations the firm may take into account the following matters:

- Size of the firm
- Structure of the firm
- Number of branches/offices
- Staffing structures and arrangements.

It would be expected that the internal reporting procedure in place for a larger and more complex firm would be different to that of a smaller and less complex firm. Firms should consider how best they can meet the requirements of the 2019 regulations whilst remaining proportionate to the size of the firm. It would be desirable that the individual to whom internal reports of contraventions of *AML Regulation*s are made should be someone other than the MLRO (for example an individual on the risk management team or on the "in-house" legal team) as there may be a perceived lack of independence in investigating contraventions of AML legislation in the firm given their responsibilities to manage AML compliance in the firm. However, this may not be possible in some smaller firms.

(b) External reporting procedure

Under the 2010 Act a *competent authority* must also establish effective and reliable mechanisms to encourage the reporting of potential and actual breaches of the 2010 Act. Each *competent authority* must provide one or more secure communication channels for persons reporting the matters referred to above, and each *competent authority* must ensure that the channels of communication referred to can also be used by persons to report any threats or retaliatory or hostile actions they are subjected to, for reporting suspected breaches of the 2010 Act.

This external mechanism is available to individuals which could include members of the public or employees within firms if they cannot make use of the internal whistleblowing option.

Should you suspect that a firm supervised by the *competent authority* for ML/TF purposes is not complying with AML legislation you may contact the *competent authority* via its AML confidential disclosure form. You do not have to disclose your personal details, although should the *competent authority* wish to clarify any information, contact details would be helpful.

(c) *Notification of certain offences to Competent authority*

Reference is also made to section 63A of the 2010 Act. This subsection requires competent authorities such as Chartered Accountants Ireland or Association of Chartered Certified Accountants to take the necessary measures to prevent persons convicted of certain offences from performing a management function in, or being the beneficial owners of, designated persons including an auditor, an *external accountant* an insolvency practitioner, a tax advisor or any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance, or advice on tax matters.

The offences include ones under the 2010 Act and the Criminal Justice Act 2011. The legislation imposes an obligation on the person performing the management function, or being the beneficial owner, or on the designated person to inform the *competent authority* within 30 days of conviction or becoming aware of the conviction (in the case of the designated person). There are penalties for failure to comply with this notification requirement, on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months, or both, and on conviction or indictment, a fine not exceeding €100,000 or imprisonment for a term not exceeding 2 years or both.

4. RISK-BASED APPROACH

- What is the role of the risk-based approach?
- What is the role of *senior management*?
- How should the risk assessment 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 Directives* 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 *MLTFs*, but a realistic assessment 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 *clients*, 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 assessment 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. I*t* should ensure that *MLTF* risks are analyzed, and their nature and severity identified and assessed, in order 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, should be documented, and systems should be 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 firm wide risk assessment 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 assessment itself.

4.2.4 The risk profile and operating environment of any *firm* changes over time. The firm-wide risk assessment 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 assessment should also be refreshed by an event-driven review. A refreshed risk assessment may require AML policies, controls, and procedures to be amended, with consequential impacts upon, for example, the training programmes for relevant employees. The Joint Practices Group red flag training guide is an example of such training.

4.3 How should a risk assessment 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 assessment processes, and these could form the basis of its *MLTF* risk assessment.

4.3.2 When designing a risk assessment process, the *firm* should look not only at itself but at its *clients* and markets also. 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 which is 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). Readers, please note that an updated Money Laundering, *Terrorist Financing*, and *Proliferation Financing* National Risk Assessment for Ireland was published in June 2026.

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; and
- 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 this 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 assessment 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 assessment 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 *clients* 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; and
- 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 normal or high risk even though other *firms* might consider it lower 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 *clients* from a *High-risk third country*, the *firm's* procedures for what they regard as normal *clients* must be designed

to address the risks associated with the *High-risk third country*. Some low- and high- risk indicators can be found in **APPENDIX D: RISK FACTORS**.

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 *clients*.

4.5.6 Taking into account key risk categories, an *accountancy firm* may be able to draw up a simple matrix or spreadsheet 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 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; and
- 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* based on its firm wide risk assessment and client risk scoring methodology documented in its *CDD* policies and procedures.

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. The beneficial ownership information must be verified against that held on the *Internal Register* and Central Register(s) of beneficial ownership prior to the establishment of a *business relationship*.

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 5.3.13 - 5.3.23 of this guidance.

4.6.6 In cases where a client is a third country national who applied for residence rights or citizenship in the state in exchange for capital transfers, property or government bonds may indicate heightened risk (as set out in schedule 4 of the 2010 Act). Readers should note that the Ireland Immigrant Investor Programme was closed to further applications from 15 Feb 2023. Please click here for FAQs – Closure of the Immigrant Investor Programme (IIP) - Immigration Service Delivery

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 to 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 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.

Firms should be aware that the fragmentation of services poses a potential risk. Criminals who require multiple services may use different firms for each service, preventing a single firm from seeing the full picture. For example, *tax advisers* and payroll agents may be employed to do specific tasks and only see limited information from their client. Bookkeepers may also be employed but only given incomplete records. Where a firm has access to, or interactions with, most or all the activities of their client, they will be better placed to understand the full picture and identify risks.

Similarly, there is risk in providing services in a supply chain. A supply chain is created when a service is provided to an end user via an intermediary. Supply chains can intensify the risks by placing distance between the service provider and the end user of the service making it easier for the end user to maintain anonymity. Where supply chains involve intermediaries or end users outside the State the risk is further increased; this combines the risk of the service being provided overseas or to high risk third countries.

4.8 What is geographic risk?

4.8.1 A *firm* should consider the following question "Are our *clients* 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: RISK FACTORS**) and the *FATF* black and grey list countries: 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, the *FATF* black and grey list and the *EU designation of*

High risk third countries).

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 only have a limited exposure (refer to definition of High-risk third country in the glossary for a list of countries).

4.9 What is sector risk?

4.9.1 A *firm* should consider the following question "Do our *clients* 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 for Ireland, (readers should note that an updated Money Laundering, *Terrorist Financing*, and *Proliferation Financing* National Risk Assessment for Ireland was published in June 2026), 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?"

Non-face-to-face *business relationship*s

Face to face interactions are considered to occur in-person, meaning the parties are in the same physical location. Non-face-to-face interactions are considered to occur remotely - meaning that the parties are not in the same physical location.

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 and for the duration of a *business relationship*.

4.10.3 For example, delivery channel risk could be increased where services/products are provided to *clients* who have not been met face-to-face, or where a *business relationship* with a *client* is conducted through an intermediary. While non face to face *business relationship*s are not automatically higher risk, the risk should be considered in the context of the overall risk profile and risk assessment of the client .Also ,firms should note that one of the suggested potentially higher risk situations listed in Schedule 4 of the 2010 Act is non face to face *business relationship*s or *transactions* without certain safeguards. Examples of safeguards are electronic identification of *clients*, qualified trust services as defined in the *Electronic identification regulation* or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the firm and/or the MLRO.

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. Such risk should be considered in the AML risk assessment process both at firm level in terms of delivery channel risk assessment and as part of the client risk assessment process referenced in 4.6 above.

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. The *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 also equips itself to make informed decisions about the *client*'s standing and acceptability.

5.1.1 *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.

5.1.2 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*.

5.1.3 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

5.1.4 Sections 33 through 39 of the *2010 Act* contain 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. *CDD* measures must be applied at any time where the relevant circumstances of a customer have changed, or where the risk of money laundering and *terrorist financing* warrants their application. It is not unusual for criminals to engage an accounting practice initially to undertake low risk work and gradually increase the risk profile of the work that is requested. It is important that the practice review their risk profile as the nature of the work changes.

5.1.5 Section 6 of the 2021 Act (which amends Section 33 of the 2010 Act) requires, in summary, that *CDD* must be performed at any time where there is a legal requirement to contact a client for any legal reason connected to the client's beneficial ownership. A legal requirement arises, for example, in some tax legislation.

5.1.6 The required components of *CDD* 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: *CLIENT* VERIFICATION);
- 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 reasonable measures shall 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*.

5.1.7 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 applied.

5.1.8 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.

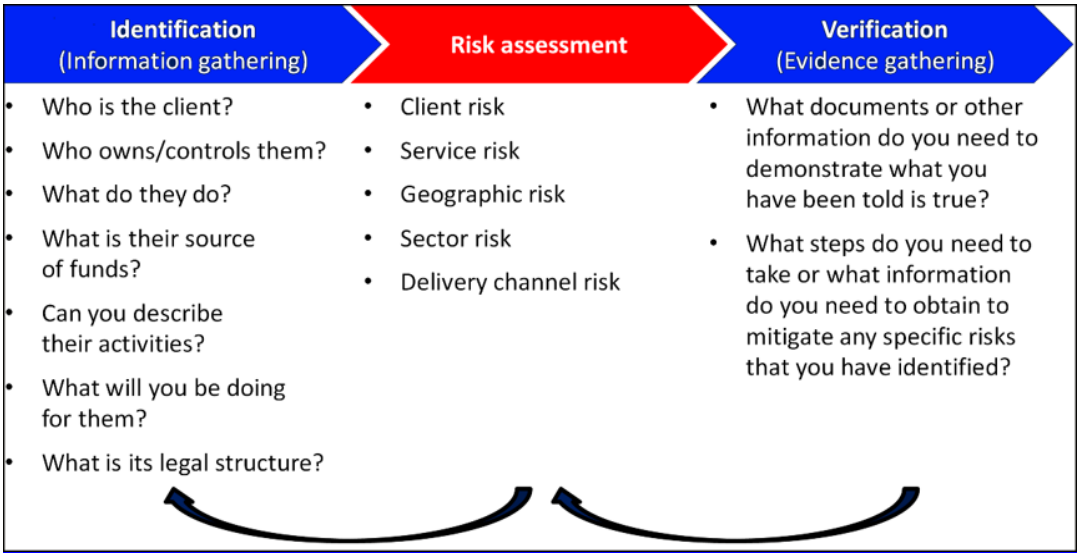
5.1.9 The *2010 Act* stipulates that *CDD* must also be performed where there is either a suspicion of *MLTF*, or any doubts about the reliability of the identity information, or documents obtained previously for verification purposes.

5.1.10 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.

5.1.11 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



5.1.12 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. The feedback loop is particularly important where the client risk profile changes or the nature of the work done for the client has an increased or decreased risk profile.

5.1.13 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 also applies to *occasional transactions*. These are defined and can be single *transactions* or a series of linked *transactions*. The 2010 Act has various thresholds for *occasional transactions* but in most cases, it is where the *transaction* is valued in excess of €15,000. Appropriate identification information for an individual is set out in Appendix B. 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 Section 6 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.

5.1.14 The next stage of *CDD* is risk assessment. This should be performed, documented, and evidenced in accordance with the risk-based approach guidance contained in Section 4 of this guidance and the client risk scoring methodology documented in the firms *CDD* policies and procedures. The risk

assessment should 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 firm-wide 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 an additional risk assessment may be required in the light of stage three (verification). The rationale for the client risk assessment (indicating if a client is rated high, moderate, or low risk from an AML perspective) should be documented and evidenced by the firm.

5.1.15 Once an initial risk assessment has been carried out for the client, 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. The type of verification required per client can be found in Appendix B.

Evidence gathering

5.1.16 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 vary. The following are illustrative of a difference 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;
- Information from qualified trust service providers as specified in the *Electronic identification regulation*;
- 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. See also section 6 concerning obligations in relation to beneficial owner searches.

Firms may also find useful the PRADO website, the Public Register of Authentic identity and travel Documents Online. It can be useful to verify the validity of identification documents received. It is an online repository

containing access to images and technical descriptions of authentic identity and travel documents of the European Union. The register is regularly updated, and the information is available in all 24 official languages of the EU.

5.1.17 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.

5.1.18 *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.

5.1.19 It is important that verification procedures are undertaken on a risk-based approach.

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

Validation of documents

Certification of documents by a third party

5.1.20 *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 in their AML policies and procedures. 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 which is supervised for ML/TF*, or *relevant independent legal professional*, or their equivalent in other Member States or High risk or non-high risk third countries as summarised at section 10.2, and provided that, in all cases, the person is subject to supervision as to his compliance with those requirements.

Annotation of sources of validation

5.1.21 If there is uncertainty as to the source of the document annotation could 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 person who downloaded the evidence to confirm who downloaded and what date (for accuracy/audit trail purposes). 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 and automated AML Compliance Solutions

5.1.22 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.

5.1.23 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 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.

5.1.24 Automated AML Compliance Solutions

A range of automated client onboarding and ongoing Anti-Money Laundering supervision and compliance software solutions are available in the market. These systems may incorporate features such as automated biometric verification and checksum (algorithmic) validation of client identification documents. Some solutions also include automated sanction screening capabilities.

Firms should note, however, that while such systems can streamline and support AML compliance processes, they do not guarantee full regulatory compliance. For example, automated tools often struggle with sanction screening in cases where sanctions apply to activities or categories of persons rather than specifically named individuals. Additionally, manual intervention is typically required to identify *Politically Exposed Persons (PEPs*), as there is no centralised global database of *PEPs*.

Practitioners need to consider whether a commercially available package is in fact adequate to deliver a genuinely risk-based approach. Such a package may not be sufficiently responsive to risk flags, and it may not contain feedback loops including requirements to reassess risk levels in response to information discovered during the subsequent stages of the process.

5.1.25 It is also important to recognise that biometric and checksum validation controls applied to documents such as passports and national identity cards can be circumvented. Accordingly, automated AML compliance systems should be used with caution and with a thorough understanding of their operational limitations. Firms must recognise that where a practice uses proprietary software to assist in the performance of the *CDD* and to sanction test an individual, the practice retains responsibility for that verification and testing. If the software fails to properly verify identification documents or generates a false negative sanction check, the ultimate responsibility for this will rest with the practice. Care should therefore be taken in selecting and using automated verification software including regular review of the rules, scenarios, and thresholds embedded in the AML system.

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 it 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*. The section sets various different threshold amounts depending on who the designated person is, or what the *transaction* is, and there is a residual category if others do not apply where the *occasional transaction* has a value more than €15,000. 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 €150) and other conditions set out in the section.

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 5.3.13 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. The degree of supervision of client activities should reflect their risk profile.

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*
- where there is a legal requirement to contact a customer for any legal reason connected to the client's beneficial ownership. A legal requirement arises, for example, in some tax legislation.

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 5.3.13 of this guidance);
- a significant change in the *client's* business activity (this would include new operations in new countries);
- 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*;

- At any time, including a situation where the relevant circumstances of a customer have changed, where the risk of money laundering and *terrorist financing* warrants their application; and
- Adverse/negative media regarding a client.

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. Firms should address the frequency that they conduct periodic reviews relative to the associated risk in their documented policies and procedures.

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.

Additional checks in non-face-to-face situations

5.2.10 Firms should be alert to, and cautious of, the ever-increasing prevalence of deep fake related identity fraud. As referenced in 4.10.3, non-face-to-face interactions are not automatically so but can be considered higher risk. Firms should consider implementing additional checks when on-boarding *clients* in non-face-to-face situations.

Additional checks could include:

- Make telephone contact with the client using a verified telephone number sourced independently (this could be by opensource research, for example, looking the number up on the internet).
- consider an electronic verification/identification method, approved or accepted by the firm and/or the MLRO if it has more than a few non-face to face *clients*.
- More frequent and detailed ongoing *monitoring* of the relationship and review of *CDD*, particularly if the client is deemed higher risk .

Firms should be aware that with the application of the AML Regulation from 10 July 2027 that AML verification requirements for both face-to-face and non-face-to-face interactions will be more prescriptive with increased emphasis on electronic identification to meet compliance obligations.

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: RISK FACTORS**.

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

Simplified due diligence (SDD)

5.3.3 'Simplified customer due diligence', is covered in Sections 34 A of the *2010 Act*. For an *accountancy firm* this means that it 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 there is lower risk as described in the section and follows the procedures described in the section.

5.3.4 Where a *client* or potential *client* has been subject to simplified due diligence and a suspicion of 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: RISK FACTORS** (taken from Schedule 3 of the *2010 Act*) and relevant information made available by its *competent authority*. Where a firm applies simplified *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*.

Enhanced due diligence (EDD)

5.3.6 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* and specifies the measures to be applied.

Article 9 of 4 AMLD (as amended) empowers the European Union to identify jurisdictions that have strategic deficiencies in their AML/CFT regimes. Please refer to the EU designation of *High risk third countries* at the following link: EU list of high-risk third countries. Also, click to access the *FATF* " Black "and "grey" lists of high risk third countries. Usually, both *FATF* and EU lists are the same, but both must be checked and if there are differences, all jurisdictions on both lists should be taken into consideration.

5.3.7 Since the 2021 Act where a customer is established or residing in a *High-risk third country* the following measures must be taken:

(a) obtain additional information on the customer and on the beneficial owner;

(b) obtain additional information on the intended nature of the *business relationship*;

(c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owner;

(d) obtain information on the reasons for the intended or performed *transactions*;

(e) obtain the approval of *senior management* for establishing or continuing the *business relationship*; and

(f) conduct enhanced *monitoring* of the *business relationship* by increasing the number and timing of controls applied and selecting patterns of *transaction* that need further examination.

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

- 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 (see 5.3.12 below in relation to complex business structures);

- any other case which, by its nature, can present a higher risk of MLTF. For example, where the purpose of the *transaction* or source of funds do not align with what the firm knows about the client's business activities.

See examples of higher risk factors in Appendix D of 2010 Act: Risk Factors

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: RISK FACTORS** (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 such as a Garda, notary public, solicitor or accountant 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*
- requiring approval from *senior management* prior to accepting / continuing the *business relationship*

Complex business structures

5.3.12 The 2010 Act makes the following provisions in relation to examining the background and purpose of certain *transaction*s:

> It provides that a designated person shall, as far as possible, in accordance with policies and procedures adopted in accordance with section 54, (of the 2010 Act) examine the background and purpose of all *transaction*s that (a) are complex, (b) are unusually large, (c) are conducted in an unusual pattern, or (d) do not have an apparent economic or lawful purpose. A designated person must increase the degree and nature of *monitoring* of a *business relationship* in order to determine whether such *transaction*s appear suspicious. It is an offence to fail to comply with the section.

Politically exposed person (PEP)

5.3.13 Section 37 of the *2010 Act* specifies that *PEPs* (as well as certain *immediate family members* and *close associates of PEPs*) and client relationships

involving a PEP must be subjected to Enhanced Due Diligence ("EDD"). The nature, and extent of, such EDD measures will 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 each particular *PEP*.

5.3.14 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 any of the following individuals (but not including any middle ranking or more junior official) : a "specified official", a member of the administrative, management or supervisory body of a state-owned enterprise or any individual performing a "prescribed" function 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 a parliament or of a similar legislative body;
- a member of the governing body of a political party;
- 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.

While section 37 explicitly notes a qualifying period of those who have held a prominent public function within the last 12 months, the 2021 Act amended the 2010 Act to require firms to continue to apply such *enhanced due diligence* measures to a PEP relationship for as long as is reasonably required to take into account the continuing risk posed by that person and until such time as that person is deemed to pose no further risk specific to politically exposed persons.

'*Immediate family member*' of a *PEP* includes parents, spouses and equivalent (e.g. civil partner), children, spouses of children and equivalent (e.g. civil partner), and any other family member of a class prescribed by the Minister (for Justice, Equality and Law Reform) (none at the time of publication). In determining whether other *immediate family member*s should be subject to EDD, *accountancy firm*s 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 member*s other than those contained within the definition set out in the 2010 Act.

'*Close associate*' includes any person who has joint beneficial ownership of

a legal entity or arrangement, or any other close business relations with a *PEP* or has sole beneficial ownership of a legal entity or arrangement set up for the actual benefit of a *PEP*.

Readers should refer to section 37 of the 2010 Act for exact definitions.

5.3.15 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, and firms should have risk sensitive measures in place to recognise *PEP*s (Sections 37(1) to 37(3)). This can be a simple check conducted by enquiring with the *client* and perhaps performing a general online/open-source search to identify additional information regarding *PEP* status of potential *clients*. *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 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*.

5.3.16 *The EDD applied by firms* wanting to enter into, or continue, a *business relationship* with a *PEP* includes:

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

5.3.17 The nature and extent of the EDD measures applied must vary depending on the levels of *MLTF* risk associated with individual *PEPs*.

5.3.18 An individual identified as a *PEP* solely because of their public function such as a director of a State-Owned Entity 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 and 2024 update 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;
- the risk profile of the specific boards and committees that the PEP is a member of, including the risk that the PEP could be offered a payment in order to influence the *PEPs* lobbying activities or decision making.

5.3.19 In lower-risk situations a *firm* may 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 *firms* should take to *MLTF* compliance.

5.3.20 While *Accountancy firms* must treat individuals as *PEPs* for as long as is reasonably required 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.

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

'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.

5.3.22 In January 2023, the Minister for Justice, with the consent of the Minister for Finance, issued Guidelines under section 37(12) of the Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 (as amended) clarifying those functions in the State that may be considered to be prominent public functions for the purposes of the 2010 Act. This will assist firms to identify domestic *PEPs* when conducting their risk assessment.

5.3.23 The preamble to the 4 AMLD (as amended), 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 Directives*, 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.

Updates to PEPs under AMLD 6

5.3.24 AMLD 6 will bring about a number of changes to *client* relationships involving *PEP*s. It will come into effect from 10th July 2027. These changes amend the definition of a *PEP*, including the definition of family member, and also includes a requirement on member states to issue and keep a list of what qualify as prominent public functions. Some more details and additional information of the changes that will occur under AMLD 6 are found in Chapter 11 of this guidance document.

Sanctions and other prohibited relationships

5.3.25 Sanctions are officially known as restrictive legally binding measures that can be taken against individuals, entities or countries. *Accountancy firms* must comply with sanction requirements when conducting business. They must complete a sanctions risk assessment, which includes assessing the

exposure of the firm's *client* base and business activities to sanctions risks and various sanction regimes currently in operation (e.g. UN, EU, UK, US where relevant). *Accountancy firms* must perform sanctions due diligence for *clients* and screen *clients* against current sanctions lists across various jurisdictions where exposure has been identified. There are various types of sanctions including asset freezes, trade restrictions, financial restrictions, and travel/transport restrictions. Sanctions is a complex and changeable area. Detailed discussion of it is beyond the scope of this guidance. *Accountancy firms* should note that the Central Bank of Ireland (CBI) is one of the competent authorities and is responsible for the administration, supervision, and enforcement of relevant aspects of financial sanctions in Ireland. Further information on financial sanctions is available at International Financial Sanctions | Central Bank of Ireland. Also, see Central Bank of Ireland | Financial Sanctions FAQs if you have general queries in relation to sanctions.

5.3.26 The other Irish competent authorities for sanctions are the Department of Enterprise, Tourism and Employment, which is responsible for the implementation of trade sanctions and the Department of Foreign Affairs, which is responsible for foreign policy and representing Ireland internationally. Failure to comply with sanction requirements can result in regulatory fines, reputational damage, and/or legal consequences.

5.3.27 Firms should note in particular the ban on providing accounting services to Russia which was brought into force in June 2022 as part of the sixth package of European Union sanctions against Russia. Click to access the relevant Article 5 n of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

The ban prohibits the provision, directly or indirectly, of certain business-relevant services such as accounting, auditing including statutory audit, bookkeeping and tax consulting services, business and management consulting, and public relations services to the Russian government, as well as to legal persons, entities or bodies established in Russia. The services of accounting, auditing, bookkeeping and tax consultancy services cover the recording of commercial *transaction*s for businesses and others; examination services of accounting records and financial statements; business tax planning and consulting; and the preparation of tax documents. Exemptions and derogations from the ban are also provided. The CBI has a specific CBI web page dedicated to derogations.

5.3.28 Restrictive measures (sanctions), emanate from the European Union (EU) and the United Nations (UN). EU restrictive measures may be either autonomous or brought about by UN Security Council resolutions. Sanctions are adopted by the United Nations Security Council under the UN Charter and, in addition, through autonomous decisions taken at European Union level. EU and UN sanctions are implemented in Ireland through EU Council Decisions and Regulations. The Regulations are directly applicable in Irish law. In addition, Statutory Instruments are frequently made in order to provide for a domestic offence for breach of the sanctions and for related penalties.

5.3.29 All natural and legal persons are required to comply with sanctions when conducting business with *clients*, suppliers, and third parties. This requires

monitoring the EU consolidated list and taking appropriate action as explained below, including sanctions risk assessment, sanctions screening, and sanctions due diligence. Please click for the consolidated list of persons, groups and entities subject to EU financial sanctions, which reflects the officially adopted texts published in the Official Journal of the EU. You can also download a PDF version of the consolidated list of financial sanctions, but members should be aware that this list is constantly being updated. Please click for sanctions lists and tools on the EU Sanctions Helpdesk website (see further below).

5.3.30 **Dual use products**: members should be aware of the application of sanctions prohibiting exporting, brokering, providing technical assistance, transit and transfer for dual use products. These are products that could enhance a country's military or technological capacity, with a specific focus on sectors like aviation, computing, and surveillance. For further details regarding sanctions on dual-use products, please refer to details included on the European Commission's web page - Sanctions on dual-use goods.

5.3.31 Sanctions due diligence extends beyond direct customer relationships and should also cover 'knowing your customer's customers' to ensure the firm knows who they are dealing with and if there is any risk of sanctions circumventions occurring and cases where customers try to avoid sanctions by using third parties. As appropriate, there may be a need to perform detailed customer mapping to ensure knowledge of your customer's customers/supply chains used. For further details regarding the risk of sanctions circumvention, please refer to European Commission Guidance to shield against sanctions circumvention and details regarding The 'Best Efforts' Rule included on the EU Sanctions Helpdesk.

5.3.32 Firms unsure of their legal obligations in relation to sanctions should consider obtaining legal advice. Members must keep up to date on sanctions and be aware of which countries, individuals and entities to which sanctions apply. They must check whether they hold any funds or economic resources for the persons set out in the current sanctions lists. The Central Bank website states that once a person or entity has been sanctioned under EU Financial Sanctions, there is a legal obligation not to transfer funds or make funds or economic resources available, directly or indirectly, to that person or entity.

Sanctions internal controls

5.3.33 Firms should where relevant, identify and assess if areas of their business are particularly vulnerable or exposed to restrictive measures and to circumvention of restrictive measures. On this basis, they should put in place, implement and maintain up-to-date policies, procedures and controls to ensure that they can comply effectively with restrictive measures regimes. Sanction controls include:

- Establishing a sanctions policy
- Performance of sanctions risk assessment to understand exposure to sanction risks for the accounting firm's business and *clients*
- Implementing sanctions training for staff

- Determining and documenting when sanctions screening and associated sanctions due diligence should be performed – for example, when onboarding a new client, onboarding a new vendor/supplier, changes in the consolidated sanctions list (for example, when the EU issues a new sanctions package)
- Establishing and documenting a process to continuously review consolidated sanctions lists given that the lists are updated frequently with the issuance of various EU sanctions packages. Once the sanctions lists are updated, review the firm's *clients* against the updated list to identify any sanction hits/sanction risks through performance of sanctions due diligence
- Consideration of any sanctions circumvention risks when performing sanctions due diligence
- Firms should also ensure that business suppliers and vendors used are not subject to sanctions
- Establishing and documenting an internal escalation process for further review of instances where a potential sanction match ('hits') against a sanctioned person/entity is identified during screening and protocols for subsequent next steps (for example immediate rejection of client, freezing of any *transaction*s, and consideration of reporting requirements to national competent authorities)
- Establishing a process for reporting a sanctions match ('hit') and/or sanctions breaches to national competent authorities (where relevant)

5.3.34 For further guidelines regarding sanctions governance arrangements, internal policies, procedures, and controls, please refer to the following document issued by the European Banking Authority. Although applicable and required for *financial institutions*, there is useful information included for the awareness of accounting firms regarding sanctions frameworks: Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures.

5.3.35 Readers may also find useful further information on the EU Sanctions Helpdesk webpages.

An EU Sanctions Helpdesk has been established, supporting European companies in complying with European Union restrictive measures imposed worldwide. It is aimed primarily at Small and Medium-sized Enterprises (SMEs), and it offers resources and personalised help to companies performing sanctions due diligence checks. Please see links below for details regarding the EU Sanctions Helpdesk:

- EU Sanctions Helpdesk
- EU Sanctions Helpdesk - Sanctions lists and tools
- EU Sanctions Helpdesk - EU sanctions primer for SMEs
- EU Sanctions Helpdesk - Sanctions due diligence

The EU Sanctions Helpdesk also has information regarding sanctions red flags. Readers are referred to information on red flags: Mastering the indicators of sanctions risk.

Other prohibited relationships

5.3.36 Firms should also note that 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 or provision of anonymous passbooks or safe deposit boxes, 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.

Proliferation Financing

5.3.37 A meaning of *Proliferation Financing* is offered in the Glossary and is taken from a *FATF* report of 2010 Combatting Proliferation Financing: A status report on policy development and consultation (see P5).

5.3.38 Guidance on the complex topic of *Proliferation Financing* is outside the scope of this document. Apart from a number of statutory instruments transposing European legislation, the concept of *Proliferation Financing* has not yet been fully introduced into Irish law. The 3rd Irish National Risk Assessment, which was published in June 2026, includes discussion of risks associated with *proliferation financing*.

5.3.39 Ireland's regulatory regime to combat the threat posed by *proliferation financing* derives from implementation of UN and EU sanctions regimes. The current focus (as of the date of publication) of the *proliferation financing* threat is on the Democratic People's Republic of Korea (North Korea/DPRK), Iran and chemical weapons activity. Firms must monitor the area for changes and developments. Adherence to the sanctions regulatory framework may assist firms in mitigating their *proliferation financing* risk.

5.3.40 Given that significant focus of UN Security Council Resolutions, EU sanctions and *FATF* guidance on *proliferation financing* relate directly to Iran and DPRK, the provision of *Accountancy services* to persons, companies, or entities connected with either of these jurisdictions poses an extremely high risk. Businesses should only provide such services in rare circumstances after taking appropriate legal advice.

5.3.41 There are several documents produced by *FATF* regarding *proliferation financing*. Information and resources regarding this area are included on *FATF's* website at the following link: *FATF* - proliferation financing.

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 firm*s 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 *transaction*s 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 5.4.9 and following 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).

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*.

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 s/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 an independent expert under section 511 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 appointment.

6. BENEFICIAL OWNERSHIP

6.1 Beneficial owner

6.1.1 A beneficial owner can only be a natural person, i.e., an individual (other than in the case of a trust, see below) who ultimately owns or controls the client and/or the natural person(s) on whose behalf a *transaction* or activity is being conducted.

6.1.2 Sections 26 to 30 of the 2010 Act set out in some detail the meaning of beneficial owner in terms of bodies corporate, partnerships, trusts and estates of deceased persons. It also includes 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.

6.1.3 The 2021 Act inserts a detailed definition in relation to beneficial owners of *Relevant Trust*s and similar wording is found in the Trust Regulations 2021.

6.1.4 Where the beneficial owner is the senior managing official, a designated person shall take the necessary measures to verify the identity of that person and shall keep records of the actions taken to verify the person's identity, including any difficulties encountered in the verification process (Section 33(2)(b)(iii) of the 2010 Act).

6.1.5 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 an *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

Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
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 partnership
Trusts				Control in respect of a *Relevant Trust* means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument concerned or by law to do any of the following: (a) dispose of, advance, lend, invest, pay or apply the trust property; (b) vary the *relevant trust*; (c) add or remove a person as a beneficiary or to or from a class of beneficiaries; (d) appoint or remove trustees; direct, withhold consent to, or veto the exercise of any power referred to in paragraphs (a) to (d). "Beneficial owner " includes: 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)

Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
				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 exhausted and recorded				The individual who ultimately owns or controls the *client*, or on whose behalf a *transaction* is being conducted (section 30 (3) 2010 Act) the senior individual responsible for management (noting the reasons why the business was unable to obtain adequate information on the beneficial owner, and considering whether it may be appropriate to cease acting, or file a *STR*) (section 33(2)(b)(iii) 2010 Act)

6.2 Beneficial ownership registers

6.2.1 In response to efforts to hide ownership and control of entities, the *EU Directives* and Irish law contain provisions the purpose of which is to increase transparency. *Accountancy firm*s must be cognisant that under the current suite of AML legislation, obligations in respect of beneficial ownership fall on:

- Entities in scope for AML obligations (either on its own behalf and / or in respect of its *business relationship*s with other designated persons)

- An individual basis, where an accountant may act as a beneficial owner in respect of a client. One example is holding shares on a client's behalf or perhaps acting as a trustee or director of a client company

6.2.2 Legislation contains obligations on entities (see further below) to maintain internal beneficial ownership registers and to register certain details on the relevant Central Register.

6.2.3 The primary obligations for:

- *Trusts:* arise from the Trust Regulations 2021
- *Corporate entities:* arise from the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019
- *Industrial and Provident Societies* arise from the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019
- *Certain Financial Vehicles* arise from European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of *Certain Financial Vehicles*) Regulations 2020 and Investment Limited Partnerships (Amendment) Act 2020
- *Partnerships* It is worth noting that establishing beneficial ownership of partnerships is regulated by section 27 of the 2010 Act. There is currently no legislative requirement to have an *internal register* of beneficial ownership for partnerships and there is no central register to register beneficial ownership of a partnership.

The following paragraphs will focus on corporate entities and trusts. The above regulations apply to all corporate entities and certain trusts where the trustees are resident in the State, or which is otherwise administered in the State, or the trust owns a business or land in the State.

The trustees of such trusts and the directors of corporate entities are now required to obtain and record beneficial ownership information in the entity's beneficial ownership register they are responsible for. (*Certain Financial Vehicles* and *Industrial and Provident Societies* have their own beneficial ownership obligations under their own updated respective legislation.)

6.2.4 In addition to maintaining an internal beneficial ownership register, each of the above types of entities must register certain details with the relevant Central Register, maintained by the relevant registrar as prescribed under the legislation. Please see the diagram below for the relevant Central Register in accordance with the different types of entities.

Beneficial ownership details – entity obligations and information

6.2.5 New obligations on designated persons - the 2021 Act introduces new obligations on 'designated persons' to ascertain that information concerning the beneficial ownership of a customer has been entered in the relevant beneficial ownership register, before establishing a *business relationship* with a customer to which *Beneficial Ownership Regulations* apply (such as a company or a trust). A designated person must not engage in that *business relationship* until the relevant information is obtained. By way of derogation however, a *financial institution* is permitted to open an account ahead of obtaining such information but cannot allow any *transaction*s on that account.

6.2.6 Prior to the establishment of a *business relationship*, the 2010 Act (as amended by the 2021 Act) requires a designated person to take reasonable steps to confirm the beneficial ownership of the customer it is entering into a relationship with. It is worth noting that the legislation allows *financial institutions* to open an account ahead of obtaining such information but cannot allow any *transaction*s on that account. The trustees and directors must provide information on beneficial ownership and notify of changes to the register to any designated person with whom they have an *occasional transaction* and /or *business relationship*.

6.2.7 *Accountancy firm*s, 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. Prior to the establishment of a *business relationship* with a customer to which the Trust Regulations 2021 apply, a designated person shall ascertain that information concerning the beneficial ownership of the customer is entered in the express trust (beneficial ownership) register. 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%.

6.2.8 Some possible options to verify 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 or relevant Central Register;
- Electronic searches either direct or via a commercial agency for electronic verification;
- The beneficial ownership register maintained by the entity.

6.2.9 Every *accountancy firm* must confirm the beneficial ownership details for their corporate and trust *clients* prior to establishing a *business relationship*. Corporate and trust *clients* are obliged to take all reasonable steps to obtain and hold adequate, accurate and current information in relation to their beneficial owners. The information they are required to maintain is as follows:

- the name, date of birth, nationality and
- the residential address of each beneficial owner
- a statement of the nature and extent of the interest/control attributed to each beneficial owner
- the PPS number of each beneficial owner or, (in the case of trusts) where no PPS number has been issued, certain forms of verification as prescribed such as foreign tax reference number
- In situations where beneficial ownership information is already held on another register in the EU corresponding to the Central Register, Trust *clients* can satisfy their filing obligations by procuring a certificate from the corresponding registrar
- Changes made to information held on a corporate or Trust client's Beneficial Ownership Register must be filed on the relevant Central Register within 14 days
- Where an *accountancy firm* acts on behalf of a corporate or trust client in respect of its beneficial ownership obligations, it is deemed to perform a " presenter" role under the *Beneficial Ownership Regulations* pertaining to corporate entities and trusts. As a "presenter", an *accountancy firm* is obliged to provide the following details to the relevant Registrar:

- The presenter's name, address, phone number and email address
- The capacity in which it is acting as a presenter for the client; and
- Where relevant, the name, address, phone number and email address of a natural person for correspondence purposes.
- An entity must deliver the beneficial ownership information to the appropriate Central Register:
- For existing trusts: within 6 months from commencement of the Regulations, i.e. 23 October 2021;

- For newly established trusts: within 6 months from coming into existence.
- It should also be noted that the Corporate and trust entities are obliged to keep the information on their beneficial ownership registers and the information held on the relevant Central Register aligned and up to date. This is referred to as the "follow up obligation" which must be discharged within 14 days from an update being required to be made to the entity's beneficial ownership register. This is to ensure the relevant Registrar is kept informed of any changes.

Give notice to beneficial owners

6.2.10 Where a relevant entity (client trust or company as the case may be) has reasonable cause to believe an individual is a beneficial owner of it, it is obliged to give notice to the individual to confirm whether this is the case and to confirm or correct the particulars to be entered in the entity's beneficial ownership register.

6.2.11 The obligation to give notice in this manner is discharged if the relevant entity has already been informed of the status of an individual's beneficial ownership and their required particulars, which were provided either by the beneficial owner or with their knowledge.

6.2.12 This is also the case where the relevant entity believes there is a change to the information held on the relevant Central Register. In this instance, the entity must give notice to the individual beneficial owner to confirm the changes. As above, the obligation to give notice in this manner is discharged if the entity has already been informed of the change and same was provided either by the beneficial owner or with their knowledge.

Duties of others

Duty of beneficial owner to notify status or a change

6.2.13 Where an individual is, or ought to know that they are, a beneficial owner and the individual's details are not included on the Trust Register, the individual must provide their details to the trustee, in writing, within 2 months. A similar obligation applies in regard to any changes.

Duty of Designated Persons in respect of beneficial ownership

6.2.14 Before a *business relationship* is established, a designated person is obliged to take reasonable steps to establish the veracity of the beneficial ownership of its *clients*. One step it is obliged to take under the 2010 Act is to confirm the beneficial ownership with the relevant Central Register. Where a Designated person identifies a discrepancy i.e. where the entry is inconsistent or incorrect between its own records and those maintained by

the Central Register, it must notify the relevant Registrar.

6.2.15 This is done by way of filing a non-compliance notice or a discrepancy notice with the relevant Central Registrar. These forms are available on request from the RBO at discrepancies@rbo.ie.

6.2.16 For Trusts *Clients*: https://www.revenue.ie/en/crbot/contact-the-registrar/index.aspx

> Any queries regarding the Central Register of Beneficial Ownership of Trusts (CRBOT) can be sent via MyEnquiries on ROS.
>
> For direct contact with the CRBOT please ensure the relevant titles below are selected for both drop-down menus:
>
> - Select 'Trust Register (Central Register of Beneficial Ownership of Trusts)' from menu 'Enquiry relates to'
> - Select 'General Query' from menu 'More specifically'
>
> The CRBOT can also be contacted via email: TrustRegister@revenue.ie

For Corporate *Clients*: FAQs - RBO

> Only a person who is an authorised officer of a 'relevant person' is entitled to report a discrepancy to the Registrar on behalf of a 'relevant person'.
>
> Please click to go to the CRO page dealing with reporting of discrepancies and non - compliance for detailed information on the processes and forms.

Access to the Register of Beneficial Ownership of Corporate Entities in Ireland

6.2.17 The introduction of S.I. No. 308/2023 amends the regulatory framework concerning access to the Register of Beneficial Ownership of Corporate Entities in Ireland. Under the updated regulations, there is no change to the unrestricted access previously granted to certain authorities such as An Garda Síochána and *FIU Ireland*, nor is there any change to the restricted access available to designated persons, for example, banks conducting customer due diligence.

6.2.18 However, for all other individuals or entities seeking access to the register, and who do not fall into the categories mentioned above, the regulations now require the demonstration of a legitimate interest. In particular, applicants must show that they are actively involved in preventing, detecting, or investigating money laundering or *terrorist financing* offences. Furthermore, they must provide evidence that the entity about which they are requesting information is connected either to persons convicted of such offences or to assets located in a *High-risk third country*.

6.2.19 Readers can find out more about this in AMLD 6 Chapter 11.

6.3 Safe-deposit boxes and payment accounts

6.3.1 Regulations were published in 2022 in Ireland to establish a central database of information on safe-deposit boxes and payment accounts. They are the European Union (Anti-Money Laundering: Central Mechanism for Information on Safe-Deposit Boxes and Bank and Payment Accounts) Regulations 2022 and amending regulations S.I. No.445/2022. The regulations authorise the Central Bank of Ireland to establish and maintain a central register of information on safe-deposit boxes and bank and payment accounts, as required under the fourth and fifth Anti-Money Laundering Directives. Click for the Central Bank of Ireland website with more details.

6.3.2 On 2 February 2023, the European Union (Money Laundering and *Terrorist Financing*) (Use of Financial and Other Information) Regulations 2023 were signed into law. This regulation makes provision for certain designated authorities to access and search bank account information when necessary for the performance of their tasks for the purposes of preventing, detecting, investigating or prosecuting a serious criminal offence.

7. 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?

7.1 What must be reported?

The reporting regime

7.1.1 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

7.1.2 Section 2 of this guidance defines the money laundering offences, and it is also defined in the Glossary. Reference should be made back to this section and the Glossary for the purpose of the definition and this paragraph.

Terrorist financing

7.1.3 '*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. See also reference in the Glossary below.

7.1.4 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.

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

7.1.6 In relation to reporting obligations, references to *accountancy firm*s are to be read as including references to a director or other officer, employee or (in the case of a partnership) principal acting on behalf of the *accountancy firm*. Section 41 of the 2010 Act 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.

7.1.7 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.

7.1.8 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*.

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

Knowledge and suspicion

7.1.10 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.

7.1.11 Having knowledge means actually knowing that something is the case. There is very little guidance on what constitutes 'suspicion', so the concept remains subjective. Suspicion does not require document-based evidence, it may be a particular fact pattern, a series of red flags or general observations that cause concern. 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 with some foundation.

Suspicion is not

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

7.1.12 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. However, an *accountancy firm* should take appropriate risk management procedures if these suspicions elevate the risk of the client. 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.

7.1.13 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.

7.1.14 '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".

7.1.15 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.

7.1.16 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*.

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

Crime and proceeds

7.1.18 *Criminal conduct* is behaviour which constitutes an offence in Ireland or, in certain circumstances, occurring elsewhere (see Section 2 above of the guidance). *Criminal conduct* is defined under Section 6 of the 2010 Act 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.

7.1.19 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.

7.1.20 The 2010 Act's definition of *money laundering offences* (Part 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).

7.1.21 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 in so far as possible explain the legal risks to them. 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.

7.1.22 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 Act 2014, 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 7.4 below. The area of privilege is a complex one and legal advice may be required . Professional guidance has been issued dealing with indictable offences under the Companies Acts which are reportable to the Corporate Enforcement Authority, and reporting of theft and fraud offences, which at date of issue are as follows:

- IAASA Guidance Note 01/2019 - The Duty of Auditors 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

[The latter two documents, while outdated, may still be of some value to members]

7.1.23 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. When completing an STR on goAML, the field Report Indicator is mandatory and this contains a dropdown of different types of suspected criminal conduct, including Money Laundering, *Terrorist Financing*, Tax Evasion and so forth.

At the date of publication under the current version of goAML software, a user can select multiple report indicators (i.e. more than one can be selected). Careful consideration should be given to selecting at least one of these as it will assist *FIU Ireland* in prioritising the STR. When selecting "*Transaction* Type" the options are Multi Party or BiParty. "BiParty" *transaction*s have a clear "From" and "To" side. "Multi-Party" is used for anything that has not a clear "From" and "To" *transaction*. (This could change in future goAML software versions).

The FIU will always try to assist if a reporter wishes to contact them when filing an STR. Their contact details are included at 7.3.32. 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 7.1.19, 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

7.1.24 *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.

7.1.25 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.

7.1.26 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: *STR* REPORTING PROCESS CHECKLIST**.

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 2014*.

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.

7.2 Offences relating to reporting

Failure to disclose

7.2.1 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.

7.2.2 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

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

- the *professional privilege reporting exemption* (see section 7.4 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*. (See paragraph 3.3.13 above). 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.

7.2.4 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')

7.2.5 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*).

7.2.6 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.

7.2.7 Considerable care must be taken when communicating with *clients* 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 firm*s keep records of these deliberations and the conclusions reached. 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 7.5.

7.2.8 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

7.2.9 There are a number of exceptions/defences 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 An Garda Síochána to the District Court), in accordance with Section 17, and the disclosure made was solely to 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 24 of the *2010 Act)*, and the institution receiving the disclosure is from a Member State or a majority-owned subsidiary or branch situated in a third country of a *credit institution* or *financial institution* incorporated in a Member State, where the subsidiary or branch was in compliance with group-wide policies and procedures adopted in accordance with section 54, or, as the case may be, Article 45 of the Fourth Money Laundering Directive.
- **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 (other than a high risk third country).

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 the *competent authority* that, at the time of the disclosure, was the *competent authority* responsible for *monitoring* the individual or firm or for *monitoring* the individual or firm on whose behalf the disclosure was made, or
  - for the purpose of the detection, investigation or prosecution of a criminal offence in 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*.

7.2.10 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.

7.2.11 *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.

7.2.12 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.

7.3 When and how should a report be made?

Is a report required?

7.3.1 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.

7.3.2 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 internal 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

7.3.3 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.

7.3.4 There are no legal or other external requirements for the format of an internal report and *accountancy firm*s 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.

7.3.5 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. Sufficient information should be retained in order to record the reported suspicion and support the firm's determination of whether to discount the suspicion, or to proceed and file the STR with the authorities. Please see chapter 8 "record keeping '' for further details of record keeping requirements.

7.3.6 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, but also undesirable since it would risk *tipping off* a money launderer.

7.3.7 *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 step 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?

7.3.8 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*.

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

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

7.3.10 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.

7.3.11 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 Section 42 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. It is important that discussions relating to suspicions of money laundering are kept confidential and are not subject to open discussion between other staff members in the office. Ideally, the only people who should be aware that an internal report has been made are the individual making the internal report and the MLRO. This is to reduce the risk of a *tipping off* offence occurring.

7.3.12 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.

7.3.13 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; and
    - 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*.

7.3.14 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.

7.3.15 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 maintains close supervision of such delegated functions. It would also be advisable for *accountancy firm*s 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.

7.3.16 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*.

7.3.17 ***Group Audits***

(a) In the context of group audits, auditors should consider protocols for reporting obligations. In a group audit situation, there is typically a group auditor and a component auditor appointed. A component auditor is a member of the engagement team under ISA (Ireland) 600. A direct supervision and review relationship is required under ISA 600 by the group auditor, and the group auditor retains ultimate responsibility for the audit work performed by every member of the engagement team (including component auditors). The reporting arrangements and instructions provided by the group auditor to a component auditor cover non-compliance with laws and regulations (NOCLAR), which would also include AML related regulations including suspicious *transaction*s. Typically, group instructions would not go into granular details about AML requirements. Rather the wider context of NOCLAR is covered in the group audit instructions - unless a group engagement team identifies a specific risk around AML compliance in a particular group audit.

(b) If a suspicious activity is identified by a component auditor, then it should be reported to the group auditor but ensuring compliance with permitted disclosures and tipping off requirements (as referred to in sections 7.2.5 - 7.2.7 and section 7.2.9). If the reader is in doubt on any matter in this complex area, they should consider obtaining legal advice.

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

7.3.18 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 7.5). 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.

7.3.19 External STRs are required to be made to both the *FIU Ireland* and the Revenue Commissioners via online systems. External STRs are submitted to the *FIU Ireland* using the goAML Online System and to the Revenue Commissioners via the Reporting Online Service (ROS). Hard copy (paper) STRs are not accepted.

7.3.20 MLROs must be registered on both goAML and ROS before submitting a STR. The MLRO is encouraged to register as soon as possible on both systems. In particular registration on goAML will allow the MLRO access to the goAML Message Board. This is a two-way secure communication between the reporting entity and *FIU Ireland*. The MLRO will receive STR acknowledgements and alerts via the Message Board. Such alerts are not available to the public and will only remain on the Message Board for 6 months for security reasons.

goAML– *FIU Ireland* has produced the following Guidance to assist MLROs:

- goAML Reporting Entity Registration Guide .This was updated in 2025
- goAML WEB Reporting Quick Reference Guide
- goAML FAQs

7.3.21 See also how to revert and amend reports submitted which have been rejected by *FIU Ireland*.

7.3.22 ROS – Information on reporting to Revenue Commissioners is available at How to submit Suspicious *Transaction* Reports (STRS) (revenue.ie)

7.3.23 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.

7.3.24 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) 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 limited to *relevant professional advisers* as defined by the *2010 Act*. Further guidance on the privilege reporting exemption can be found in section 7.4 of this guidance.

7.3.25 The MLRO may want to make reasonable enquiries 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.

7.3.26 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

7.3.27 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). It is understood that this provision is 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.

7.3.28 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.

7.3.29 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?

7.3.30 The following details are required by the *STR* report to be completed and 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. They are also required to respond, as soon as practicable to any request for additional information made by FIU or Revenue.

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

7.3.32 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.

If there are any queries on registering on goAML, the submission of STRs or submitting STRs, *FIU Ireland* may be contacted on the goAML Message Board or as follows:

by email : FIU-Ireland@garda.ie or

by telephone : 003531 6663730

by post: Finance Intelligence Unit (FIU),Garda National Economic Crime Bureau (GNECB), Clyde House, Ballycoolin, Dublin 15. D15 Y6NT.

Confidentiality

7.3.33 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).

7.3.34 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

7.3.35 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.

7.3.36 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.

7.3.37 For the *MLRO's* efficiency and ease of reference, a reporting index may be kept and each internal *STR* given a unique reference number as this internal reference number is a mandatory field when submitting an STR on ROS.

7.4 Reporting and the privileged circumstances exemption in section 46 of the 2010 Act

7.4.1 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.

7.4.2 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."

7.4.3 *Relevant professional advisers* who know about or suspect *MLTF* (or have reasonable grounds for) 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 which also extends to other documentation and advice.

7.4.4 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.

7.4.5 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.

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

Discussion with the MLRO

7.4.7 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*.

The crime/fraud exception

7.4.8 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.

7.4.9 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 continue evasion, then an *external report* could be required.

7.4.10 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 adviser*s (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*)?

7.4.11 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.

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

7.5.1 As noted above, *external reports* must be made as soon as practicable. Section 42(7) of the *2010 Act* requires an *accountancy firm* to make an *external STR* 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.

7.5.2 These exceptions do not apply to situations where the *accountancy firm* has received a valid direction from An 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).

7.5.3 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 by providing the service (as instructed by the *client*).

Proceeding with a transaction or service

7.5.4 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 about, 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 arising 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 *clients* when the money is suspected of having criminal origins.

7.5.5 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*. In such an instance the auditor should discuss this item with the MLRO and/or consider seeking legal advice where relevant.

Instructions not to proceed with a transaction or service

7.5.6 Under Section 17(1), a member of An 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 E.

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

Client relationships

7.6.1 *Accountancy firms* do not have to stop working after submission of an *external STR* unless a direction of an appropriate member of An Garda Síochána (rank of superintendent or above) or an order from a judge of the District Court is received (See APPENDIX E: DIRECTIONS FROM An GARDA SÍOCHÁNA OR COURT REGARDING PROCEEDING WITH *A* TRANSACTION OR **SERVICE**), 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.

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

7.6.3 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.

7.6.4 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 (*for example an STR*)*.

Balancing professional work and the requirements of the 2010 Act

7.6.5 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 7.2.5 to 7.2.1) 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.

7.6.6 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*.

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

7.6.8 *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, An 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 Corporate Enforcement Authority 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

7.6.9 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 An Garda Síochána in order to understand their perspective and document such discussion.

7.6.10 Such a discussion with An 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 consider seeking legal advice and potentially the directions of the Court to protect itself.

7.6.11 *Accountancy firm*s 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 (if any) by professional bodies.

7.7 Requests for further information

Requests from FIU Ireland and/or the Revenue Commissioners

7.7.1 *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 An 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 in order to carry out its functions. For example, *FIU Ireland* can make a request in writing to ascertain if the designated person has a *business relationship* with a named person. 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. FIU or Revenue may seek such information, for example, if required for the proper analysis of STRs. All written requests for information from *FIU Ireland* will be sent on the goAML message board.

7.7.2 Before responding to the Revenue Commissioners, it is recommended that a verification process is undertaken to ensure the person making contact is a bona fide member of 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.

7.7.3 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.

7.7.4 However, if the request is for production of documents or provision of information over and above the provisions of 40C (3) or s42(6A) of the 2010 Act, 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*.

7.7.5 Before providing information to a member of An Garda Síochána other than in *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 firm*s may attend the premises of the relevant agency to hand over the information.

7.7.6 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
- what information should be excluded *e.g.,* that subject to

legal privilege

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

7.7.7 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 consider seeking legal advice.

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

Requests regarding client identification or information regarding suspicious transactions

7.7.8 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

7.7.9 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.

7.7.10 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.

Secondees and those temporarily working outside of Ireland

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.

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.

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.

8. 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? (see section 9.1)
- 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?

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

8.1.1 Section 55 of the 2010 Act contain detailed provisions relating to record keeping. 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 relationship*s 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.

8.1.2 All records related to an *occasional transaction* must be retained for five years after the date of the *transaction*. A member of An Garda Síochána may give an *Accountancy Firm* a direction in writing to retain documents and other records for a period, up to a maximum of 5 years, additional to the initial 5-year period.

8.1.3 The 2010 Act does not specify the medium in which records should be kept, but they must be readily retrievable. *Accountancy firms* using solutions for their AML compliance should ensure their providers are compliant with this requirement.

8.2 What should be considered regarding retention policies?

8.2.1 *Accountancy firms* must be aware of the interaction between of *MLTF* laws with the requirements of the GDPR. The Irish 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. Retaining the records required, for the period required by the MLTF laws is never a breach of GDPR. A subject access request under GDPR legislation, for information included in a *suspicious transaction report* should not be complied with by the practices as to do so would be an offence under the "*tipping off*" rules.

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

8.3.1 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* or the firm's determination of whether to discount the suspicion
- requests received for additional information in accordance with Section 42(6A) of the *2010 Act* sent to the *FIU Ireland* and Revenue Commissioners, and/or its responses to such requests
- Copies of requests received from *FIU Ireland* or Revenue Commissioners in accordance with Section 40 C(3) 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

8.3.2 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.

8.4 Where should reporting records be located?

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.

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

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 sufficient 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. For further details on reliance and outsourcing, please refer to Chapter 10.

8.6 What are the requirements regarding the deletion of personal data

Section 55 of the 2010 Act provides that on the expiry of the retention periods referred to in the section a designated person shall ensure that any personal data contained in any document or other record retained solely for the purposes of the section is deleted.

9. 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?

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

9.1.1 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 *transaction*s and other events which may be related to MLTF, as well as to identify and report anything that gives grounds for suspicion (see Section 7 of this guidance).

9.1.2 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 additional training, and members of *senior management* may also benefit from a customised approach or some supplementary additional training. Training must be provided initially for new staff and there should be regular refresher training for all staff. The training provided should be sufficient in terms of time and in -depth enough for the person being trained to understand their legal obligations in relation to MLTF relevant to their role in the firm. The training provided should reflect the risk of the role.

9.1.3 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.

The records relating to training 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.

9.1.4 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.

9.1.5 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.

9.2 What should be included in the training?

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

9.2.2 The programme itself should include:

- an explanation of the law within the context of the *firm's* own commercial activities
- the *firm's* AML policies and procedures
- how to identify a *transaction* or other activity that may be related to money laundering or *terrorist financing*, and how to proceed once such a *transaction* or activity is identified
- 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)
- 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 7 of this guidance)
- procedures for escalating any issues to *senior management*/MLRO for further investigation
- record retention requirements related to AML activities
- compliance with sanction requirements

It is recommended, as good practice, that AML training would include an assessment to demonstrate the employee's understanding at completion of the training. Under AMLD 6 assessment of individual skills, knowledge and expertise will be compulsory from July 2027. See further at Chapter 11.

9.2.3 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, *firms* 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*.

9.2.4 Records should be kept showing who has received training, the training received and when training took place (see above). 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, when legislation in this area changes or when the role of an individual changes.

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

9.2.6 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.

9.3 When should training be completed?

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

9.3.2 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, the output and findings of ongoing *monitoring* of AML compliance (Ref 3.3.20) and the internal reporting of contraventions of the 2010 Act (See 3.3.22), and service lines.

9.3.3 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.

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

10. RELIANCE AND OUTSOURCING

10.1 Introduction

10.1.1 In the context of using third parties to support *CDD* activities (Sections 33 or 35 (1) of the *2010 Act*[1]), *accountancy firms* can use various frameworks depending on the nature of the relationship established between the firm and the third party. The frameworks that can be used include:

- **Reliance on relevant third parties** where a firm uses another designated entity to perform *CDD* activities on its behalf. Reliance is placed on the third party's AML policies and procedures.
- **Outsourcing to a service provider** where a firm delegates *CDD* activities to a third party and activities are performed based on the AML policies and procedures of the firm outsourcing to the third party.

10.1.2 One of the main differences between reliance and outsourcing includes which entity is managing AML policies and procedures. In the case of reliance, the third party (another designated entity) uses its own AML policies and procedures and in the case of outsourcing, it is the firm outsourcing to the third party which manages AML policies and procedures. As noted above, the type of third party also differs between reliance and outsourcing – in reliance, the third party is another designated entity and in outsourcing, it is generally a service provider company (which may/may not be a designated entity).

10.1.3 An *accountancy firm* that places reliance on a relevant third-party or uses an outsourced service provider remains liable for any failure to apply the required measures under the 2010 Act. In addition, firms relying on a relevant third-party or outsourcing to a service provider should establish policies and procedures for managing this activity including checks performed on the third party prior to establishing the arrangement, putting a reliance or outsourcing agreement in place with the third party, and firms should also oversee *CDD* activities performed by the third-party post establishment of the arrangement to ensure ongoing compliance with *CDD* requirements.

10.1.4 Where an *accountancy firm* chooses to implement a reliance or outsourcing framework, it is still obliged to maintain appropriate risk management procedures to prevent *MLTF*. This requires the *firm* to consider whether the establishment of a reliance or outsourcing framework 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. This could be considered as part of the firm's overall risk assessment process.

---

[1] **Section 33:** Identification and verification of customers and beneficial owners; **Section 35 (1)** A designated person shall obtain information reasonably warranted by the risk of money laundering or *terrorist financing* on the purpose and intended nature of a *business relationship* with a customer prior to the establishment of the relationship.

10.1.5 Where a *firm* contracts with a *client*, it remains responsible for ensuring that it undertakes *CDD* on that client to Irish standards, including maintaining the appropriate records even if execution of all or part of the *CDD* activities are outsourced or where reliance is placed on another designated entity.

10.2 Reliance on relevant third parties

10.2.1 Section 40 of the 2010 Act provides that *accountancy firm*s 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 *accountancy firm* and the relevant third party. Firms should consider implementing a signed reliance agreement with the relevant third party outlining a clear definition of *CDD* activities that the third party is performing on behalf of the firm and the associated obligations of the relevant third party appointed. The *accountancy firm* should also consider including details in their policies/procedures regarding the approach for identifying, assessing, selecting, and *monitoring* relevant third parties. 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 by a designated person include:

- *Credit institution*s
- *Financial institutions* (excluding undertakings solely providing foreign exchange or payment services)
- *external accountants*, auditors, *tax advisers* and *relevant independent legal professionals*
    - who are members of a Designated Accountancy Body, a supervised member of the Irish Taxation Institute or the Law Society of Ireland respectively;
    - supervised or monitored for compliance with 4AMLD (as amended) (or equivalent)[2] and who are subject to mandatory professional registration or mandatory

[2] **The meaning of ‘Supervised or monitored for compliance with’** in the requirements specified in 4AMLD (as amended) or equivalent per Section 40 (1A) of the amended Act refers to the case where ‘(a) the person and the designated person seeking to rely upon this section are part of the same *group*, (*b*) the *group* applies customer due diligence and record keeping measures and policies and procedures to prevent and detect the commission of money laundering and *terrorist financing* in accordance with the 4AMLD (as amended) or equivalent requirements, and (c) the effective implementation of the requirements referred to in *paragraph (b)* is supervised at *group* level by a competent authority of the state where the parent company is incorporated.

professional supervision under the laws of another Member State or a place (other than a member State) which is not a high risk third country; or

- who carry on business in a *High-risk third country*, are subject to mandatory professional registration or mandatory professional supervision under the laws of the place and are a branch or majority-owned subsidiary of an obliged entity established in the Union, and fully complies with group-wide policies and procedures in accordance with Article 45 of the Fourth Money Laundering Directive (as amended).

- *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
  - supervised or monitored for compliance with 4AMLD (as amended) (or equivalent) and who are subject to mandatory professional registration or mandatory professional supervision under the laws of another Member State or a place (other than a member State) which is not a *High-risk third country*; or
  - who carry on business in a *High-risk third country*, are subject to mandatory professional registration or mandatory professional supervision under the laws of the place and are a branch or majority-owned subsidiary of an obliged entity established in the Union, and fully complies with group-wide policies and procedures in accordance with Article 45 of the Fourth Money Laundering Directive (as amended).

10.2.2 The relevant third parties in the abovementioned places (i.e. places other than an EU Member State) must be supervised or monitored in the place for compliance with requirements equivalent to those specified in the fourth Money Laundering Directive (as amended).

10.2.3 *Accountancy firms* may rely on a relevant third party to carry out their *customer due diligence* measures, but the firm remains liable for any failure in the *customer due diligence*.

10.2.4 Reliance is permitted only if the other party is required to apply the requirements of the fourth Money Laundering Directive (as amended) (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 fourth Money Laundering Directive (as amended).

10.2.5 Firms should note that where they place reliance on a relevant third party, they should enter into a reliance agreement. The reliance agreement should be in writing and signed/approved by the MLRO/*senior management*, and it should outline the obligations of the relevant third party to ensure that the third party will provide the *CDD* documentation as soon as practicable after a request (based on an established/agreed timeframe). The agreement should also contain details of what *CDD* documentation is needed and the format for providing *CDD* documentation by the relevant third party to the designated person. The reliance agreement should include the following:

- The designated person, when relying on a relevant third party should document the specific services provided by the relevant third party
- The documented arrangement must commit the relevant third party to applying appropriate controls to the provided services to prevent or mitigate the risk of money laundering/*terrorist financing*. This provision should ensure that the relevant third party applies controls equivalent to those that the designated person would implement if carrying out the *CDD* themselves
- That the relevant third party provides the designated person with *CDD* documentation or information as requested and as soon as is practicable after a request from the designated person based on established/agreed timeframe
- The provision of the *CDD* documentation or information to the designated person upon termination or ending of the arrangement
- It would also be expected that the designated person would have a right to inspect the premises and review the processes of the relevant third party to ensure compliance with the provisions of the documented agreement
- It is best practice to review the implementation of the reliance agreement at appropriate intervals to ensure it is applied correctly and effectively. Part of this review process should include a sampling of customer records as part of oversight performed by the designated person to confirm effectiveness and accuracy of *CDD* activities performed by the relevant third-party

- STR reporting protocols should be established (and included in the reliance agreement) where relevant, taking into account the obligation not to prejudice an investigation (*tipping off* requirements per Section 49 of the 2010 Act) and ensuring compliance with Section 52 of the 2010 Act in terms of permitted disclosures. For further details on permitted disclosures, please refer to section 7.2.9 of this guidance. If the reader is in doubt on any matter in this complex area, they should consider obtaining legal advice. *Accountancy firms* may on occasion need advice to assist them in considering such reporting issues.

10.2.6 Liability for inadequate *CDD* remains with the relying party. *Firms* placing reliance on another should satisfy themselves with the level of *CDD* being undertaken including performing checks on the third party prior to entering into the reliance arrangement to ensure the relevant third party can comply with the *CDD* requirements of the firm.

10.2.7 To manage reliance on relevant third parties, firms should also consider establishing reliance policies and procedures setting out how reliance arrangements are managed and governed. In addition, firms should consider any risks associated with reliance on a relevant third party and how these risks are mitigated in its firm wide risk assessment process.

10.2.8 STR reporting obligations remain the responsibility of the designated person where reliance on another designated entity is used for *CDD* activities.

10.3 Parties seeking reliance

10.3.1 A *firm* relying on a third party is not required to apply standard *CDD,* but it must still carry out a risk assessment and perform ongoing *monitoring* of the designated firms 'own *clients*. That means it should still obtain a sufficient quantity and quality of *CDD* information to enable it to meet its *monitoring* obligations.

10.3.2 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 (as noted above in section 10.2.5) that confirms that the party being relied on will provide copies of identification and verification documentation as soon as practicable after a request.

10.4 Parties granting reliance

10.4.1 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 them

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.

10.4.2 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.

10.5 Outsourcing to service providers

10.5.1 *Accountancy firms* may also outsource (Section 40 (7)) their customer due diligence measures (Sections 33 or 35 (1) of the 2010 Act) to a third party (service provider) but the firm would remain liable for any failure in the customer due diligence per requirements outlined in the 2010 Act.

10.5.2 When outsourcing to a service provider, *accountancy firm*s should consider establishing the following additional outsourcing oversight controls including:

- implementing an outsourcing policy/procedure covering the lifecycle of the outsourcing relationship including how the service provider is identified, assessed, and selected (checks performed prior to starting an outsourcing arrangement) and ongoing oversight of *CDD* activities performed by the service provider
- establishing an outsourcing agreement including agreed service levels to monitor and oversee outsourced activities (which should be included in the signed/approved outsourcing agreement)
- where volume of *CDD* activities outsourced is significant, consider implementing a key performance indicator (KPI) reporting protocol by the service provider to enable timely oversight of outsourced activities (and consider adding KPI reporting obligations in the signed outsourcing agreement)
- inclusion of standard clauses in the outsourcing agreement covering areas such as the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data associated with outsourced customer due diligence activities, obligations of the service provider to follow the *firm's* AML policies and procedures, management of STR reporting obligations, and protocols/exit strategy in the event of a termination of the outsourced relationship between the service provider and the *accountancy firm*
- consideration of any risks associated with outsourcing in the *firm* wide risk assessment process and details of how these risks have been mitigated

10.5.3 Regardless of any outsourcing arrangement, a *firm* remains responsible for reporting any knowledge or suspicion of *MLTF* it becomes aware of in the course of its own activities. *Firms* should establish a *MLTF* reporting protocol in the outsourcing agreement with the third party. If an *STR* is made by the outsourcing service provider, the *firm* should also consider and comply with its own reporting obligations. If the reader is in doubt on any matter in this complex area, they should consider obtaining legal advice. *Accountancy firms* may on occasion need advice to assist them in considering such reporting issues.

10.6 Subcontracting

10.6.1 *Accountancy firms* often subcontract to another member *firm* relating to specific client engagements for relevant service lines (audit, tax, consulting). Where the *firm* subcontracts, the *accountancy firm* should establish a policy/procedure outlining how subcontracting (to a member *firm*) can be used and how *CDD* activities are managed in the context of the subcontracting arrangement. This includes consideration of who owns the relationship and engagement letter with the underlying client (e.g., where it is the *firm* which owns this relationship, the *firm* will be responsible for performing *CDD* activities). In cases where the relationship and the engagement letter is between the member *firm* and the client, consideration of the impact of the AML risk (low or high risk) of the jurisdiction where the member *firm* is located should occur including how this may impact performance and responsibilities for *CDD* activities.

10.6.2 Subcontracting arrangements should also be subject to a written agreement (engagement terms) outlining the rights of the *accountancy firm*/obligations of the subcontractor. The agreement should consider including the terms of the engagement regarding the scope of the work involved, fees payable, and confirmation that the services will be performed in accordance with applicable firm's global policies.

10.6.3 Other subcontracting cases to consider include:

- 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. This situation can arise in, for example, when specialist tax advice is sought by one accounting practice from another and in this case the "client" for *CDD* purposes may be the practice and not the ultimate client indirectly seeking the advice.
- 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*.

10.6.4 When a sub-contractor is integrated into an Irish business, subcontractor staff should be trained in the *MLTF* procedures adopted by that *firm* so that common standards can be implemented across the *firm*.

10.6.5 Where all or part of a piece of work is contracted out to a subcontractor, protocols for managing reporting of suspicious *transactions* should 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.

11. CHANGES FOR AMLD 6

11.1 Introduction

11.1.1 The European Union 6th Anti Money laundering package entered into force on 9 July 2024. It comprises:

11.1.2 A regulation on the prevention of the use of the financial system for the purposes of money laundering or *terrorist financing: AML Regulation*. ((EU)2024/1624).

11.1.3 A directive on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or *terrorist financing: AML Directive***.** ((EU) 2024 /1640).

11.1.4 There was also a directive adopted to establish the European Anti Money Laundering Authority *AMLA*. This chapter focusses on some of the changes to the current anti -money laundering regime which will occur because of the *AML Regulation* and the *AML Directive*. These changes will take effect in the main from 10 July 2027 when the current 4 *AML Directive* (2015/849) as amended by 5 *AML Directive* (2018/843) (referred to from now on in this chapter as AMLD4 (as amended)) is repealed by the *AML Directive*. Any changes referenced below to be made under *AML Regulation* and *AML Directive* will occur on 10 July 2027 unless otherwise specified.

11.1.5 With the new package, the rules applying to the private sector will be transferred to the *AML Regulation*, the *AML Regulation* contains the bulk of the new framework. For example, who obliged entities are, internal policies, procedures and controls of obliged entities, compliance function, employees, outsourcing, customer due diligence, politically exposed persons, reporting obligations, information sharing, limits on large cash payments, beneficial ownership transparency. (The *AML Directive* also contains provisions on beneficial ownership - see further below).

11.1.6 Some key matters which the *AML Directive* will deal with are the organisation of institutional AML/CFT systems at national level in the member states. It lays down rules about setting up and accessing central beneficial ownership registers, tasks and responsibilities of national *Financial Intelligence Units (FIUs)*, co-operation between competent authorities and exchange of information.

11.1.7 In many respects, the main obligations under the *AML Regulation* reflect the requirements under the existing regime under AMLD 4 (as amended) but in the form of a regulation. However, there are several areas where the requirements are more prescriptive.

11.1.8 There is a strong theme in the *AML Regulation* and the *AML Directive* for the provisions of the legislation to be supplemented by *AMLA* delivering guidance and regulatory technical standards.

11.2 General

Obliged entities – extended scope

11.2.1 There have been several additions of obliged entities which will be subject to EU AML/CFT rules upon coming into force of the AML Regulation. Readers should consult the AML Regulation for full details. For example, the provisions under AMLD 4 (as amended) whereby traders in goods to the extent that payments are made or received in cash in an amount of EUR 10, 000 or more are obliged persons have been changed to include traders in luxury goods, including precious metals, stones, yachts, and cultural goods. Cultural goods and high value goods are defined in the AML Regulation. Obliged entity also includes all crypto asset service providers. They have been specifically included as designated persons under Irish law since the coming into force of S.I. No. 724 of 2024.

11.3 Governance

Policies and Procedures

11.3.1 Policies and procedures are applicable across various AML related areas. The AML Regulation harmonises and clarifies the scope of internal policies, procedures and controls that obliged entities must put in place. Internal policies should be approved by the management body. Internal procedures and controls should be approved at least at the level of the compliance manager.

11.3.2 Article 9 of the AML Regulation provides that obliged entities must have internal policies and procedures to include the following:

- Carrying out and updating of the Business Wide Risk Assessment (BWRA) (this is the *Accountancy firm*'s firm wide risk assessment);
- Risk management framework;
- *Customer due diligence (CDD*) including procedures to determine if a customer or a beneficial owner is a politically exposed person, family member or *close associate*;
- Reporting suspicious *transaction*s;
- Outsourcing and reliance on customer due diligence done by other obliged entities;
- Record retention and processing personal data;
- *Monitoring* and managing compliance with internal policies and procedures, identifying and managing deficiencies and implementing remedial actions;
- Verification of good repute when recruiting and assigning staff and appointing agents and distributors;
- Communication of internal policies procedures and controls including to agents, distributors and service providers involved in implementing AML/CFT policies;
- Internal controls and independent audit function;
- Training employees, agents, distributors;

- Implementation of a sanctions compliance programme as part of a firm's AML internal policies, procedures and controls. See more under separate "Financial Sanctions" heading at 11.9 below.

11.3.3 Article 13 of the *AML Regulation* requires obliged entities to have in place procedures to prevent and manage conflicts of interest that may affect the carrying out of tasks related to the obliged entity's compliance with the *AML Regulation*.

Compliance Function, Money Laundering Reporting Officer (MLRO)

11.3.4 In Ireland, there is currently no legal requirement on a firm to appoint an MLRO unless requested by its designated accountancy body. However, where appropriate to the size, complexity and structure of an *Accountancy firm* and in the light of the legal requirements imposed, the firm may find it beneficial to appoint an individual at management level or to appoint a member of *senior management*, a '*money laundering reporting officer' ("MLRO")* with responsibility for ensuring the firm's compliance with the Irish anti-money laundering regime. Both Chartered Accountants Ireland and Association of Chartered Certified Accountants require firms to have a nominated MLRO.

11.3.5 Article 11 of the *AML Regulation* deals with compliance function. Under the *AML Regulation* there is an obligation to:

- appoint a member of the management body as compliance manager. This person will ensure consistency with risk exposure and implementation of policies, procedures and controls and is obliged to report to the management body once a year on implementation of internal policies, procedures and controls;
- appoint a compliance officer. This person is responsible for day-to-day AML CFT implementation of requirements and for making *suspicious transaction reports*.

11.3.6 Adequate resources must be allocated to, and adequate powers must be given to the compliance manager and officer to carry out their functions. There are protections to these *individuals* given in the *AML Regulation* (Article 69) against retaliation, discrimination and any other unfair treatment for carrying out their tasks which protections may need to be incorporated into their employment terms.

11.3.7 The *AML Regulation* provides that where the nature of the business of the obliged entity, including its risks and complexity, and its size justify it, the functions of the compliance manager and the compliance officer may be performed by the same natural person. Those functions may be cumulated with other functions.

11.3.8 Under Article 9 (4) of the Regulation, *AMLA* will provide guidelines by July 2026 including on this area. *AMLA*'s work programme issued in January 2026 indicates that these guidelines will be consulted on in 2027.

Independent Audit Function

11.3.9 As part of the internal policies, procedures and controls that obliged entities are required to have in place under the *AML Regulation*, they must have

internal controls and an independent audit function to test the internal policies and procedures and the controls in place in the obliged entity; in the absence of an independent audit function, obliged entities may have this test carried out by an external expert. Obliged entities must ensure that the person responsible for the audit function can report directly to the management body. Independent audit appears to be mandatory under the *AML Regulation*.

Employees

11.3.10 Article 46 of AMLD 4 (as amended) requires obliged entities to take measures including participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or *terrorist financing*, and to instruct them as to how to proceed in such cases.

11.3.11 When the *AML Regulation* is implemented, obliged entities will be required to take measures to ensure employees, agents, distributors and the like are aware of AML requirements and these measures include participation of those employees, agents, distributors in specific ongoing training programmes to help them recognise operations which may be related to money laundering or *terrorist financing* and to instruct them how to proceed in such cases.

11.3.12 Article12 of the *AML Regulation* references business wide risk assessment (this is the *Accountancy firm*'s firm wide risk assessment) and processing of personal data in the context of training areas.

11.3.13 Under article 13 of the *AML Regulation* (which deals with Integrity of Employees) persons such as employees, agents and distributors directly participating in the obliged entity's compliance with anti-money laundering laws must be assessed as having appropriate skills, knowledge and expertise to carry out their functions effectively. The assessment will also consider their honesty and integrity and whether they are of good repute. It is not clear if there will be guidance on how to test this. The *AML Regulation* (Article 9 2(a)(viii)) requires the obliged entity to have a policy/procedure for verification that staff, agents and distributors are of good repute.

11.4 Outsourcing and Reliance

11.4.1 Current provisions on outsourcing are contained in AMLD4 (as amended). These will be repealed from 10 July 2027. Thereafter the provisions contained in the *AML Regulation* (and any rules in *RTSs* or guidelines) will regulate outsourcing.

11.4.2 Outsourcing is permitted under Article 18 of the *AML Regulation*. There is an obligation to notify the supervisor of outsourcing prior to carrying out of the task. 'Supervisor' is defined and means the body entrusted with responsibilities aimed at ensuring compliance by obliged entities with the requirements of the *AML Regulation*. The obliged entity must have an outsourcing policy/procedure.

11.4.3 Certain tasks cannot be outsourced:

- Proposal & approval of the business wide risk assessment (this is the *Accountancy firm*'s firm wide risk assessment);
- Approval of internal policies, procedures, controls;

- Decisions on customer risk profile;
- A decision to enter a *business relationship* or carry out an *occasional transaction*;
- The reporting to FIU of suspicious activities or the threshold-based reports in articles 74 and 80 of the *AML Regulation* except where such activities are outsourced to another obliged entity belonging to the same *group* and established in the same Member State;
- Approval of criteria for detecting suspicious or unusual *transaction*s or activities.

11.4.4 The obliged entity must assure itself that the service provider is sufficiently qualified to carry out the tasks to be outsourced.

11.4.5 A written agreement about applying the obliged entity's policies & procedures must be entered into with the outsourcer. The obliged entity must perform regular controls to ascertain the effective implementation of such policies and procedures by the service provider. The frequency of such controls shall be determined based on the critical nature of the tasks outsourced.

Current regime	**New regime under AML Regulation**
Outsourcing permitted	Outsourcing permitted
Not specified that certain tasks are prohibited	Certain tasks cannot be outsourced
Prior notification to supervisor not specified	Prior notification to supervisor required
Prohibition on reliance on 3rd parties in high-risk 3rd countries	Prohibition on reliance on 3rd parties in high-risk 3rd countries
Saver from prohibition on high-risk 3rd countries under certain conditions	Saver from prohibition on high-risk 3rd countries for *group* situations with certain conditions

11.4.6 Article 48 of the *AML Regulation* continues to permit reliance on other obliged entities to meet *customer due diligence* requirements. This is provided that the third party is a person situated in a member state/third country which applies *CDD* and record keeping requirements as laid down in the *AML Regulation* or equivalent and is supervised in a manner consistent with the *AML Directive*. Reliance is not permitted on obliged entities established in high risk third countries or third countries with AML /CFT compliance weaknesses (save in *group* situations under certain conditions).

11.4.7 The relevant sections of the *AML Regulation* on outsourcing and reliance provide that *AMLA* will issue guidelines on outsourcing and reliance.

11.5 Business-wide Risk Assessments (BWRAS)

11.5.1 Current provisions on BWRAs include a requirement to have the BWRA approved by *senior management*, persons carrying out a *business risk assessment* must have regard to any guidance on risk issued by the *competent*

authority for the *designated person* and certain risk factors must be taken into account.

11.5.2 Article 10 of the *AML Regulation* specifically deals with BWRAs, and Annex 1 now includes a non-exhaustive list of risk variables for obliged entities to consider. Article 10 also includes items to consider for risk assessment and calls out other items to consider including Union level risk assessment and Union level/*AMLA* publications.

11.5.3 Under the A*ML Regulation*, the BWRA must be drawn up by the Compliance Officer and approved by the management body in its management function and where it exists it must be communicated to the management body in its supervisory function.

11.6 Customer Due Diligence

When should *CDD* be done?

11.6.1 For the first time, pursuant to Article 26, the *AML Regulation* introduces a timeframe for ongoing *monitoring* rules for obliged entities. It mandates *CDD* refresh every 5 years for all customers. For higher-risk customers, updates must be carried out on an annual basis.

11.6.2 In addition to the current provisions some new situations will require *CDD* under the *AML Regulation*.

Requirement for *CDD* under current regime (Article 11 AMLD4 (as amended)	**Requirement for *CDD* under AML Regulation (Article 19).**
When establishing a *business relationship*	When establishing a *business relationship* (Art 19 1 (a))
Occasional transactions €15,000 or more*	*Occasional transactions* at least €10,000 (*Art.*19* 1 (b))
Suspicion of ML/TF regardless of derogation exemption or threshold	Suspicion of ML/TF regardless of derogation exemption or threshold (Art.19 1 (d))
Doubts about veracity/adequacy of previously obtained customer identification data	Doubts about veracity/adequacy of previously obtained customer identification data (Art.19 1 (e))
Gambling service providers ...*transaction*s amounting to €2,000 or more	Gambling service providers ...*transaction*s amounting to at least €2,000 (Art.19 5)
Occasional transaction of transfer of funds exceeding €1,000	*Occasional transaction* of transfer of funds of value at least €1,000 (exception with more stringent rules for crypto asset service providers –see further below) (Art.19 2)
-	where an obliged entity is participating in the creation of a legal entity, the setting up of a legal arrangement or, for obliged entities including auditors, *external accountants* and *tax advisers* in the transfer of ownership of a

	legal entity, irrespective of the value of the *transaction*. (Art.19 1 ©)
-	when there are doubts as to whether the person the obliged entity is interacting with is the customer or person authorised to act on the customer's behalf. (Art.19 1 (f))

*See further at 5.3.6 below on *occasional transaction*s

What *CDD* should be done?

11.6.3 In general, *CDD* measures to be applied under the *AML Regulation* are consistent with the current AMLD 4 (as amended) regime but there are some additional mandatory *CDD* measures. This includes seeking information on the nature of the customer's business additionally in the case of *occasional transactions*. Also, under the *AML Regulation*, obliged entities will be required to verify whether the customer or the beneficial owner(s) are subject to targeted financial sanctions. See section below on financial sanctions.

What's extra or new in *CDD* measures under the *AML Regulation*?

Documenting *CDD* actions

11.6.4 Currently AMLD 4 (as amended) requires documentation of *CDD* actions. It requires [Article 13 (1)(d)] that documents, data or information held are kept up to date and the keeping of records in a case where there are difficulties verifying beneficial owners. It also requires retention of *CDD* documents for 5 years after the end of the *business relationship* with their customer or after the date of an *occasional transaction* [Article 40].

11.6.5 The *AML Regulation* provides more detail whereby it requires obliged entities to keep a record of the actions taken in order to comply with the requirement to apply *customer due diligence* measures, including records of the decisions taken and the relevant supporting documents and justifications. Consideration must be given as to how decisions and justifications are documented. Where there are serious concerns, for example, where a potential client may be denied onboarding or is off boarded, legal advice may be required, to avoid any potential legal exposure.

11.6.6 The documents, data or information held by the obliged entity are to be updated whenever the *customer due diligence* is reviewed in accordance with ongoing *monitoring*. The obligation to keep records also applies to situations where obliged entities refuse to enter into a *business relationship*, terminate a *business relationship* or apply alternative measures.

Identity and verification requirements of customers under *AML Regulation*

11.6.7 The *AML Regulation* brings further granularity to *CDD*. There are more detailed requirements in respect of the identification of the customer and verification of the customer's identity. Below is a summary (only) and readers must consult the *AML Regulation* for exact details.

11.6.8 Article 22 of the *AML Regulation* provides "with the exception of cases of lower risk to which measures under section 3 apply", the information below should be collected. The referencing to section 3 may seem confusing, but this should be cross-referred to section 3 (which is article 33 onwards). Taking into account risk factors this allows for less information to be collected in relation to certain aspects of the client.

Natural person

Names and surnames

Place and full date of birth

Nationalities (or statelessness, refugee, subsidiary protection) national identification no. (where applicable)

the usual place of residence or, if there is no fixed residential address with legitimate residence in the Union, the postal address at which the natural person can be reached and, where available the tax identification number

11.6.9 The wording of the provision in relation to tax identification number is ambiguous. Subject to clarification in an *RTS* or *AMLA* guidance, the better view is that a tax identification number must be obtained where one exists.

Legal Entity

Legal form and name

Office address

Names of legal representatives, registration no., tax identification no., legal entity identifier

Names of shareholders, holders of directorships

11.6.10 The *AML Regulation* also details *CDD* provisions for trustees and other organisations having legal capacity under national law.

Identifying a beneficial owner for *CDD*

11.6.11 Under the *AML Regulation*, in order to identify a beneficial owner an obliged entity must collect certain information (see Article 62). The details vary depending on the nature of the entity. This includes names, surnames, place and full date of birth, residential address, country of residence, nationality of the beneficial owner, number of identity document, unique personal identification number (if it exists) assigned to the person, the nature and extent of the beneficial interest held in a legal entity / arrangement, and the date as of which the beneficial interest is held. A future RTS on Customer Due Diligence (currently in draft form and being consulted on by *AMLA* as of the date of

publication of this Technical Release) will provides further detail on verification of beneficial owner.

Simplified due diligence measures

11.6.12 AMLD 4 (as amended) permits simplified *customer due diligence* measures where areas of lower risk are identified [article 15]. The *AML Regulation* provides an exhaustive list of the simplified measures (performed by taking into account risk factors set out in in Annexes II and III) that obliged entities can apply (see Article 33): -

- Verifying the identity of the customer/beneficial owner after establishing the *business relationship* (but within 60 days)
- Reducing the frequency of customer identification updates
- Reducing the amount of information collected relating to the purpose/nature of *business relationship* or *occasional transaction*
- Reducing frequency /degree of scrutiny of customer *transaction*s
- Applying other relevant simplified DD measures identified by *AMLA*

11.6.13 Under the *AML Regulation*, obliged entities must regularly verify that conditions for simplified DD continue to exist and pursuant to Article 33 (5) cannot apply simplified DD in certain cases:

- doubt as to veracity of information provided;
- factors indicating lower risk are no longer present;
- *monitoring* of the customer's *transaction*s and the information collected in the context of the *business relationship* exclude a lower risk scenario;
- there is a suspicion of money laundering or *terrorist financing*;
- there is a suspicion that the customer, or the person acting on behalf of the customer, is attempting to circumvent or evade targeted financial sanctions.

***Enhanced due diligence*:**

11.6.14 The *enhanced due diligence* measures in the *AML Regulation* are largely similar to AMLD 4 (as amended) such as getting more information on a customer or source of funds but there are a couple of new measures to mention. For example, the *AML Regulation* requires additional *enhanced due diligence* measures to be applied to *business relationships* identified as having a higher risk which involve the handling of assets with a value of at least EUR 5,000,000 for certain customers with assets over EUR 50,000,000. This is largely aimed at personalised asset management services, but it also applies to *trust or company service provider*s and is therefore potentially relevant to *accountancy firms*.

Occasional Transactions* – Obligation to do *CDD

11.6.15 Article 19 of the *AML Regulation* lowers the EU wide threshold for the application of *CDD* for *occasional transactions* from a value of €15,000 to €10,000.

11.6.16 Further, obliged entities may also need to apply *CDD* for particular lower value *transaction*s.

11.6.17 *CDD* must be applied for a transfer of funds within the meaning of the transfer of funds regulation (2023/1113) where the *transaction* amounts to a value of at least €1,000.

11.6.18 The obligation for *CDD* in the case of crypto asset service providers is stricter with an obligation imposed to apply certain *CDD* measures when carrying out an *occasional transaction* of at least €1,000 and limited *CDD* (identify and verify the identity of their customers) even when the value of the *transaction* is below €1,000.

11.6.19 When an *occasional transaction* is in cash then under the *AML Regulation* limited *CDD* measures must be applied for such *occasional transactions* in cash amounting to a value of at least €3,000.

***Electronic money* derogation**

11.6.20 The derogation under article 12 of AMLD 4 (as amended) is contained in Article 19 (7) of *AMLD 6* with an exemption from *CDD* measures for *electronic money*. The threshold of €150 still applies and reference is now made to the payment instrument not being linked to a payment account and not permitting any stored amount to be exchanged for cash or for crypto assets.

Limits to large cash payments

11.6.21 From 10 July 2027, under article 80 of the *AML Regulation*, persons trading in goods or providing services may accept or make a payment in cash only up to an amount of € 10,000. This applies whether the *transaction*s are single or linked. Member states can set lower limits. The limit does not apply to payments between natural persons who are not acting in a professional capacity and payments or deposits at *financial institutions*. In the case of such a payment or deposit at a *credit institution* of cash in excess of €10,000, there is an obligation under Article 80 to report this to the FIU. The preamble to the *AML Regulation* (para 162) explains that such a large cash payment (over €10,000) should not, by default, be considered an indicator for suspicion of money laundering, its *predicate offences* or *terrorist financing* but the reporting of such *transaction*s enables the FIU to assess and identify patterns concerning the movement of cash.

Verification- Electronic and Other

11.6.22 Article 22(6) of the *AML Regulation* specifies two means by which obliged entities can obtain information, documents and data necessary for the verification of the identity of the customer (and of any person purporting to act on their behalf).

11.6.23 One is using electronic identification means which meet the requirements of Regulation (EU) No 910/2014 [3]. This is arguably more stringent than AMLD 4 (as amended) which includes such electronic identification and trust services

[3] with regard to the assurance levels 'substantial 'or 'high', or relevant qualified trust services as set out in that Regulation.

under Reg 910/2014, *or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities*.

11.6.24 The other way to verify set out in the *AML Regulation* is by submission of identity documents and acquiring information from reliable independent sources whether accessed directly or obtained through a customer. (There are similar provisions in AMLD4 (as amended)).

11.6.25 Readers should also refer to the draft RTS referred to in section 11.6.11 above, Article 6 for further proposed guidance on verification. In addition to the above verification, the *AML Regulation* requires obliged entities to verify information on beneficial owners by consulting the central registers. AMLD 4 (as amended) requires that obliged entities do not rely exclusively on the central register to fulfil their *customer due diligence* requirements.

Annexes-higher and lower risk factors and risk variables

11.6.26 As with AMLD 4 (as amended), Annexes II and III of the *AML Regulation* set out lower and higher risk factors to be taken into account. Annex II, lower risk factors, is unchanged from that in AMLD 4 (as amended). Annex III, higher risk factors, has had some changes made to it from the Appendix in AMLD4 (as amended).

11.6.27 In addition, a new annex (Annex I), has been included in the *AML Regulation* called an indicative list of risk variables. The new annex contains a non-exhaustive list of risk variables that obliged entities should take into account when drawing up their risk assessment (See also BWRA at 11.5 above) and when determining to what extent to apply *customer due diligence* measures in accordance with *AML Regulation* Article 20.

High Risk Third Countries

11.6.28 The approach to identification of *high risk third countries* in the *AML Regulation* is different to AMLD 4 (as amended). While AMLD 4 (as amended) identifies third country jurisdictions with strategic deficiencies, the *AML Regulation* identifies (1) *high risk third countries* with significant strategic deficiencies but also (2) *high risk third countries* with compliance weaknesses and (3) *high risk third countries* posing a specific and serious threat to the Union's financial system. In the case of countries with compliance weaknesses, the EU Commission will take into account, as a baseline for assessment, information on jurisdictions under increased *monitoring* by international organisations (such as *FATF*). The countermeasures to mitigate money laundering and *terrorist financing* threats from outside the Union in Article 35 of *AML Regulation* are the same as those in AMLD 4 (as amended) (see Article 18a 2&3).

11.7 Politically Exposed Persons (PEPS)

Differences in Definition of Politically Exposed Person (see Article 2 paragraph 1, point 34)

Current regime	New regime under AML Regulation
	In a member state
heads of State, heads of government, ministers and deputy or assistant ministers	(a)(i)) heads of State, heads of government, ministers and deputy or assistant ministers
members of parliament or of similar legislative bodies	(a)(ii) members of parliament or of similar legislative bodies
members of the governing bodies of political parties	(a)(iii) members of the governing bodies of political parties that hold seats in national executive or legislative bodies, or in regional or local executive or legislative bodies representing constituencies of at least 50 000 inhabitants
members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;	(a)(iv) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances
members of courts of auditors or of the boards of central banks	(a) (v) members of courts of auditors or of the boards of central banks
ambassadors, chargés d'affaires and high-ranking officers in the armed forces	(a) (vi) ambassadors, chargés d'affaires and high-ranking officers in the armed forces
members of the administrative, management or supervisory bodies of State-owned enterprises	(a) (vii) members of the administrative, management or supervisory bodies of enterprises controlled under any of the relationships listed in Article 22 of Directive 2013/34/EU either by the state, or, where those enterprises qualify as medium sized or large undertakings or medium sized or large *group*s, as defined in Article 3(3), (4), (6) and (7) of that Directive, by regional or local authorities
---	(a)(viii) heads of regional and local authorities, including groupings of municipalities and metropolitan regions, with at least 50 000 inhabitants
	(a)(ix) other prominent public functions provided for by Member States
directors, deputy directors and members of the board or equivalent function of an international organisation	(b) in an international organisation: (i) the highest-ranking officials, their deputies and members of the board or equivalent functions of an international organisation; (ii) representatives to a Member State or to the Union

---	© at Union level: functions at the level of Union institutions and bodies that are equivalent to those listed in points (a) (i), (ii), (iv), (v) and (vi)
---	(d) in a third country: functions that are equivalent to those listed in point (a)

11.7.1 Under the *AML Regulation* certain regional local and municipal heads are now caught within the *PEP* definition (see chart above).

11.7.2 The definition of family member has been widened in the *AML Regulation* to include the siblings of *PEPs* in cases where *PEPs* involve heads of state, heads of government, ministers, and deputy or assistant ministers and equivalent function at Union level or in a third country (see Article 2, paragraph 1, point (35)(d)). Also, where it is justified by their social and cultural structures and by risk, Member States may apply a broader scope for the designation of siblings as family members of politically exposed persons (see Article 2, paragraph 5).

11.7.3 The *AML Regulation* extends to *occasional transactions*, the obligation in AMLD4 (as amended) to obtain *senior management* approval, for *business relationships* with *PEPs*, establishing source of wealth and funds and conduct enhanced ongoing *monitoring* (see Article 42).

11.7.4 As with AMLD 4 (as amended), the *AML Regulation* requires as part of *CDD* that an obliged entity determines whether a customer or beneficial owner of a customer is a *politically exposed person*, a family member or a person known to be a *close associate*.

Prominent public function

11.7.5 Like AMLD 4 (as amended), the *AML Regulation* provides that prominent public functions shall not be understood as covering middle-ranking or more junior officials. (see Article 2, paragraph 2).

11.7.6 Article 43 of the *AML Regulation* requires each Member State to issue and keep up to date a list indicating the exact functions which, in accordance with its national laws, regulations and administrative provisions, qualify as prominent public functions. Member States must request each international organisation accredited on their territories to issue and keep up to date a list of prominent public functions at that international organisation.

11.7.7 The *AML Regulation* provides measures for persons who cease to be *politically exposed persons*. There is a nuanced change in wording from AMLD 4 (as amended) where Article 45 of the *AML Regulation* provides that due diligence measures should apply until the risks posed no longer exist but, in any case, for not less than 12 months following the time when the individual ceased to be entrusted with a prominent public function. AMLD 4 (as amended) requires the risk to be taken into account for at least 12 months and to apply appropriate

and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to *politically exposed persons*.

11.8 Beneficial Ownership

Beneficial ownership transparency

11.8.1 Under current provisions of AMLD 4 (as amended) beneficial owner in the case of corporate entities means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a *transaction* or activity is being conducted and includes at least a shareholding of *25% plus one share or an ownership interest of more than 25%* held by a natural person.

11.8.2 With effect from July 2027 under the *AML Regulation*, there is a nuanced change in wording where ownership interest in a corporate entity will mean direct or indirect ownership of *25% or more* of the shares or voting rights or other ownership interest in the corporate entity (see Article 52 (1)).

11.8.3 Also, the *AML Regulation* permits a lower percentage threshold where member states identify categories of corporate entities that are exposed to higher money laundering and *terrorist financing* risks. The beneficial ownership threshold can be lowered to 15% or even lower for corporate entities deemed as high-risk for money laundering and *terrorist financing* (see Article 52 (2)).

11.8.4 The *AML Regulation* sets out more detailed provisions than before to establish a consistent approach to identifying beneficial ownership. In the case of indirect ownership, that is calculated by multiplying the shares or voting rights or other ownership interests held by intermediate entities and by adding together the results from the various ownership chains.

11.8.5 In relation to what control means for the purposes of beneficial ownership, readers should refer in particular to Article 53 of the *AML Regulation*. It introduces extra criteria for control via other means such as right to appoint or remove the majority of members of a board, veto rights or decision rights or decisions regarding distribution of profits.

11.8.6 The *AML Regulation* contains provisions (see Articles 57-61) for identification of beneficial owners of express trusts and similar legal arrangements and collective investment undertakings.

Beneficial Ownership Register

General

11.8.7 Both the *AML Directive* and the *AML Regulation* contain provisions in relation to beneficial ownership. In relation to the central register, the *AML Directive* focusses on the mechanics of the *central register*, and the *AML Regulation* deals with obliged entities' obligations vis a vis the *central register*.

11.8.8 Like AMLD 4 (as amended), Article 10 of the *AML Directive* makes provision that beneficial ownership information must be held in a *central register*. The information in the *central register* must be available in machine readable

format. Information in registers will be available for 5 years after dissolution of the legal entity or 5 years after the legal arrangement has ceased to exist.

11.8.9 Article 10 of the *AML Directive* grants more powers to entities in charge of *central registers*. They can request any information necessary to identify and verify beneficial owners, including board resolutions, minutes of meetings, partnership agreements, trust deeds, powers of attorney, other contractual documentation. They can also carry out checks including on-site inspections to establish and verify beneficial ownership.

11.8.10 If no beneficial owner is identified, the *central register* must include a statement that there is no beneficial owner, or one cannot be identified. There must also be a justification as to why it was not possible to determine the beneficial owner and what constitutes uncertainty about the information. Details of natural persons who hold the position of senior managing officials must be provided.

11.8.11 Member states must ensure that information held in beneficial ownership registers is adequate accurate and up to date. They must also ensure verification of whether beneficial ownership information in registers concerns persons or entities designated in relation to financial sanctions and if so an indication on the register that the person or entity is so subject.

11.8.12 The *AML Regulation* requires obliged entities when entering new *business relationship*s with entities such as a legal entity, trustee of an express trust, person holding an equivalent position in a similar legal arrangement , as listed in Article 23 (4) of the *AML Regulation*, to collect valid proof of registration or a recently issued excerpt of the register confirming validity of registration (subject to registration of beneficial ownership information pursuant to the *AML Directive*).

11.8.13 Article 10 of the *AML Directive* contains provisions regarding discrepancies including a specific mention on the register that there is a discrepancy reported until it is resolved, and a time frame of 30 days (longer if the discrepancy is complex) for the entities in charge of managing central registers to resolve discrepancies.

11.8.14 The *AML Regulation* (Article 24) focusses on obliged entities' obligations in the case of discrepancies in the *central register*. It includes mandatory reporting without undue delay and in any case within 14 calendar days of their detection. There is an exception for minor errors where the obliged entity can request additional information from the customer (client).

Access rules for beneficial ownership registers

11.8.15 The current provisions are contained in AMLD4 (as amended) which require information on the beneficial ownership of corporate /other legal entities to be accessible in all cases to any member of the general public. Under a 2022 ECJ ruling the ECJ held invalid that accessibility to the general public. The court said it was a "serious interference" in the privacy and personal data rights of the beneficial owners.

11.8.16 Ireland responded to the CJEU ruling by implementing the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) (Amendment) Regulations 2023 on 13 June 2023. These changes mean that

there has been no change to the unrestricted access afforded for example to An Garda Síochána and *FIU Ireland* and no change to the restricted access granted, for example, to designated persons such as banks doing *customer due diligence*. However, others who seek access and are not in these categories must provide evidence of legitimate interest in inspecting the register by demonstrating that the person is engaged in preventing , detecting or investigating money laundering or *terrorist financing* offences and that the relevant entity about which information is sought is connected with persons convicted of money laundering or *terrorist financing* offences or holds assets in a *high risk third country*.

EU changes required by 10 July 2025

11.8.17 On the EU side, Article 74 of the *AML Directive* makes an interim amendment to AMLD 4 (as amended) which had to be transposed by 10 July 2025 in relation to the accessibility of central registers of beneficial ownership of corporates and trusts.

11.8.18 From that date information on beneficial ownership in the central registers of beneficial ownership of corporates and trusts must be accessible to:

- competent authorities and FIUs (without restriction)
- obliged entities (where required for customer due diligence purposes)
- those persons and organisations (in the case of corporate and legal entities) and natural or legal persons (in the case of trusts) that can demonstrate a legitimate interest in accessing that information. They will be able to access a more limited sub-set of the information stored on the relevant register namely: name, month, year of birth, country of residence and nationality of beneficial owner and nature and extent of beneficial interest held.

EU changes required by 10 July 2026:

Full access by competent authorities etc.

11.8.19 Under Article 11 of the *AML Directive*, from 10 July 2026 competent authorities, self-regulatory bodies, tax authorities, *AMLA*, EPPO, OLAF, Europol and Eurojust must have immediate, unfiltered, direct and free access to the information in the central registers. Obliged entities must have timely access, and the Article provides that member states may impose a fee on obliged entities.

More limited access for persons with legitimate interest

11.8.20 Under Article 12 of the *AML Directive*, from 10 July 2026 persons with legitimate interest will have access to the following information stored on the relevant register namely: name, month, year of birth, country of residence and nationality of beneficial owner and nature and extent of beneficial interest held. The Article sets out persons deemed to have a legitimate interest and includes the likes of journalists and civil society organisations which are connected with preventing or combatting money laundering or *terrorist financing*. Please refer to Article 12 to find out more about persons having a legitimate interest.

11.8.21 Under Article 13 of the *AML Directive*, which is also to be implemented by 10 July 2026, member states must ensure that entities in charge of central registers take measures to verify legitimate interest based on documents, information and data they obtain from someone seeking to access the register. Function or occupation of the applicant and (except for journalists and civil society organisations and the like) connection with the entity or arrangement whose information is sought will be taken into consideration.

11.8.22 Under Article 15 of the *AML Directive*, from 10 July 2026 access to information on the register may not be given in cases where the beneficial owner might be exposed to disproportionate risk of e.g. fraud, kidnapping, blackmail. Such possible exemptions are to be examined on a case-by-case basis.

11.8.23 Finally, on the information sharing side, Article 61 of the *AML Directive* provides in its general provisions for sharing of beneficial ownership information between competent authorities of member states or third counties in a timely manner and free of charge.

11.9 Financial Sanctions

"Targeted financial sanctions" and "UN financial sanctions" are defined in the *AML Regulation*.

11.9.1 Under Article 9 of the *AML Regulation* obliged entities must have in place internal policies, procedures and controls to apply targeted financial sanctions and to mitigate and manage the risks of non-implementation and evasion of targeted financial sanctions.

11.9.2 Under Article 10 of the *AML Regulation* there is a requirement to include the risks of non-implementation and evasion of targeted financial sanctions in an obliged entity's business-wide risk assessment.

11.9.3 Under Article 11 of the *AML Regulation* the compliance officer is responsible for implementation of targeted financial sanctions.

11.9.4 As part of *CDD* measures, obliged entities will be required to verify under Article 20(d) of the *AML Regulation* whether the customer or the beneficial owner(s) are subject to targeted financial sanctions. As part of ongoing *monitoring*, this requires regular verification. The frequency of the verification is commensurate with the exposure of the obliged entity and the *business relationship* to risks of non-implementation and evasion of targeted financial sanctions. Under Article 33 one of the cases where an obliged entity should refrain from simplified DD is where there is suspicion of circumvention or evasion of targeted financial sanctions.

11.9.5 Article 27 of the *AML Regulation* provides for temporary measures for certain customers/persons/entities subject to UN financial sanctions. For such customers/persons/entities obliged entities must keep records of:

(a) the funds or other assets that they manage for the customer at the time when UN financial sanctions are made public;

(b) the *transaction*s attempted by the customer;

(c) the *transaction*s carried out for the customer.

This article is to be applied between the time the UN financial sanctions are made public and the time of application of the relevant targeted financial sanctions in the EU.

11.9.6 The above provisions effectively bring sanctions compliance into the *AML* compliance framework. They may bring about a requirement to update the procedures manual (article 9), and they also require ongoing *monitoring*. Obliged entities are expected to use their *AML* controls for ensuring compliance with targeted financial sanctions and for preventing sanctions evasion.

11.10 Reporting obligations to FIU

11.10.1 Article 69 deals with reporting of suspicions. Obliged entities must promptly report to the *FIU* and reply to requests for information by the *FIU* within 5 working days. In justified and urgent cases, the *FIU* may shorten that deadline, including to less than 24 hours.

11.10.2 Article 74 imposes an obligation to perform threshold-based reporting to *FIU*. These relate to *transaction*s involving sale of certain high value goods being cars of at least €250,000 and watercraft /aircraft value at least €7.5 million when the goods are acquired for non-commercial purposes. It should be noted that this is not a *suspicious transaction report* and there may be a requirement to report twice if there are also suspicions.

11.10.3 Under Article 80, in the case of a payment or deposit at a *credit institution* of cash in excess of €10,000 there is an obligation to report this to the *FIU*. (see above).

GLOSSARY

2005 Act Criminal Justice (*Terrorist Offences*) Act 2005(as amended).

2010 Act Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 refers to the Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 as amended by the Criminal Justice Act 2013, the Criminal Justice (Money Laundering and *Terrorist Financing* (Amendment) Act 2018 and the Criminal Justice (Money Laundering and *Terrorist Financing*) (Amendment) Act 2021.

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

2021 Act *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021*.

AMLA means the Anti Money Laundering Authority established pursuant to Regulation 2024/1620.

AMLD 6 means the European Union 6th Anti Money laundering package which entered into force on 9 July 2024.

AML Regulation EU Regulation 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or *terrorist financing*.

AML Directive EU Directive2024 /1640 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or *terrorist financing*.

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.

Beneficial Ownership Regulations These include but are not limited to the regulations relating to beneficial ownership listed in section 1.1.10 and the Investment Limited Partnerships (Amendment) Act 2020 - which includes new sections relating to beneficial ownership registers (including Central Registers).

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*.

Central Registers means the Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies, Central Register of Beneficial Ownership of Trusts and the Central Register of Beneficial Ownership of *Certain Financial Vehicles* as applicable.

Certain Financial Vehicles means ICAVs, Unit Trusts, Credit Unions, Investment Limited Partnerships, Common Contractual Funds and such other financial vehicles as are added by legislation from time to time.

Certified true copy shall be a copy certified from a reputable independent source such as a solicitor, accountant, notary public, or a member of An Garda Síochána

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 who 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 the *politically exposed person* (Section 37(10) of the *2010 Act*).

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).

Companies Act 2014 means the *Companies Act 2014* as amended and updated from time to time.

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 *transaction*s or funds transfers or relationships established for *transaction*s in crypto-assets or transfers of crypto-assets.

Credit Institution means a c*redit institution* as defined in section 24 of the 2010 Act.

Criminal conduct has the meaning ascribed to it in Section 6 of the *2010 Act*.

Customer Due Diligence (CDD) The process by which information regarding the customer 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 by *accountancy firms* or *individuals* as an auditor, *external accountant*, insolvency practitioner or *tax adviser* or as *trust or company service providers* (e.g. company secretarial services).

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

EEA European Economic Area. Countries which form the combined membership of the European Union (EU) and Norway, Iceland and Liechtenstein.

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

'***Electronic Identification Regulation'*** means Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic *transaction*s in the internal market and repealing Directive 1999/93/EC as amended by Regulation (EU) 2024/1183 and as further amended and updated from time to time.

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 Directives Refers in this document to the Fourth Money Laundering Directive (Directive (EU) 2015/849) as amended by the Fifth Money Laundering Directive (Directive (EU) 2018/843).

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 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.

FATF Recommendations means the *FATF Recommendations* adopted by the FATF Plenary in February 2012 updated June 2021 and as further updated from time to time.

Financial institution has the meaning given by Section 24 of the *2010 Act*.

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

Group has the meaning ascribed to it in section 24 of the 2010 Act.

High-risk third country has the meaning given to it in section 24 of the 2010 Act as follows '*High-risk third country*' means a jurisdiction identified by the European Commission in accordance with Article 9 of the Fourth Money Laundering Directive; jurisdictions that are identified by the EU as having strategic deficiencies in their AML/CFT regimes can be found here. Click to access the *FATF* " Black "and "grey" lists of high risk third countries. Usually Both *FATF* and EU lists are the same (but note there can be a time lag between changes). Both must be checked and if there are differences all jurisdictions on both lists should be taken into consideration.

Immediate family member of a politically exposed person' has the meaning ascribed to it in section 37 of the 2010 Act.

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

Internal Register means the internal beneficial ownership register which a company, an industrial and provident society, a trust or *Certain Financial Vehicles* are obliged by law to maintain.

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

Money laundering offences See section 2 of this Guidance.

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 2010 Act.

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 *transaction*s, and the source of wealth or of funds for those *transaction*s, undertaken during the relationship in order to determine if the *transaction*s are consistent with the *designated person's* knowledge of:
    (i) the customer,
    (ii) the customer's business and pattern of *transaction*s, 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.

Non-face-to-face: see narrative in section 4.10 for definition of face-to-face.

Occasional transaction has the meaning ascribed to it in section 24 of the 2010 Act.

PEPs Politically exposed persons. As defined in section 37 of the *2010 Act*.

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 and whether that criminal conduct occurs before, on or after the commencement of this Part of the 2010 Act (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 7.4 of this Guidance).

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

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

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.

Relevant Trust a "relevant trust" is defined in section 106ZC of the 2010 Act and the *Beneficial Ownership Regulations*.

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.

RTS means a Regulatory Technical Standard adopted by *AMLA* from time to time.

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. (Section 59(6) of the 2010 Act.

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*).

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*. 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 *transaction*s 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 See Appendix A.

Trust Regulations 2021 are defined in section 1.1.10 under "Statutory Instruments".

APPENDIX A: *TRUST OR COMPANY SERVICE PROVIDERS*

A.1 Section 24 of The Criminal Justice (Money Laundering and *Terrorist Financing*) Act 2010 defines what a *trust or company service provider* (TCSP) is. TCSPs are designated persons under the 2010 Act. The section describes the services which makes a provider of the services a TCSP.

A.2 A TCSP is any firm (including sole practitioner) whose business is to:

• form companies or other legal persons or entities including where the work is subcontracted to another TCSP;

• provide a registered office, business address, correspondence address, administrative address for a company, partnership, other legal person or arrangement

• act or arrange for another person to act as a:

- director or secretary of a company

- partner (or in a similar position) for other legal persons

- trustee of an express trust or similar legal arrangement

- nominee shareholder for another person, unless the other person is a company listed on a regulated market which is subject to acceptable disclosure requirements.

A.3 Many accountants will provide some of these services for their *clients*. *Accountancy firm*s which provide any of these services must be supervised for AML purposes in respect of the provision of these services. In Ireland TCSPs are regulated by one of the Irish Central Bank, the Dept. of Justice or a designated accountancy body. Five prescribed accountancy bodies in Ireland act as competent authorities for their members under the 2010 Act and are responsible in specified circumstances for supervising members which provide TCSP services.

A.4 As with other "designated persons", TCSP entities providing TCSP services have anti-money laundering obligations. Readers should refer to Ireland's Trust or Company Service Provider Risk Assessment of 2022. The risk assessment emphasises that TCSPs should know the client and know the purpose for which a company it sets up is to be used, including whether there is a business rationale. Readers should refer to Table 8 of the risk assessment, which sets out TCSPs' legal obligations under the 2010 Act. Please also refer to the case studies at the back of the 2022 risk assessment.

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. See section 5.1.17 which sets out the hierarchy of documents.

Reference in this Appendix to a *certified true copy* shall be as defined in the Glossary.

B.1 Individuals

B1.1 General

Where appropriate, evidence of source of wealth and source of funds should be obtained and that can be from searching for public information sources like the internet, company registers and land registers. 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. Also, there should be an understanding of the purpose of the *transaction*, does it make commercial sense.

Client **identification**

B.1.2 The full name, date of birth, and residential address should be obtained. It may also be useful depending on the circumstances to get details of nationality, place of birth, country of residence.

Nationality is suggested because sometimes an address would not disclose if a person had a different nationality. If nationality was flagged as different it might mean more due diligence questions should be asked. **Place of birth/country of residence** is suggested to highlight that members should be mindful that the country of residence and place of birth may differ and to be vigilant that additional customer due diligence procedures may need to be carried out in the event either of those are higher risk jurisdictions.

Client **verification**

NOTE: Two documents required**:** one as proof of identification, one as proof of address. References are made below to documents being current. We would suggest that current should mean be dated within the previous six months.

B.1.3 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 current. Photo identification documents should have a photo that still looks like the client. 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.

Verification	
Proof of Identity	The original, or a *certified true copy*, of one of the following documents or similar should be seen and an acceptably certified copy retained:

Verification	
	• valid passport • valid driving licence (with photo) • national Identity card
Proof of address	The original of a second document should be seen and an acceptably certified copy (*certified true copy* suggested) proof of address document retained. This should be one of the following: • recent evidence of entitlement to a state or local authority-funded benefit (including housing 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 are not acceptable) • PAYE balancing statements • current bank statements or credit/debit card statements issued by a regulated financial sector firm in Ireland or the EU • 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) • current household/motor insurance certificate and renewal notice • official documentation/cards issued by the Department of Social and Family Affairs and addressed to the individual

Note: In higher risk situations such as, for example, if the person doing the verification has not met the proposed client or they are in a high-risk jurisdiction, the firm should consider if any additional procedures are needed for example getting the documents certified and/or an extra layer of approval from *senior management*/risk committee (if applicable).

B.2 Private companies, DACs, Partnerships and Trusts

Client identification and verification

B.2.1 Entity documentation should be collated (i.e. Certificate of Incorporation and constitutional documents, Annual Return, Financial Statements, Partnership/Trust Agreements etc). Also, 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). Information concerning the beneficial ownership should be checked to that entered in the Central Registers
- identify and verify one director/trustee/partner (name, home address, date of birth and nationality, (place of birth, country of residence will assist in obtaining more accurate searches) proof of identity and proof of address) as well as ultimate beneficial owners and the entity
- PEP checks on all directors/partners, trustees and beneficial owners (names, home address and date of birth can be used to aid screening). For completeness, PEP checks also to be completed on Key Management members for all entity types (i.e. CEO, CFO, COO etc) and on the entity itself
- 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*
- for *Relevant Trust*s, an *Accountancy firm* must establish the information concerning the beneficial ownership of the client is entered in the *Relevant Trust*'s *Internal Register* or in the Central Register(s), as appropriate

Unless the entity is listed on a *regulated market*, (as defined in section 24 of the 2010 Act) reasonable steps should be taken to determine and verify its constitution (for example via governing documents) and the full names of all directors (or equivalent) and senior persons responsible for the operations of the company.

Company *Internal register*s of beneficial ownership may be used but not solely relied upon. In exceptional cases, where an *accountancy firm*, having exhausted all other options to identify a beneficial owner and provided there are no grounds for suspicion, it may consider the senior managing official(s) of the client to be its beneficial owner(s).

B.3 Listed or regulated entity

***Client* identification**

B.3.1 The following information should be gathered:

- full name

- membership or registration number
- address
- PEP checks on all directors/partners of listed and regulated entities (names, home address and date of birth can be used to aid screening). For regulated entities only, PEP checks on ultimate beneficial owners

***Client* verification**

Recommended verification

One of the following documents should be seen and a copy retained:

- a printout from the website of the relevant regulator or exchange (which should be annotated in accordance with the procedures outlined in 5.1.22) and which confirms the entity's regulatory or listing status.

If the entity was assessed as higher risk, *senior management* approval of the onboarding might be prudent.

Listed entities (particularly in certain jurisdictions) may be less forthcoming with this information. If listed, they should still be able to provide a list of directors or can confirm those in the entity's annual report are correct. From there a screening tool (if used/available to the firm) can check them for *PEPs*/adverse media and the like. Screening tools would usually provide the address/nationality and date of birth also. You can also ask for the foreign equivalent of Irish company registration office documents which would have directors and company details on them. A Company secretary would usually have this to hand. For Irish/EU listed companies whilst exempt from filing with the RBO, a paid search service can be used to get directors details and confirm these are correct with the client. Ultimately If *clients* are unwilling to inform who the directors are then that should be considered a red flag.

B4. Government or similar bodies

***Client* identification**

B.4.1 The following information should be verified:

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

***Client* verification**

Recommended verification

The following information should be obtained and reviewed, and a copy retained:

- a printout from the website of the relevant body (which should be annotated in accordance with the procedures laid down in 5.1.22).

Additionally for housing associations:

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

B5. Charities

Client identification

Entity documentation should be collated (e.g. Certificate of Incorporation, Annual Return, if they are a company, other constitutional documents if not, Financial Statements, Partnership/Trust Agreements etc.

Also, the following information should be gathered:

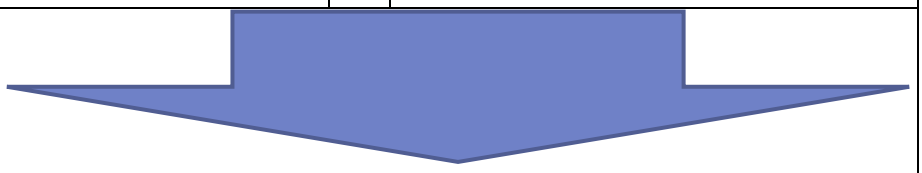
- full name and charity number of the charity
- the trust deed or constitution for the charity
- a list of the members/trustees of the charity
- confirmation that the charity is registered with the Charity Regulator
- see above for checks in respect of incorporated charities and charities formed as trusts
- PEP checks on all directors and trustees (names, home address and date of birth can be used to aid screening).

Consider the risks associated with on boarding a charity as part of the client risk assessment process. Charities are occasionally used to finance terrorism and this needs to be addressed in the risk assessment of the charity client. Reference should be made to risk assessment in section 4 of this guidance.

When onboarding a charity client, the question of why the charity was established is useful. It is also worthwhile obtaining open-source information such as an internet search of the charity, a search of the names of its members, trustees and directors. Please click to access a publication by the Irish Charities Regulator "Guidance on Anti-Money Laundering and Counter-*Terrorist Financing* for Charities". The document is designed as a guide for charities, but firms may find useful the Money Laundering and *Terrorist Financing* indicators at 5.1 and 5.2 which gives details of what are some of the types of *transaction*s that could indicate money laundering *or terrorist financing*.

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 7.4)?



CHECKLIST: Essential elements of an external STR – to be submitted to *FIU Ireland* using goAML and uploaded to the Revenue Commissioners on ROS	
• 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	• 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

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 • Who is otherwise involved in or associated with the matter and in what way?	• 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;

(h) the customer is a third country national who applies for residence rights or citizenship in the State in exchange for capital transfers, purchase of property or government bonds or investment in corporate entities in the State.

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

(a) private banking;

(b) products or *transaction*s that might favour anonymity;

(c) non-face-to-face *business relationship*s or *transaction*s without certain safeguards, such as electronic identification means, *relevant trust* services as defined in the *Electronic identification regulation* or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

(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;

(f) *transaction*s related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare or scientific value, as well as ivory and protected species.

(3) Geographical risk factors:

(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

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

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

(d) 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*).

(3) Geographical Risk Factors-registration, establishment, residence in:

(a) Member States;

(b) third countries having effective anti-money laundering (AML) or combating financing of terrorism (CFT) systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and *terrorist financing* consistent with the revised Financial Action Task Force (*FATF*) recommendations and effectively implement these requirements.

APPENDIX E: DIRECTIONS FROM An GARDA SÍOCHÁNA OR COURT REGARDING PROCEEDING WITH A *TRANSACTION* OR SERVICE

E1 Directions not to proceed

E1.1 Under Section 17(1), a member of An 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 not 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 the 2010 Act.

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 An 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 must be satisfied by information provided on oath by a member of An 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 ex parte and otherwise than in public 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 An 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 An 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 An 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 An 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 20 of 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 of the cessation.

E4 Authorisation from An Garda Síochána to proceed

E4.1 A member of An 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 An 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.