2018 AML GUIDANCE

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

LAW SOCIETY OF IRELAND

INDEX

INDEX

INDEX

SECTION 1 - INTRODUCTION

CONTENTS

A. THE 2018 ACT IS NOT A SEA-CHANGE

2.1.1. This is guidance for solicitors about the Criminal Justice (Money Laundering and Terrorist Financing) Act 2018 (the '2018 Act') which completed all stages in the Oireachtas on 7 November 2018. The Society understands that the Act will be commenced in the shortest possible time following enactment and by the end of November 2018. This guidance supplements the Society's current Guidance Notes for Solicitors on Anti-Money Laundering (AML) Obligations (the '2010 Guidance') as well as the Summary Sheet for the Criminal Justice (Money Laundering and Terrorist Financing) Act 2013. In order to provide the most up-to-date guidance to best meet the needs of members, this Guidance will be a 'living document' which may be updated as needed to draw upon evolving guidance for other designated bodies in Ireland as well as best practice for lawyers in other jurisdictions.

2.1.2. The Fourth Directive requires Member States to further embed the risk-based approach to prevent it from becoming a tick-the-box exercise.

2.1.3. The 2018 Act is not a sea-change for our members – the rudiments of AML compliance for solicitors remain unchanged. Rather, statutory changes are being introduced to ensure that the current regime cannot become a tick-the-box exercise. For example, statutory requirements on solicitors' firms to adopt AML policies and to follow a risk-based approach were well-developed duties in the 2010 Act. However, so as to ensure that AML CDD is more than a mere administrative exercise, the 2018 Act places a renewed emphasis on these obligations. Modified statutory duties will require solicitors' firms to adopt and implement robust AML Policies, Controls and Procedures (PCPs) which include (i) an assessment of money laundering risk in each firm by carrying out a Business Risk Assessment (BRAs) (new section 30A), (ii) the development of policies which introduce controls to mitigate money laundering risk (substituted section 54) which include (iii) Customer Risk Assessments (CRAs) (new section 30B) on every customer/legal service in order to determine the level of CDD to be undertaken.

2.1.4. During the development of the 2018 Act and its passage through the Oireachtas, the Society made a number of recommendations to the Department of Justice and Equality, the Department of Finance and a number of political parties. The Society's AML law reform submissions are available to download from our dedicated AML webpage - www.lawsociety.ie/aml - please use your login to access the AML webpage which is in the members' area. A number of our recommendations concern the creation of FIU powers by the 2018 Act and the manner in which those powers will apply to solicitors. The Society will issue supplemental guidance in relation to the use of these powers should the concerns expressed by the Society in our submissions materialise in the future.

B. CHANGES TO CURRENT GUIDANCE

2.1.5. Sections 2 and 4 are new and provide guidance about the new business and customer risk

assessment obligations. The absolute minimum number of amendments have been made to existing guidance. The entirety of the 2010 Guidance Notes remain extant, except for Chapters 4, 5 and 10, which have been replaced by this Guidance. To understand your AML obligations in the round, you should use the infographs which will navigate you through the two sets of Guidance, depending on your needs at any given time. The infographs are as follows:

- Infograph 1 – Overview of AML Duties
- Infograph 2 – Business Risk Assessment
- Infograph 3 – Customer Risk Assessment to determine CDD and ML Risk

C. CHANGES TO STATUTORY OBLIGATIONS

2.1.6. Our objective has been to make the transition as smooth as possible for solicitors' firms. This Guidance adopts the same user friendly FAQ approach as in the 2010 Guidance Notes. In addition, we outline the key statutory obligations and provide relevant internationally developed best practice guidance for the legal sector tailored to the needs of solicitors in Ireland. Where feasible a step-by-step approach to assist compliance is provided together with adaptable templates. An unofficial revised 2010 Act which reflects the changes introduced by the 2018 Act is also provided, together with a Glossary of Terms.

2.1.7. For your convenience, a summary of the impact of the 2018 Act on solicitors (including any additional necessary updates) is provided and you can access relevant guidance by clicking on the corresponding hyperlink. You can navigate back by using the pdf bookmark function.

D. SUMMARY OF HEADLINE IMPACTS OF THE 2018 ACT ON SOLICITOR AML DUTIES

Description of new/ amended requirement	Section of Primary Act being amended	Section of 2018 Act	Where you will find guidance with hyperlinks?
1. Conduct business risk assessments on AML-regulated legal services	New section 30A	Section 10	Section 2 – Business Risk Assessments
2. Replace Internal AML Policies with new Policies, Controls and Procedures ('PCPs')	Substituted section 54	Section 26	Section 3 – Policies, Controls and Procedures
3. Conduct Customer Risk Assessments on AML-regulated legal services to determine the appropriate type of CDD (Standard, Simplified or Enhanced) to be applied to clients in receipt of AML-regulated legal services	New section 30B	Section 10	Section 4 – Customer Risk Assessments

Description of new/ amended requirement	Section of Primary Act being amended	Section of 2018 Act	Where you will find guidance with hyperlinks?
4. Modified approach to Simplified CDD	Section 34 repealed and new section 34A	Section 13	Section 5 – Updated Guidance on CDD
5. Modified approach to Standard CDD: i. Duty to verify identity of persons acting on behalf of customers ii. Requirement to carry out CDD at any time where the risk of money laundering or terrorist financing requires, in addition to the times already required iii. Amended approach to CDD on beneficial owners and trusts iv. Amended ongoing monitoring obligations	Sections 33 and 35	Sections 11 and 14	Section 5 – Updated Guidance on CDD
6. Modified approach to Enhanced CDD: i. In accordance with a firm's AML Policies, Controls and Procedures, to examine the background and purpose of complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose	Sections 36 repealed, new section 36A	Section 15	Section 5 – Updated Guidance on CDD
ii. to take steps, which are reasonably warranted by the risk of a client being involved in money laundering or terrorist financing, to determine if that client is a domestic PEP and new measures to be applied to all PEPs	Section 37 amended	Section 16	Section 5 – Updated Guidance on CDD

Description of new/ amended requirement	Section of Primary Act being amended	Section of 2018 Act	Where you will find guidance with hyperlinks?
iii. to apply additional measures including enhanced monitoring to manage and mitigate the risk of money laundering and terrorist financing where a customer is established or resides in a high-risk third country	New Section 38A	Section 18	Section 5 – Updated Guidance on CDD
iv. to apply enhanced measures, additional to existing measures, to manage and mitigate the risk of money laundering or terrorist financing to business relationships which present a higher degree of risk including those listed in Schedule 4 and any others prescribed by the Minister	Substituted Section 39	Section 19	Section 5 – Updated Guidance on CDD

E. GLOSSARY

Term	Explanation
ML/TF	Money Laundering/Terrorist Financing *The substantive offences of money laundering and terrorist financing. Anti-Money Laundering obligations are designed to prevent money laundering and terrorist financing.*
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism *Statutory processes which must be applied by banks and other sectors, including solicitors, to prevent the use of certain services they provide being vulnerable to money laundering and terrorist financing.*
Customer	The 2010 Act as amended uses the term 'customer'. For solicitors this means clients to whom they provide AML- regulated legal services.

Term	Explanation
AML-Regulated Legal Services	AML obligations only arise where a solicitor participates in certain types of legal work. This work is specified in the definition of the term "relevant independent legal professional" contained in section 24(1) as a solicitor who carries out any of the following services: "(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following: (i) buying or selling land or business entities; (ii) managing the money, securities or other assets of clients; (iii) opening or managing bank, savings or securities accounts; (iv) organising contributions necessary for the creation, operation or management of companies; (v) creating, operating or managing trusts, companies or similar structures or arrangements; (b) acting for or on behalf of clients in financial transactions or transactions relating to land;" Accordingly, legal activities falling outside these categories are exempt from AML CDD. Irrespective of whether an AML-regulated legal service is being provided, a solicitor must always remain alert to the risk of unwittingly committing the substantive offence of money laundering or terrorist financing. See further Chapters 2 and 9 of the 2010 Guidance Notes.
2010 Act	The Criminal Justice (Money Laundering and Terrorist Offences) Act 2010 *The primary Act for all AML CDD together with substantive offence of money laundering which implemented the Third Directive.*
2013 Act	The Criminal Justice (Money Laundering and Terrorist Offences) (Amendment) Act 2013 *An amending Act which introduced minor changes, for example, to simplified due diligence which reflected best practice principles.*
2018 Act	The Criminal Justice (Money Laundering and Terrorist Offences) (Amendment) Act 2018 *An amending Act which embeds the risk-based approach so as to prevent a tick-the-box approach to AML CDD.*
2MLD	Second Money Laundering Directive *This Directive incorporated the amendments to the FATF recommendations. It extended anti-money laundering obligations to a defined set of activities provided by a number of service professionals, including solicitors. Legislation transposing 2MLD was repealed and replaced when 3MLD was being transposed.*

Term	Explanation
3MLD	Third Money Laundering Directive *This Directive extended due diligence measures to beneficial owners, recognised that such measures can be applied on a risk-based approach, and required enhanced due diligence to be undertaken in certain circumstances. It was transposed into Irish law by the 2010 Act.*
4MLD	Fourth Money Laundering Directive - most of this Directive will be transposed by the 2018 Act *This Directive responded to changes made to the requirements issued by FATF in February 2012 and to a review conducted by the European Commission on the implementation of the Third Money Laundering Directive.* *There were a number of new developments contained in the 4th Directive. The key ones include the following:* • *requirements to have a written risk assessment* • *amendments to the way in which simplified due diligence may be applied* • *changes to the beneficial ownership provisions* • *extension of enhanced due diligence to domestic PEPs* • *requirements for Member States to maintain registers recording the beneficial owners of companies and trusts which generate tax consequences*
BRA	Business Risk Assessment
CRA	Customer Risk Assessment
PCPs	Policies, Controls and Procedures
2010 Guidance Notes	Guidance Notes for Solicitors on AML Obligations published by the Law Society in July 2010

F. HOW TO TRANSITION TO FULL COMPLIANCE WITH THE 2018 ACT

2.1.8. During the development of the 2018 Act and its passage through the Oireachtas, the Society made strong recommendations to the Department of Justice and Equality, the Department of Finance and a number of political parties that solicitors and other designated persons be provided with adequate time between enactment and commencement of the Act. The Society's AML law reform submissions are available to download from our dedicated AML webpage - http://www.lawsociety.ie/aml/ - please use your login to access the AML webpage which is in the members' area. Preparation time ensures that businesses and competent authorities alike have an opportunity to have visibility of final wording of their statutory obligations, review and update relevant guidance and update their AML policies so as to ensure compliance with new statutory obligations on the day that those statutory obligations commence. However, the Society understands that the Act will be commenced in the shortest possible time following enactment and by the end of November 2018.

2.1.9. It is important to note that, until the commencement of the 2018 Act, the new requirements have no statutory effect.

2.1.10. The Law Society's Investigating Accountants will take a common sense approach when monitoring compliance with the 2018 Act following its initial commencement. All firms/solicitors must familiarise themselves fully with the new obligations, conduct a Business Risk Assessment, implement new PCPs and commence the process of completing a Customer Risk Assessment for all clients to whom they provide AML-regulated legal services to determine the type and extent of CDD to be applied to that client.

2.1.11. The 2018 Act will not automatically require solicitors to refresh their customer due diligence for all existing clients for whom AML-regulated legal services are currently in train and CDD has already been completed. This is because sections 33 and 35 of the 2010 Act require that CDD take place prior to the establishment of a business relationship with the client. Accordingly, on a date which precedes the commencement of the 2018 Act, solicitors will have already completed the CDD exercise for existing clients. Therefore, when the 2018 Act is commenced, it is likely that any instructions in train will already have been in compliance with the 2010 Act for CDD purposes.

2.1.12. By way of clarification, solicitors should note that the CDD requirements of sections 33 and 35 must be completed prior to taking on a client. Some limited flexibility is available only in relation to the timing of verification of identity. Please see 'When must identification and verification be undertaken?' in Section 5 for further guidance. Section 33(5) permits verification to be delayed to "as soon as practicable" after initial contact where there is no ML/TF risk and to do otherwise would interrupt the normal conduct of business. For the avoidance of doubt, section 33(5) does not envisage verification or any other CDD requirements being completed during the course of providing an AML-regulated legal service. Irrespective of the limited flexibility with regard to verification of identity taking place as soon as practicable after initial contact, the Society recommends that solicitors complete their customer risk assessment and apply all necessary CDD prior to deciding to provide an AML-regulated legal service. This approach is in a firm's best interest from a risk management perspective and allows firms the flexibility to decide to not provide an AML-regulated legal service where the ML/TF risk is too high and/or the extent of CDD required would be onerous/outside of the expertise of some firms.

2.1.13. After the commencement of the 2018 Act, best practice will require that all new instructions for AML-regulated legal services comply in full with the 2018 Act irrespective of whether the client is an existing one or a client to whom a legal service has been provided in the past. This includes the application of a Customer Risk Assessment to all new instructions for an AML-regulated legal service received after the commencement of the 2018 Act from new and existing clients.

2.1.14. It is important for solicitors to be aware that, irrespective of whether a client or AML-legal service falls before or after the commencement of the 2018 Act, all AML-regulated legal services are subject to ongoing monitoring in section 35 on a risk sensitive basis. This is in accordance with the 2010 Act.

2.1.15. Therefore, as a general rule of thumb, for current clients for whom the solicitor is in the course of providing an AML-regulated legal service, if CDD was completed prior to the commencement of the 2018 Act and there are no ML/TF red flags, a solicitor can proceed to provide the current legal service on a risk sensitive basis without any additional CDD being required. In all other circumstances, (new and existing/historical clients for whom there is no live/current legal service/ instruction being provided), solicitors should ensure that the CDD applied is in full compliance with the 2018 Act.

2.1.16. Solicitors may wish to categorise clients/files as follows:

At the time of commencement of the 2018 Act, an AML-legal service is already in train and statutory CDD requirements under the 2010 Act recently completed → follow ongoing monitoring guidance, be alert to ML/TF red flags, complete legal service in a timely manner and likely within 6 months of commencement of 2018 Act – [NB new section 33(1)(e) will apply and it requires CDD at any time where risk of ML/TF requires in addition to at times already required]

After the commencement of the 2018 Act, all new instructions for AML-regulated legal services from existing clients → comply fully with 2018 Act for Customer Risk Assessments and CDD - Customer Risk Assessment, CDD etc...

After a solicitors' firm has on-boarded a client in compliance with their 2018 AML obligations and subsequent new instructions for an AML-regulated legal service are received → Onoing monitoring applies. In addition, the Society recommends that solicitors complete a new CRA for each new instruction. [NB new section 33(1)(e) which requires CDD at any time where risk of ML/TF requires in addition to at times already required]. It is good practice to refresh the CDD if there has been a gap of over three years between instructions or you become aware of any changes to your due diligence on your client, for example, a change of name, address or business. You are not required to undertake a renewal of CDD on a client on-boarded after the 2018 Act if there has been no change in the risk profile of the client, the type of work you are undertaking or their personal details.

G. SCOPE AND STATUS OF GUIDANCE

2.1.17. In some instances, this Guidance has adapted guidance issued by the Legal Sector Affinity Group which comprises the AML Supervisors for the legal sector in Britain and which has also been approved by HM Treasury. Sample PCPs, CRAs and BRAs published by the Law Society of Scotland have also been adapted to reflect the Irish legislative framework. Infographs have been developed by the Law Society of Ireland and are copyrighted.

2.1.18. While care has been taken to ensure that guidance, sample forms and infographs are accurate, up to date and useful, the Law Society will not accept any legal liability in relation to them.

2.1.19. Law Society AML Guidance is designed to guide solicitor firms and employees of solicitors' firms on the application of the relevant provisions of the Act. The guidelines do not constitute legal advice or secondary legislation and solicitors must always refer directly to the Act as amended when ascertaining their statutory obligations. The guidelines are subordinate to the Act.

2.1.20. The guidelines are not intended to be exhaustive nor to set the limits for the steps to be taken by designated persons in working to prevent money laundering or terrorist financing. The Act involves a combination of risk-based and rules-based approaches to the prevention of money laundering and terrorist financing; the general approach of designated persons should be to take the steps warranted by the risk of money laundering in any given circumstance.

2.1.21. In addition to providing guidance on the requirements of the Act, and how solicitors covered by its provisions can best meet their obligations, the guidelines also;

- Indicate good standards of industry practice in AML/CFT procedures through a proportionate, risk-based approach; and
- Assist solicitors firms to design and implement the systems and controls necessary to mitigate the risk of solicitors being used in connection with money laundering and the financing of terrorism.

SECTION 2 - BUSINESS RISK ASSESSMENTS

A new Section 30A inserted by section 10 of the 2018 Act

CONTENTS

A. BACKGROUND

Are Business Risk Assessments a new concept?

2.2.1. No. The 2010 Act introduced many concepts to implement the risk-based approach envisioned by the Third Directive. The exercise will have been something which solicitors' firms will have engaged in previously when developing their AML policies: section 30A simply places this exercise on a more formal statutory footing.

What is the reason for the change?

2.2.2. The Fourth Directive requires Member States to further embed the risk-based approach to prevent it from becoming a tick-the-box exercise.

B. THE STATUTORY REQUIREMENT TO CONDUCT BUSINESS RISK ASSESSMENTS

2.2.3. A new stand-alone statutory requirement to carry out business risk assessments will be introduced by a new Section 30A. This requirement will be independent from the requirement to have

AML policies. This will embed the risk-based approach by placing a renewed emphasis on the importance of solicitors' firms conducting a business risk assessment of their firm's exposure to ML/TF risks.

2.2.4. In addition, section 54(3)(a) will maintain the requirement from the 2010 Act that a firm's AML policies include the identification and assessment of money laundering and terrorist financing (ML/TF) risk factors.

What does section 30A require?

2.2.5. Solicitors should read carefully the new section 30A in full which provides:

30A.— (1) A designated person shall carry out an assessment (in this Act referred to as a "business risk assessment") to identify and assess the risks of money laundering and terrorist financing involved in carrying on the designated person's business activities taking into account at least the following risk factors:

(a) the type of customer that the designated person has;
(b) the products and services that the designated person provides;
(c) the countries or geographical areas in which the designated person operates;
(d) the type of transactions that the designated person carries out;
(e) the delivery channels that the designated person uses;
(f) other prescribed additional risk factors.

(2) A designated person carrying out a business risk assessment shall have regard to the following:

(a) any information in the national risk assessment which is of relevance to all designated persons or a particular class of designated persons of which the designated person is a member;
(b) any guidance on risk issued by the competent authority for the designated person;
(c) where the designated person is a credit institution or financial institution, any guidelines addressed to credit institutions and financial institutions issued by the European Banking Authority, the European Securities and Markets Authority or the European Insurance and Occupational Pensions Authority in accordance with the Fourth Money Laundering Directive.

(3) A business risk assessment shall be documented unless a competent authority for a designated person decides under Article 8 of the Fourth Money Laundering Directive that an individual documented risk assessment is not required and notifies the designated person …

(4) A designated person who fails to comply with this section commits an offence and is liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or
(b) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).

C. CURRENT GUIDANCE ABOUT ASSESSING ML/TF RISK

What is the Law Society's current best practice guidance for assessing the ML/TF risk exposure of a solicitors' firm?

2.2.6. The Society's existing guidance for solicitors' firm ML/TF risk assessment, at paragraphs 4.13 to 4.15 of the 2010 Guidance Notes, remains relevant:

"How to assess your firm's risk profile?

This depends on your firm's size, type of clients, and the practice areas engaged in. You should consider the following factors:

(1) Client demographic

A firm's client demographic can affect the risk of money laundering or terrorist financing. Factors which may vary the risk level include whether a firm:

- has a high turnover of clients or a stable existing client base
- acts for 'politically exposed persons' (PEPs)
- acts for clients without meeting them
- practices in locations with high levels of acquisitive crime or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property
- acts for clients affiliated to countries with high levels of corruption or where terrorist organisations operate
- acts for entities that have a complex ownership structure
- can easily obtain details of beneficial owners of their client or not

(2) Services and areas of law

Some services and areas of law could provide opportunities to facilitate money laundering or terrorist financing. For example:

- complicated financial or property transactions
- providing assistance in setting up trusts or company structures, which could be used to obscure ownership of property
- payments that are made to or received from third parties
- payments made by cash
- transactions with a cross-border element
- Simply because a client or a retainer falls within a risk category does not mean that money laundering or terrorist financing is occurring.

Chapter 9 provides more information on warning signs to be alert to when assessing risk."

D. THE SOCIETY'S EXPECTATIONS IN RELATION TO BUSINESS RISK ASSESSMENTS WHEN THEY MONITOR/SUPERVISE A FIRM'S AML COMPLIANCE

2.2.7. Section 30A(3) requires solicitors' firms to document their Business Risk Assessment:

"A business risk assessment shall be documented unless a competent authority for a designated person decides under Article 8 of the Fourth Money Laundering Directive that an individual documented risk assessment is not required and notifies the designated person."

2.2.8. For the avoidance of doubt, the Law Society as the competent authority for solicitors requires that all solicitors' firms document their Business Risk Assessment for all AML-regulated legal services.

2.2.9. In addition, section 30A(6) requires all solicitors' firms to make records of Business Risk Assessments available on request to the Law Society: "A designated person shall make records of a business risk assessment available, on request, to the competent authority for that designated person." Solicitors should therefore ensure Business Risk Assessments and related documents are available for any Law Society authorised person should they request same.

E. STEP-BY-STEP GUIDANCE ABOUT HOW TO CONDUCT A BUSINESS RISK ASSESSMENT?

2.2.10. The Society has developed the following best practice step-by-step approach for solicitors to help them ensure their compliance with the new statutory requirement to conduct a Business Risk Assessment.

STEP 1 - DEVELOP YOUR KNOWLEDGE OF ML/TF RISKS INHERENT IN LEGAL SERVICES

2.2.11. Regard should be had to the following credible sources about ML/TF risks/red flags in the legal sector:

i. The known legal services vulnerable to money laundering which are also the legal services for which solicitors are designated for AML compliance – 'the AML-Regulated Legal Services'. This work is specified in the definition of the term "relevant independent legal professional" contained in section 24(1) as follows:

"(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:

(i) buying or selling land or business entities;
(ii) managing the money, securities or other assets of clients;
(iii) opening or managing bank, savings or securities accounts;
(iv) organising contributions necessary for the creation, operation or management of companies;
(v) creating, operating or managing trusts, companies or similar structures or arrangements;

(b) acting for or on behalf of clients in financial transactions or transactions relating to land;"

2.2.12. Legal activities falling outside these categories are not subject to statutory AML, because they pose little or no ML/TF risk.

ii. Section 30A(2) requires that, when carrying out a BRA, regard be had to the most recent **National Risk Assessment** and guidance on risk issued by a competent authority.

The ML/TF vulnerabilities for the sector are set out in pages 60 to 62 of Ireland's National Risk Assessment as follows:

- *"The specialist nature of the knowledge and services provided by the legal services sector makes solicitors and barristers vulnerable to being sought out and exploited by criminals who seek to launder the proceeds of crime or evade tax. This is because the involvement of legal professionals is necessary to complete certain transactions which are attractive to criminals.*

- *Vulnerable services can include:*
  - *Complicated financial and property transactions;*
  - *Company and trust formations; [See further MOU with the Department of Justice and Equality on TCSPs]*
  - *Securities and funds transactions;*
  - *Complicated cross-border transactions; and*
  - *Establishing charities - [See further MOU with the Department of Justice and Equality on TCSPs]*

- *Due to the nature and potential scale of transactions associated with the vulnerable services offered, there is an increased risk that substantial proceeds could be laundered. This increases the risk of money laundering associated with these services.*

- *Solicitors who regularly provide such vulnerable services may be at a higher risk of unknowingly facilitating money laundering through lack of identification of the true source of funds and the ultimate beneficial owner of funds. Involvement of the legal profession can be perceived as adding legitimacy to transactions.*

- *Where solicitors obtain client money, they are obliged to segregate such funds from their own business funds by operating a separate client account. While client accounts are an important and highly regulated feature of solicitors' practices, if improperly managed, i.e. where inadequate or inconsistent CDD procedures are applied by a practice to its client account, there could be significantly heightened risk. Cases have occurred where solicitors' client accounts have been misused.*

- *The overall ML/TF risk in the legal services sector is judged to be Medium-High..."*

iii. The Internationally Recognised Money Laundering Typologies in Legal Sector

The FATF 2013 Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals

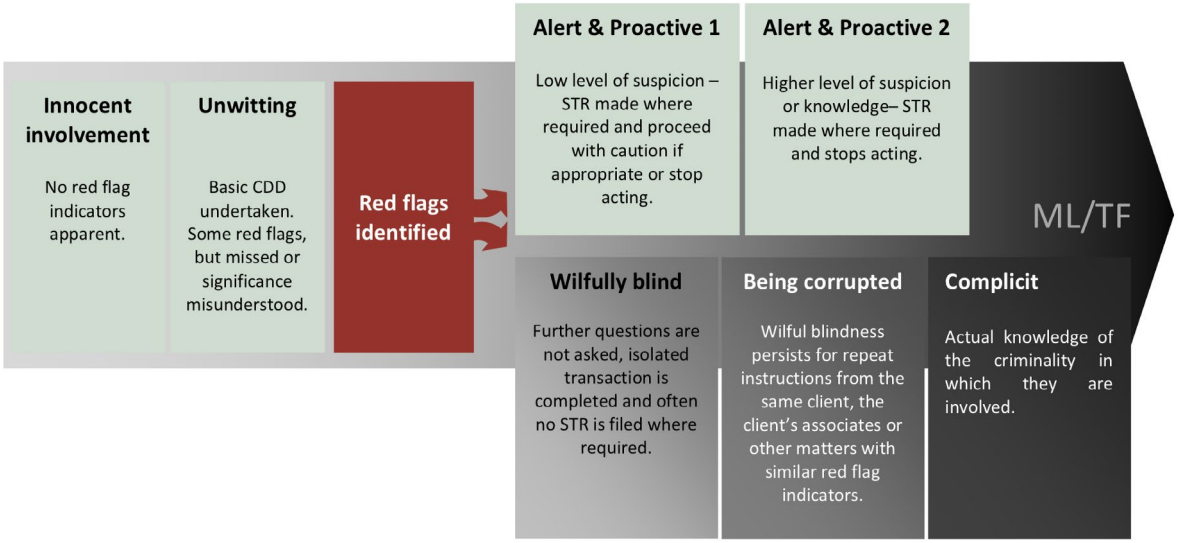
The report identifies a number of ML/TF methods that commonly employ or, in some countries, require the services of a legal professional. Inherently these activities pose ML/TF risk and when clients seek to misuse the legal professional's services in these areas, even law abiding legal professionals may be vulnerable. The methods are:

- *misuse of client accounts;*
- *purchase of real property;*
- *creation of trusts and companies;*
- *management of trusts and companies;*
- *managing client affairs and making introductions;*
- *undertaking certain litigation; and*
- *setting up and managing charities.*

See Chapter 4: ML Typologies

iv. The Internationally Recognised ML/TF Red Flag Indicators in the Legal Sector

From reviewing the case studies and literature as a whole, the involvement of legal professionals in the money laundering of their clients is not as stark as complicit or unwitting, but can best be described as a continuum.



See Chapter 5: Red flags about the client, source of funds, choice of lawyer and the nature of the retainer.

v. **Comparative research published by the Solicitors Regulation Authority** about ML/TF vulnerabilities observed by the SRA in England and Wales.

vi. **Comparative Guidance for the legal sector in England and Wales, published by the Legal Sector Affinity Group and approved by HM Treasury,** provides comprehensive key insights for solicitors about legal sector specific risk factors.

2.3.1 Customer risk factors

When assessing risk factors relating to your customers you should consider the demographic of your client base. Factors which may affect the level of risk associated with your client base are set out below.

2.3.1.1 High client turnover v stable client base

Although not determinative, you should take into account the length and strength of your typical client relationships.

If you have long-term and strong relationships with your clients you will be in a better position to identify any potential money laundering issues, which may mean your practice is at a lower risk of being subject to money laundering or terrorist financing (although you should always be mindful of clients that put pressure on you citing their long-standing relationship). Conversely, if you tend to have shorter relationships and a higher client turnover, you may conclude that the lack of a long and strong client relationship means your practice faces greater risk.

2.3.1.2 Clients based in high-risk jurisdictions

Country risk factors should feature prominently in your assessment of the money laundering and terrorist financing risks your practice faces. Key issues to consider are whether the jurisdictions in which your clients, or the beneficial owners of your clients, are based or operate their businesses:

- *have deficient anti-money laundering legislation, systems and practice*
- *have high levels of acquisitive crime or higher levels of corruption*
- *are considered to be 'offshore financial centres' or tax havens*
- *permit nominee shareholders to appear on the share certificate or register of owners.*

Conversely, where your clients or the beneficial owners of your clients are based or operate their business in low risk jurisdictions this should be reflected in your risk assessment...

2.3.1.3 Clients in higher risk sectors

Given the wider international focus and extra territorial issues surrounding anti-bribery and corruption laws in some jurisdictions, you should take into consideration the elevated risks attached to certain sectors when carrying out your practice-wide risk assessment.

Certain sectors have been identified by credible sources as giving rise to an increased risk of corruption and, in some countries, are subject to international or UK, UN or EU sanctions.

Sectors that may be higher risk, particularly when coupled with a high-risk jurisdiction include (but are not limited to):

- *public work contracts and construction, including post-conflict reconstruction*
- *real estate and property development*

- *the oil and gas industry*
- *the nuclear industry*
- *mining (including diamond mining and trading)*
- *arms manufacturing/supply and the defence industry*

Clearly not all work in these sectors will be higher risk but it is essential to be aware of the potential for risk so that you can implement proportionate procedures for closer scrutiny on client and matter acceptance.

2.3.1.4 Acting for politically exposed persons (PEPs)

An independent legal professional's exposure to PEPs is also a major consideration in carrying out your practice-wide risk assessment. A PEP may be a client or a beneficial owner of a client but it is important to consider the type of PEPs that you act for and whether the work to be undertaken will affect your overall risk profile…

2.3.1.5 Acting for clients without meeting them

In an increasingly global and technologically advanced environment, it is commonly the case that you will act for clients without meeting them. You should include this as a factor when you carry out your practice-wide risk assessment. In addition, you should consider the systems and procedures that you have implemented to mitigate the risks associated with acting for clients you do not meet.
When you act for clients without meeting them you must be satisfied that it makes sense in all the circumstances that you have not met the client and you must be comfortable that you can mitigate the risks of identity fraud.

2.3.1.6 Clients with high cash turnover businesses

You should consider whether your practice frequently acts for clients who operate or benefit from high cash turnover businesses as these businesses may be appealing to criminals seeking to launder money.

2.3.2 Services and areas of law and geographical location of services provided

In carrying out your practice-wide risk assessment you must consider risks associated with the services you provide, the transactions you participate in and the countries or geographic areas in which you operate.

2.3.2.1 Services and areas of law

Many studies have highlighted that independent legal professionals face the greatest potential risks in the following areas:
- *misuse/abuse of client accounts*
- *sale/purchase of real property*
- *creation of trusts, companies and charities*
- *management of trusts and companies*
- *sham litigation*

The involvement of your practice in the sale/purchase of real property, creation of trusts, companies and charities, and management of trusts and companies does not automatically lead to the conclusion that your business is high risk. However, you should consider these areas and

consider other risk factors, such as jurisdictional or sector risk, in the context of your business so that you can put in place additional controls where necessary to minimise the risk of money laundering.

Other areas of risk focus more closely on factors which may be more prevalent when considering a particular client or mandate, including unusually complicated transactions. You should consider how you might ensure that your staff can identify the warning signs as part of your risk assessment.

Criminals are constantly developing new techniques, so no list of examples can ever be exhaustive. This section does, however, provide some further guidance on areas of money laundering risk.

2.3.2.2 Client accounts and payments

In carrying out your practice-wide risk assessment you should take into account the risk that criminals may attempt to misuse/abuse your client account. You must ensure that you only use client accounts to hold client money for legitimate transactions where this is incidental to the legal services you supply. Putting the proceeds of crime through your client account can give them the appearance of legitimacy, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into the banking system can be part of the placement stage of money laundering. Therefore, the use of cash may be a warning sign.
Legal professionals should not provide a banking service for their clients.

2.3.2.3 Sale/purchase of real property

Law enforcement authorities believe that the purchase of real estate is a common method for disposing of or converting criminal proceeds.

Real estate is generally an appreciating asset and the subsequent sale of the asset can provide an apparently legitimate reason for the existence of the funds.

2.3.2.4 Creation and management of trusts, companies and charities

Company and trust structures may be exploited by criminals who wish to retain control over criminally derived assets while creating impediments to law enforcement agencies in tracing the origin and ownership of assets. Criminals may ask legal professionals to create companies and trusts and/or to manage companies and trusts, to provide greater respectability and legitimacy to the entities and their activities.

Shell companies are corporate entities that do not have any business activities or recognisable assets. They may be used for legitimate purposes such as serving as transaction vehicles. However, they can also be an easy and inexpensive way to disguise beneficial ownership and the flow of illegitimate funds and so are attractive to criminals engaged in money laundering. You should be suspicious if a client engages your services only in connection with the routine aspects of forming an entity, without seeking legal advice on the appropriateness of the corporate structure and related matters. In jurisdictions where members of the public may register companies themselves with the company register the engagement of a legal professional to register the company may indicate that the client is seeking to add legitimacy to a shell company. [See further the Law Society's MOU with the Department of Justice and Equality on TCSPs]

2.3.2.5 Sham litigation

Litigation may constitute sham litigation if the subject of the dispute is fabricated (there is no actual claim and the litigation is merely a pretext for transferring the proceeds of crime from one entity to another, possibly through a client account) or if the subject of the litigation is a contract relating to criminal activity that a court would not enforce.

2.3.2.6 Geographical location of services

You should carefully consider the jurisdictions in which you are offering your services and whether there are any particular local issues of which you ought to be aware which may impact on your risk assessment. Information on jurisdictional issues is set out above in section 2.3.1.2."

STEP 2 - DRAFT YOUR FIRM'S BUSINESS RISK ASSESSMENT

2.2.13. Using your knowledge of the ML/TF risks to solicitors' firms gained in Step 1, document your understanding of the types of legal services your firm provides and the ML/TF risks posed i.e. the nature, scale and complexity of ML/TF risks for your firm with regard to "at least" the following risk factors as required by section 30A(1):

(1) Customer type
(2) Products and services provided by the solicitors' firm
(3) Countries/geographical areas
(4) Transaction type
(5) Delivery channel type
(6) Other prescribed additional risk factors

2.2.14. Key questions to ask under the statutory risk factors include:

(1) Customer type

Begin by assessing your client base and the level of money laundering risk associated with it. Consider the following questions.

- How often do you undertake regulated work?
- Do you tend to have a stable client base or high client turnover?
- Do you have clients based in high risk jurisdictions? See the country and geographic risk factors set out below.
- Do you know your clients personally?

Ensure that your policies, controls and procedures, especially in relation to customer due diligence and ongoing monitoring, address and mitigate the client risk factors relevant to your firm.

(2) Products and services provided by the solicitors' firm

Consider whether any services you provide are attractive to money launderers such as:

- misuse or abuse of client accounts
- the sale or purchase of real property
- creation of trusts, companies and charities
- management of trusts and companies
- sham litigation.

(3) Countries/geographical areas

Country risk factors should feature in your assessment of the money laundering and terrorist financing risks your practice faces. Consider whether the jurisdictions in which your clients

or the beneficial owners of your clients are based or operate their businesses:

- have deficient anti-money laundering legislation, systems and practice
- have high levels of acquisitive crime or higher levels of corruption
- are situated in 'offshore financial centres' or tax havens
- are subject to sanctions.

(4) Transaction type

Consider how frequently you carry out higher risk transactions. Factors that might make a transaction higher risk include:

- the size and value of the transaction
- the payment type (for example cash or fund transfers from outside the EU into your client account)
- transactions or products that are complex, facilitate anonymity or don't fit a usual pattern.

(5) Delivery channel type

The way services are delivered can enhance or reduce your risk.

- Do you provide services to clients you have not met face-to-face?
- Do you enter into business relationships with clients that are conducted through intermediaries?

STEP 3 - CONSIDER ADAPTING THE SOCIETY'S BUSINESS RISK ASSESSMENT TEMPLATE

2.2.15. The Society has developed a sample Business Risk Assessment to assist solicitors. It is available to download from our dedicated AML webpage - www.lawsociety.ie/aml - please use your login to access the AML webpage which is in the members' area.

STEP 4 - OBTAIN SENIOR MANAGEMENT APPROVAL OF THE FIRM'S BUSINESS RISK ASSESSMENT

2.2.16. Section 30A(5) requires that senior management approve the Business Risk Assessment: *"A business risk assessment shall be approved by senior management."*

2.2.17. Accordingly, once Steps 1 to 3 are complete, the Society recommends that the firm's partners review and approve the Business Risk Assessment.

STEP 5 - KEEP BUSINESS RISK ASSESSMENTS UNDER REVIEW IN LINE WITH POLICIES, CONTROLS AND PROCEDURES

2.2.18. Section 30A(4) specifically requires that Business Risk Assessments be kept up-to-date:

"A designated person shall keep the business risk assessment, and any related documents, up to date in accordance with its internal policies, controls and procedures adopted in accordance with section 54."

2.2.19. For example, a Business Risk Assessment would need to be reviewed should there be any changes to a firm's business model such as the provision of new legal services or changes in delivery channels or should new ML/TF risks for the legal sector emerge.

SECTION 3 - POLICIES, CONTROLS AND PROCEDURES

Consolidates and replaces Chapter 4 (Risk-Based Approach) and Chapter 10 (Internal Policies)
Section 54 substituted by section 26 of the 2018 Act

CONTENTS

A. BACKGROUND

Are Policies, Controls and Procedures a new concept?

2.3.1. No, Policies, Controls and Procedures (PCPs) are not a new concept. Most of the current statutory obligations in relation to solicitors' firm AML policies are being carried over in the substituted section 54. While new statutory obligations are being introduced, these will primarily bring the legislation into line with current Law Society best practice.

2.3.2. Firms will identify firm-wide risk through their Business Risk Assessment while fee earners will identify the risk posed by each AML-regulated legal service in their Customer Risk Assessment which is discussed in the next Section.

2.3.3. The word "controls" is introduced into the concept of AML policies and this simply reflects the need for PCPs to be designed to manage the ML/TF risks specific to each firm or AML-regulated legal service.

B. THE STATUTORY REQUIREMENT

What's new?

2.3.4. New aspects which will be introduced into PCPs on a statutory basis, to reflect requirements of the Fourth Directive, include requirements that PCPs:
- Address record keeping (section 54(3)(h)),
- Include CDD (section 54(3)(b)),

- deal with PCPs around monitoring transactions and business relationships (section 54(3)(c)),
- include PCPs which keep Business Risk Assessment documents and information up-to-date (section 54(3)(j)),
- include PCPs to identify emerging risks and keep Business Risk Assessments up-to-date (section 54(3)(k)),
- have regard to guidelines issued by the Law Society (section 54(5))
- if directed in writing by the Law Society, appoint a compliance officer who is "an individual at management level" to monitor and manage a firm's compliance with PCPs (section 54(7))
- if directed in writing by the Law Society, appoint a senior manager to implement and manage PCPs (section 54(8))
- if directed in writing by the Law Society, undertake an independent, external audit to test effectiveness of PCPs (section 54(9))

What does the new section 54 require?

2.3.5. Solicitors should read carefully the new section 54 in full, which provides:

(1) A designated person shall adopt internal policies, controls and procedures in relation to the designated person's business to prevent and detect the commission of money laundering and terrorist financing.

(2) In particular, a designated person shall adopt internal policies, controls and procedures to be followed by any persons involved in carrying out the obligations of the designated person under this Part.

(3) The internal policies, controls and procedures referred to in subsection (1) shall include policies, controls and procedures dealing with—

(a) the identification, assessment, mitigation and management of risk factors relating to money laundering or terrorist financing,

(b) customer due diligence measures,

(c) monitoring transactions and business relationships,

(d) the identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature to be related to money laundering or terrorist financing,

(e) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,

(f) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments including the use of new products and new practices and the manner in which services relating to such developments are delivered,

(g) reporting (including the reporting of suspicious transactions),

(h) record keeping,

(i) measures to be taken to keep documents and information relating to the customers of that designated person up to date,

(j) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,

(k) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and

(l) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures.

(4) A designated person shall ensure that policies, controls and procedures adopted in accordance with this section are approved by senior management and shall keep such policies, controls and procedures under review, in particular when there are changes to the business profile or risk profile of the designated person.

(5) In preparing internal policies, controls and procedures under this section, the designated person shall have regard to any guidelines on preparing, implementing and reviewing such policies and procedures that are issued by the competent authority for that designated person.

(6) A designated person shall ensure that persons involved in the conduct of the designated person's business are—
(a) instructed on the law relating to money laundering and terrorist financing, and
(b) provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified...

(10) A reference in this section to persons involved in carrying out the obligations of the designated person under this Part includes a reference to directors and other officers, and employees, of the designated person.

(11) The obligations imposed on a designated person under this section do not apply to a designated person who is an employee of another designated person...

(15) A designated person who fails to comply with this section commits an offence and is liable—
(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or
(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

C. INFORMATION ABOUT HOW TO PREPARE PCPS

What should PCPs include/cover?

2.3.6. The specific statutory requirements about what a firm's PCPs should cover are listed in section 54(3). PCPs *"shall include policies, controls and procedures dealing with—*
(a) the identification, assessment, mitigation and management of risk factors relating to money laundering or terrorist financing,
(b) customer due diligence measures,
(c) monitoring transactions and business relationships,
(d) the identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing,
(e) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,
(f) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments including the use of new products and new practices and the manner in which services relating to such developments are delivered,
(g) reporting (including the reporting of suspicious transactions),
(h) record keeping,
(i) measures to be taken to keep documents and information relating to the customers of that

designated person up to date,

(j) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,

(k) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and

(l) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures."

Who is responsible for developing and monitoring/keeping PCPs up-to-date?

2.3.7. Most firms will already have compliance officers and well-developed internal AML policies. Therefore, a firm's compliance officer may be best placed to develop and keep PCPs up-to-date in conjunction with a firm's senior management.

2.3.8. Paragraph 10.16 of the Society's 2010 Guidance Notes recommended that a Compliance Officer be appointed to develop and document a firm's AML policies and procedures and also ensure compliance:

"It is also the Society's strong recommendation that each firm should appoint a Compliance Officer with responsibility for establishing and documenting the firm's policies and procedures, ensuring compliance with the firm's obligations and organising training for the relevant staff"

2.3.9. Paragraph 10.3 provides:

"Senior management has an important role to play in implementing a solicitor's AML approach. A firm's internal systems should include allocation to a partner of overall responsibility for the establishment and maintenance of effective AML systems and controls and, where appropriate given the scale of and nature of the firm, the appointment of a person with adequate seniority and appropriate professional training and experience as responsible for the internal and external reporting process. However, it is not a legal requirement to appoint a person to either of these posts. In some firms, depending on complexity, it may be appropriate for the same person to fulfill both roles. Some firms may also consider it appropriate to appoint a person to the role of MLRO with responsibility on a day-to-day basis for maintaining the firm's AML systems and processes aside from reporting."

2.3.10. Furthermore, the 2015 CPD Scheme Regulations introduced a requirement for a solicitor (including a senior practitioner) who is a sole practitioner or a compliance partner and/or an anti-money laundering compliance partner to undertake, as part of their minimum 3 hours of regulatory matters which at least 2 hours of accounting and anti-money laundering compliance.

2.3.11. In addition, it is important to note that the 2018 Act will require that a firm's senior management adopt the PCPs and keep them under review and up-to-date. This replicates much of the Society's current guidance. A substituted section 54(4) provides:

"A designated person shall ensure that policies, controls and procedures adopted in accordance with this section are approved by senior management and shall keep such policies, controls and procedures under review, in particular when there are changes to the business profile or risk profile of the designated person."

2.3.12. Effective management of AML and CTF risks are, therefore, very much the responsibility of senior management of a solicitors' firm and, at a minimum, must be overseen by management.

2.3.13. You can learn more about the Society's guidance about MLROs at paragraphs 10.11 to 10.15 of the Society's 2010 Guidance Notes.

What is the Society's recommended approach to bring your current AML policies up-to-date with new PCP requirements?

2.3.14. All firms will already have written internal AML policies in place and their first step will be to update those policies to ensure compliance with the substituted section 54 and, in particular, section 54(3) which prescribes what the PCP must cover. The new statutory requirements are listed at the beginning of this Section. Your current internal policies may already meet the statutory requirements as they reflect current guidance.

2.3.15. Firms need to develop their own tailored approach to develop PCPs which fit their firm's risk and business needs. It is important that the PCPs take into account the specific outcome of their firm's own Business Risk Assessment.

2.3.16. Firms will need to develop and document systems to meet their obligations and risk profile in a risk-based and proportionate manner. Policies and procedures supporting these systems enable staff to apply the systems consistently and demonstrate to supervisors that processes facilitating compliance are in place.

2.3.17. These PCPs need to be proportionate to the size and nature of your practice.

D. WHAT AREAS SHOULD PCPs COVER?

2.3.18. The Society's existing guidance, at paragraph 10.4, about the systems and controls which a firm's AML policy should cover remains relevant:

- *"Appropriate training on money laundering and terrorist financing to ensure that staff are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;*
- *Appropriate provision of regular and timely information to senior management relevant to the management of the firm's money laundering/terrorist financing risks;*
- *Appropriate documentation of the firm's risk management policies and risk profile in relation to money laundering, including documentation of the firm's application of those policies;*
- *Appropriate measures to ensure that money laundering risk is taken into account in the day-to-day operation of the firm, including in relation to:*
  - *the development of new services;*
  - *the taking-on of new clients; and,*
  - *changes in the firm's business profile.*
- *Appropriate documented internal reporting procedures to ensure prompt reporting of suspicions of money laundering and terrorist financing."*

2.3.19. Similarly paragraph 10.6 of current guidance underpins one of the basic concepts of the risk-based approach - know your client:

"The importance of "knowing your client" for money laundering prevention purposes should be emphasized within firms. Staff should be made aware, not only of the need to know the true identity of the client, but also the need to know enough about the type of business activities expected in relation to that client at the outset in order to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a client's transactions or circumstances that might constitute criminal activity."

2.3.20. In addition, firms should ensure their PCPs comply with section 54(3) in full. Therefore, PCPs must include:

1. PCPs which provide for the identification and scrutiny of matters where:
   - a transaction is complex and unusual and has no apparent economic or legal purpose
   - there is an unusual pattern of transactions and they have no apparent economic or legal purpose
   - there appears to be no apparent economic or legal purpose, or where the commercial rationale is unclear, and a high risk of money laundering is present.

   Legal professionals must carefully consider whether it is appropriate for them to proceed on a matter in the absence of a clear understanding of the nature and purpose of the transaction.

2. Consideration of additional measures to prevent the misuse of products and transactions which favour anonymity.

   It is important that you are able to distinguish between those legal services that you provide and/or transactions in which you act which provide or allow the client a legitimate level of anonymity and those where no good reason for that anonymity has been established and understood.

   Additional measures could include ensuring a better understanding of the background of the transaction and your role in the matter and/or any wider transaction.

3. Consideration of the AML/CTF risk posed to the practice by new technology/legal service delivery methods adopted by the practice.

2.3.21. In addition, the Society has also developed the following supplemental guidance about the issues PCPs must consider:

1. ML/TF risk management practices
2. CDD controls
3. Reliance and record keeping
4. How ML/TF suspicions are managed
5. Review, monitoring and management of compliance with the PCPs

(1) ML/TF risk management practices

2.3.22. A firm's PCPs are interconnected with their Business Risk Assessment and reflect the firm's approach to mitigate the ML/TF risk they face.

2.3.23. Firms should ensure that they have documented their understanding of the key AML/CTF risks that they face in their Business Risk Assessment and refer to those risks in their PCPs. They should keep a record of the sources used in completing their AML/CTF risk assessment.

2.3.24. It is important that decisions taken in relation to the application of the PCPs are documented. For example, if a decision is taken to adopt extra controls in relation to a client or matter, fee earners should record the reason for the additional controls and the nature of the controls.

2.3.25. In relation to your firm's risk management practices you may also wish to consider:

- the level of personnel permitted to exercise discretion on the risk-based application of the AML legislation, and the circumstances under which that discretion may be exercised

- the CDD requirements to be met for simplified, standard and enhanced due diligence
- if outsourcing of CDD obligations or reliance will be permitted, and on what conditions
- the circumstances in which delayed CDD is permitted
- how you will restrict work being conducted on a file where CDD has not yet been completed
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- the manner in which ML/TF suspicions are to be dealt with in a firm

(2) CDD Controls

2.3.26. A firm's PCPs must include a system which outlines the CDD measures to be applied to specific clients.

2.3.27. A firm's risk assessment should record your practice's risk tolerances so that you are able to demonstrate to the Law Society that your CDD measures are appropriate and proportionate.

2.3.28. A firm's CDD system can document:

1. When CDD is to be undertaken
2. Information to be recorded on client identity
3. Information to be obtained to verify identity, either specifically or providing a range of options with a clear statement of who can exercise their discretion on the level of verification to be undertaken in any particular case
4. When simplified due diligence may occur
5. What steps need to be taken for enhanced due diligence
6. What steps need to be taken to ascertain whether your client is a high-risk or low-risk PEP and subsequent controls that will be put in place
7. When CDD needs to occur and under what circumstances delayed CDD is permitted
8. How to conduct CDD on existing clients when it is necessary to do so and how often CDD information will be reviewed to ensure that it is up to date
9. What ongoing monitoring is required

2.3.29. For further information on conducting CDD see Section 5.

(3) Reliance and record keeping

Reliance

2.3.30. PCPs must cover reliance, which is discussed further in Chapter 7 of the 2010 Guidance Notes. A firm should consider including in their PCPs:

- the circumstances in which they consider it appropriate to rely on another regulated person, and
- the steps they will take when relying on another regulated person to satisfy themselves that they have complied fully with the requirements of the Regulations.

Information about reliance on others

2.3.31. In relation to the legality of funds, the acceptance of funds by one designated body is not necessarily an indication of the legality of those funds. This is for a variety of reasons including the fact that once a report has been made there is the risk of the tipping off offence/offence of prejudicing an investigation (this precludes a person who has made a report from informing another person that a report has been made).

2.3.32. Chapter 7 of the 2010 Guidance Notes provides guidance in relation to third party reliance. It is important to note that the fact that one designated entity (a third party) is carrying out its own CDD to meet its AML obligations, does not negate the need for any other designated person to carry out CDD to satisfy their own AML obligations. However, each designated person (whether a solicitor, or a financial or credit institution, etc.) involved in a transaction must carry out their own individual CDD to satisfy their AML obligations. The statutory AML obligations of a designated entity will not be satisfied by simply seeking and/or receiving any form of "confirmation" from another designated entity involved in a transaction. Nor is any such practice envisaged under the AML legislation. As per the AML legislation, each designated entity is required to fulfil their own statutory AML obligations, and it remains their responsibility and statutory obligation to do so, regardless of what other designated entities in a transaction may or may not be doing to meet their AML obligations.

Record keeping

2.3.33. PCPs should set out how the firm complies with the record keeping obligations contained in the AML legislation.

2.3.34. Various records must be kept to comply with the Regulations and also to defend any allegations against the practice in relation to money laundering and failure to report offences.

2.3.35. Your records system must outline what records are to be kept, the form in which they should be kept and for how long they should be kept.

2.3.36. Section 55(7B) (inserted by section 27 of the 2018 Act) requires solicitors to delete any personal data obtained solely for the purposes of AML record retention compliance after the expiry of the current data retention period.

2.3.37. Guidance about statutory record retention obligations is provided in Chapter 11 of the 2010 Guidance.

(4) How ML/TF suspicions are managed?

2.3.38. The Society's strong recommendation is that all firm's appoint a Money Laundering Reporting Officer (MLRO). Guidance is provided at paragraphs 10.11 to 10.15 of the 2010 Guidance Notes.

2.3.39. Guidance about the reporting obligation is provided in Chapter 8 and also in information about the FIU's goAML online reporting system.

2.3.40. In addition, the PCPs can include detail about how suspicions are dealt with. For example, a PCP should require that comprehensive records of suspicions and reports are kept. These records may be necessary in the future in potential criminal proceedings. Such records may include notes of:

- ongoing monitoring undertaken and concerns raised by fee earners and staff
- discussions with the MLRO regarding concerns
- advice sought and received regarding concerns
- why the concerns did not amount to a suspicion and a disclosure was not made
- copies of any disclosures made
- correspondence with the Gardaí/Revenue
- decisions not to make a report which may be important for the MLRO to justify his or her position to law enforcement agencies in the future

(5) Review, monitoring and management of PCP compliance

2.3.41. A significant amount of section 54(3) is concerned with creating requirements that PCPs and the business risk assessment are kept up to date and that compliance with PCPs is monitored. Sections 54(3)(j) to (l) require:

"(j) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,

(k) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and

(l) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures."

2.3.42. Firms must regularly review and update their PCPs and maintain a written record of any changes made following such a review.

2.3.43. Firms must also maintain a written record of any steps taken to communicate PCPs (and any changes) to staff.

2.3.44. Monitoring compliance will assist in assessing whether the PCPs that a firm has implemented are effective in identifying and preventing money laundering and terrorist financing opportunities within their practice.

2.3.45. Paragraph 10.9 of 2010 Guidance remains relevant which suggests that a review for the purposes of monitoring effectiveness cover the following issues:

1. Procedures to be undertaken to monitor compliance, which may involve:
   - random file audits
   - file checklists to be completed before opening or closing a file
   - a compliance officer's log of situations brought to their attention, queries from staff and reports made

2. Reports to be provided to senior management/MLRO on compliance

3. How to rectify lack of compliance, when identified

4. How lessons learnt will be communicated back to staff and fed back into the risk profile of the practice

E. WHO DO PCPS APPLY TO IN A FIRM?

2.3.46. Sections 54(2) and (10) clarify that PCPs apply to sole practitioners, partners and all employees (solicitors and non-solicitors) who provide an AML-regulated legal service.

2.3.47. Solicitors' Firms must ensure their PCPs are documented and available to all relevant staff. Your staff members are the most effective defence against launderers and terrorist financiers who would seek to abuse the services provided by your practice. Guidance is provided about your statutory requirements under section 54(6) to train staff in Chapter 12 of the Guidance Notes: section 54(6) remains unchanged by the 2018 Act.

2.3.48. It is vital that, where staff make decisions in line with the PCPs identified by the practice, they record their decisions and, where appropriate, the decision-making process either on the client record or matter file.

2.3.49. Paragraph 10.5 of the Society's 2010 Guidance Notes emphasised the importance of staff awareness of ML/TF risk and AML policies:

"The effectiveness of the procedures and recommendations contained in these Guidance Notes depends on the extent to which staff in solicitors' firms appreciate the background against which the legislation has been enacted. Relevant staff should be made aware of their statutory obligations and that they may be personally liable for failure to report information in accordance with internal procedures. All relevant staff should be encouraged to become familiar with the requirements of the Act and to provide a prompt report to the designated Money Laundering Reporting Officer (MLRO) of any suspicious transactions."

F. WHAT ARE THE ADDITIONAL PCP MEASURES WHICH THE LAW SOCIETY CAN DIRECT A SOLICITORS' FIRM TO TAKE?

2.3.50. Subsections 54(7), (8) and (9) empower the Law Society to direct solicitors' firms to undertake additional measures to guarantee the robustness of their PCPs as follows:

"(7) A designated person shall 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 under this section if directed in writing to do so by the competent authority for that designated person.

(8) A designated person shall appoint a member of senior management with primary responsibility for the implementation and management of anti-money laundering measures in accordance with this Part if directed in writing to do so by the competent authority for that designated person.

(9) A designated person shall undertake an independent, external audit to test the effectiveness of the internal policies, controls and procedures outlined in this section if directed in writing to do so by the competent authority for that designated person."

2.3.51. Subsection 54(14) empowers the Law Society to direct a category of solicitors' firms to apply additional measures:

"(14) A competent authority may make a direction to a class of designated persons for whom it is the competent authority for the purposes of subsection (7), (8) and (9)."

2.3.52. Subsection 54(12) discharges these additional measures from being applied by sole practitioners:

"(12) Subsections (6), (7), (8), and (9) do not apply to a designated person who is an individual and carries on business alone as a designated person."

2.3.53. In addition, subsection 54(13) requires that regard be had to the appropriateness of applying additional measures to firms on the basis of the size and nature of the firm:

(13) A competent authority shall not issue a direction for the purposes of subsection (7), (8) or (9) unless it is satisfied that, having regard to the size and nature of the designated person, it is appropriate to do so.

G. INFORMATION ABOUT THE NEW REQUIREMENT TO HAVE SYSTEMS IN PLACE TO RESPOND TO ENQUIRIES FROM AN GARDA SIOCHANA

2.3.54. The 2018 Act extends section 56 to designated persons outside the financial sector for the first time and also to solicitors.

2.3.55. The Society made recommendations to the Department of Justice and Equality and also the Department of Finance in relation to the sweeping powers which this may afford An Garda Síochána over the solicitors profession.

2.3.56. It requires that solicitors' firms must establish and maintain systems which enable it to respond fully and promptly to An Garda Síochána enquiries as to—

(a) whether it maintains, or has maintained during the previous five years, a business relationship with a person specified by An Garda Siochana; and
(b) the nature of that relationship.

2.3.57. Responses must factor in legal professional privilege, which is not overridden by such requests. Guidance about legal professional privilege is available in the 'A Guide to Good Professional Conduct for Solicitors' (3rd edition) published by the Guidance and Ethics Committee.

2.3.58. The Society is concerned that an enquiry might arise in relation to a client for whom the solicitor/ firm does not provide an AML-regulated legal service as defined by "relevant independent legal professional" in section 24(1). If a solicitor receives a section 56 request, they must ensure that the named person is/was in receipt of an AML-regulated legal service, otherwise the solicitor is not subject to section 56 and has no statutory power to reveal any information to An Garda Síochána without a warrant for that client's file. In some instances, it may be necessary for the solicitor to request the guidance of the District Court.

2.3.59. In addition, section 42(6A) requires designated persons who have made a report under section 42 to respond to requests for additional information from FIUs.

SECTION 4 - CUSTOMER RISK ASSESSMENTS

A new Section 30B inserted by section 10 of the 2018 Act

CONTENTS

A. BACKGROUND

Are Customer Risk Assessments a new concept?

2.4.1. No. The 2010 Act introduced many concepts to implement the risk-based approach envisioned by the Third Directive. For example, paragraph 4.1 of the Guidance Notes explains how the "legislation allows designated persons, including solicitors, to apply aspects of the client due diligence requirements on a risk-sensitive basis depending on the type of client, business relationship, product or transaction."

What is the purpose of the change?

2.4.2. The Fourth Directive requires Member States to further embed the risk-based approach to prevent it from becoming a tick-the-box exercise.

Existing guidance about how to assess customer/legal service ML/TF Risk

2.4.3. The Society's existing guidance for assessing ML/TF risk when determining client/instruction risk, at paragraphs 4.17 to 4.30 of the 2010 Guidance Notes, remains relevant when determining the risk an instruction poses. However, solicitors should also refer to Section 2 of this Guidance which deals with how to assess ML/TF risk during the course of carrying out a firm's Business Risk Assessment.

2.4.4. A new Section 30B places the need for risk assessment in applying customer due diligence on a statutory footing. The exercise will already be something which solicitors carry out when providing an AML-regulated legal service.

2.4.5. Similarly, paragraphs 11.17 to 11.19 of the Society's 2010 Guidance recommend keeping risk assessment notes:

"Why is it important to keep risk assessment notes?

11.17 Solicitors should consider keeping records of decisions on risk assessment processes of what CDD was undertaken. This does not need to be in significant detail, but merely a note on the

CDD file stating the risk level the solicitor attributed to a file and why the solicitor considered s/he had sufficient CDD information.

11.18 For example:
"This is a low risk client with no beneficial owners providing medium risk instructions. Standard CDD material was obtained and medium level ongoing monitoring is to occur."

11.19 Such an approach may assist firms to demonstrate they have applied a risk-based approach in a reasonable and proportionate manner. Notes taken at the time are better than justifications provided later."

2.4.6. In addition, for many years the Society's AML Helpline has recommended the following approach to solicitors:

"Consider documenting your thought process
In some cases, you may find it helpful to document your thought process, this enables solicitors to:

i. assess the risk of money laundering (i.e., the risk of committing the substantive offence, and whether any known indicators of suspicion may/may not be present);
ii. consider the potential statutory reporting obligation; and,
iii. carry out compliance, should you proceed with the instructions/legal service.

This approach allows solicitors to place all relevant circumstances in context and, should the need arise in the future, enables solicitors to demonstrate their level of knowledge and rationale for proceeding with a legal service or not. By documenting your thought process, solicitors can follow the FATF's (Financial Action Task Force) recommended method for interpreting red flags/indicators of suspicion as follows:
"...the methods and techniques used by criminals to launder money may also be used by clients with legitimate means for legitimate purposes. Because of this, red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation. These red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements of knowing who their client and the beneficial owners are, understanding the nature and the purpose of the business relationship, and understanding the source of funds being used in a retainer. Where there are a number of red flag indicators, it is more likely that a legal professional should have a suspicion that ML or TF is occurring." See page 77 of the FATF 2013 Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals."

B. THE STATUTORY REQUIREMENT

What new?

2.4.7. It is now a statutory requirement to carry out a stand-alone risk assessment on each customer to whom you provide an AML-regulated legal service when determining the type of CDD to be applied to that customer. This will embed the risk-based approach by placing a renewed emphasis on the importance of solicitors' firms conducting a risk assessment of every client to determine their firm's exposure to ML/TF risks and the appropriate CDD to be applied.

What does section 30B require?

2.4.8. Solicitors should read carefully the new section 30B in full, which provides:
30B.— (1) For the purposes of determining the extent of measures to be taken under subsections (2) and (2A) of section 33 and subsections (1) and (3) of section 35, a designated person shall

identify and assess the risk of money laundering and terrorist financing in relation to the customer or transaction concerned, having regard to—

(a) the relevant business risk assessment,

(b) the matters specified in section 30A(2),

(c) any relevant risk variables, including at least the following:

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity of transactions or duration of the business relationship;

(iv) any additional prescribed risk variable,

(d) the presence of any factor specified in Schedule 3 or prescribed under section 34A suggesting potentially lower risk,

(e) the presence of any factor specified in Schedule 4, and

(f) any additional prescribed factor suggesting potentially higher risk.

(5) A designated person who fails to document a determination in accordance with a direction under subsection (2) commits an offence and is liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(b) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).

What does section 30B mean in practice for solicitors?

2.4.9. Section 30B(1) requires that solicitors must assess the ML/TF risk when providing AML-regulated legal services to determine the extent of CDD measures to be applied. This will differ from case to case.

2.4.10. When assessing ML/TF risk of each AML-regulated legal service, solicitors must have regard to:

a. section 30B(1)(a) - their firm's Business Risk Assessment,

b. section 30B(1)(b) – matters specified in section 30A(2) of the Business Risk Assessment requirement which are

   a. information about legal sector risk in the National Risk Assessment – see Section 2 - Business Risk Assessment Chapter

   b. guidance about risk issued by a competent authority – see Section 2 - Business Risk Assessment Chapter

   c. section 30B(1)(c) – any relevant risk variables, including at least the following:

      (i) the purpose of the account or relationship (as neither "account" or "relationship" is defined in the 2018 Act, in the case of solicitors, regard is likely to be had to the purpose of an instruction for an AML-regulated legal service)

      (ii) the level of assets to be deposited by a customer or the size of transactions undertaken. ("Transactions" is defined in the 2010 Act as, in the case of solicitors, meaning the AML-regulated legal services. Please see Glossary for information about the AML-regulated legal services.)

      (iii) the regularity of transactions or duration of the business relationship

   d. the presence of any potentially low risk factor specified in Schedule 3

   e. the presence of any potentially high risk factor specified in Schedule 4

SCHEDULE 3
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:
- *(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.*

SCHEDULE 4

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY HIGHER RISK

(1) Customer risk factors:
- *(a) the business relationship is conducted in unusual circumstances;*
- *(b) customers that are resident in geographical areas of higher risk as set out in subparagraph (3);*
- *(c) non-resident customers;*
- *(d) legal persons or arrangements that are personal asset-holding vehicles;*
- *(e) companies that have nominee shareholders or shares in bearer form;*
- *(f) businesses that are cash intensive;*
- *(g) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.*

(2) Product, service, transaction or delivery channel risk factors:
- *(a) private banking;*
- *(b) products or transactions that might favour anonymity;*
- *(c) non-face-to-face business relationships or transactions;*

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

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

(3) Geographical risk factors:

(a) countries identified by 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.

C. INFORMATION ABOUT HOW TO COMPLETE CUSTOMER RISK ASSESSMENTS

What is the society's guidance for solicitors when complying with 30B requirements?

2.4.11. When assessing individual client and retainer risk, the way in which solicitors comply with CDD requirements must reflect the business risk assessment and customer risk assessment arising in the particular case. In assessing the level of risk arising when providing AML-regulated legal services, legal sector guidance in England and Wales suggests assessing:

- the purpose of the transaction or business relationship,
- the size of the transactions undertaken by the customer and
- the regularity and duration of the business relationship.
- whether the client is within a high-risk category, including whether:
  - they are based or conduct their business in high-risk jurisdictions and/or sectors
  - the retainer involves high-risk jurisdictions, or appears to fall outside of the sector in which the client ordinarily operates.
- whether extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.
- in the event you are aware of negative press or information in respect of your client, which gives you cause for concern in relation to money laundering compliance, you may need to consider:
  - the nature and seriousness of any allegations
  - the level of press coverage and whether the sources of the allegations are reliable or if there is doubt as to their veracity.
- you can be easily satisfied the CDD material for your client is reliable and allows you to identify the client and verify their identity.
- you can be satisfied that you understand their ownership and control structure (particularly if the client or entities in the control structure are based in jurisdictions which permit nominee owners).
- There are concerns about the source of funds or wealth or there are payments to be made by unconnected third parties or payments in cash.
- The retainer involves an area of law or service at higher risk of laundering or terrorist financing.
- Whether the instructions might be considered to be unusual or higher risk, for example:
  - unusually complicated financial or property transactions or transactions where the commercial rationale is unclear
  - instructions on transactional work outside your area of expertise

- transactions involving various potentially connected private individuals (as clients or as beneficial owners) in higher risk jurisdictions
- transactions with an unexplained cross-border element

2.4.12. This assessment will help you to consider whether you are comfortable acting in the particular circumstances and, if so, to adjust your internal controls to the appropriate level of risk presented by the individual client or the particular retainer. Different aspects of your CDD controls will meet the different risks posed:

- If you are satisfied that you have verified the client's identity, but the retainer is high risk, in line with your statutory enhanced CDD obligations you may require fee earners to monitor the transaction more closely, rather than seek further verification of identity.
- If you have concerns about verifying a client's identity, but the retainer is low risk, you may expend greater resources on verification and monitor the transaction in the normal way.

2.4.13. Risk assessment is an ongoing process both for the practice generally and for each client, business relationship and retainer. It is the overall information held by the legal professional gathered while deciding whether to act and also in the course of acting for the client that will inform the risk assessment process, rather than sophisticated computer data analysis systems.

2.4.14. The better you know your client and understand your instructions, the better placed you will be to assess risks and spot suspicious activities.

Consider adapting the Society's Sample Customer Risk Assessment Forms

2.4.15. The Society has developed two sample Customer Risk Assessment Forms to assist solicitors. A 'Risk Factor Questionnaire' and 'Document your throught process' forms. These are available to download from our dedicated AML webpage - www.lawsociety.ie/aml - please use your login to access the AML webpage which is in the members' area.

D. WHAT ARE THE SOCIETY'S EXPECTATIONS IN RELATION TO THE NEW STATUTORY CUSTOMER RISK ASSESSMENT REQUIREMENTS?

2.4.16. Section 30B(2) envisions the documentation of risk assessments to determine the level of CDD to be applied to a customer:

(2) A determination by a designated person under subsection (1) shall be documented where the competent authority for the designated person, having regard to the size and nature of the designated person and the need to accurately identify and assess the risks of money laundering or terrorist financing, so directs.

2.4.17. For the avoidance of doubt, the Law Society as the competent authority for solicitors, recommends that all solicitors document, for every new AML-regulated legal service (whether for an existing or a new client), a Customer Risk Assessment which determines the extent of CDD to be applied.

SECTION 5 - UPDATED CUSTOMER DUE DILIGENCE GUIDANCE

Amendments to sections 33, 35, 36, 37, 38A and 39 and definitions

2.5.1. The changes which the 2018 Act will introduce to the current Client/Customer Due Diligence (CDD) requirements are designed to strengthen the risk-based approach. They do not represent a radical departure and many firms may find their current policies will already deliver the required compliance outcome.

2.5.2. All solicitors will already be very familiar with Chapter 5 first issued in 2010 and, accordingly, the absolute minimum amendments have been made with new guidance only where necessary and helpful. So that solicitors can easily identify new material, new text appears in blue.

2.5.3. A solicitor's Customer Risk Assessment will now inform the type and extent of CDD applied. Information about this new obligation is provided earlier in this Guidance. It is no longer possible to conduct CDD on the basis of a specific category of client. Instead, a solicitor will need to determine the type of CDD to apply based on the outcome of the individual customer risk assessment.

A. SUMMARY

1. Standard CDD (sections 33 – 35)
2. Simplified (section 34A)
3. Enhanced (sections 37 and 39)

B. STANDARD CDD

- Generally, how should CDD be applied?

1. Standard CDD Measure 1 - Identifying the client and verifying the client's identity
    - Identification or verification?
    - What does identification mean?
    - What does verification mean and what sources of evidence can be used?
    - When must identification and verification be undertaken?
    - What are the requirements where contact is non face-to-face?
    - What is electronic verification?
    - What about using electronic verification providers?
    - How can the identity of different types of clients be verified?
    - New requirement to identify persons acting on behalf of the client introduced by the 2018 Act?
2. Standard CDD Measure 2 - Identifying the beneficial owners and taking measures reasonably warranted by the ML/TF risk to verify their identity
    - What is the obligation to identify beneficial owners?
    - What are the different definitions of "beneficial owner"?
3. Standard CDD Measure 3 - Obtaining information reasonably warranted by the risk of ML/TF on the purpose and intended nature of the business relationship
    - Do I need to obtain evidence or "determine" the source of funds/wealth?
4. Standard CDD Measure 4 - Conducting ongoing monitoring
    - How can ongoing monitoring of the business relationship be conducted

C. SIMPLIFED CDD

- What is the statutory criteria for SCDD eligibility?
- What does section 34A mean in practice for solicitors?

D. ENHANCED CDD

1. Enhanced CDD Duty 1- Complex/Unusual transactions - Section 36A
2. Enhanced CDD Duty 2 - Risk that client involved in ML/TF, ascertain PEP status - Section 37
    - Who is a PEP?
    - What do I have to do if my client is a PEP?

- Establishing source of wealth and funds
- How can PEPs be identified?

3. Enhanced CDD Duty 3 - Client is established or resides in a high-risk third country - Section 38A
   - Who is on the list?
   - Can a country pose a higher ML/TF Risk but not be designated as a "high-risk third country"?
   - Other useful resources
4. Enhanced CDD Duty 4 - Business relationship (client or AML-regulated legal service) is High Risk for ML/TF - Section 39
   - High risk circumstances requiring enhanced CDD where non face-to-face clients

A. SUMMARY

2.5.4. There are three categories/types of client due diligence – (1) simplified, (2) enhanced and (3) 'standard'. You must apply CDD to clients to whom you provide AML-regulated legal services (please see Glossary for more information about what is meant by AML-regulated legal service). A summary is provided below:

1. 'Standard' CDD (sections 33 – 35)

2.5.5. Typically, most solicitors' clients will require standard CDD and the solicitor's Customer Risk Assessment will indicate the type and extent of CDD required in each case. The standard CDD measures are:

(1) Identifying the client and verifying the client's identity

(2) Identifying the beneficial owners and taking measures reasonably warranted by the ML/TF risk to verify their identity

(3) Obtaining information reasonably warranted by the risk of ML/TF on the purpose and intended nature of the business relationship

(4) Conducting ongoing monitoring

2.5.6. The 2018 Act removes the CDD requirement to apply additional measures to non-face-to-face clients (formerly section 33(4)). However, while non-face-to-face instructions are not described as "enhanced", Schedule 4(2)(c) will mean that non-face-to-face clients/instructions are regarded as a factor suggesting potentially higher risk for consideration in the customer risk assessment.

2. Simplified (section 34A)

2.5.7. Section 34A permits simplified due diligence to be undertaken where the solicitor determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing on the basis of specific statutory criteria.

3. Enhanced (sections 37 and 39)

2.5.8. The legislation now prescribes the following four specific circumstances when enhanced due diligence measures must be applied:

(1) Complex/Unusual transactions - Section 36A

(2) Risk that client involved in ML/TF, ascertain PEP status - Section 37

(3) Client is established or resides in a high-risk third country - Section 38A

(4) Business relationship (client or AML-regulated legal service) is High Risk for ML/TF - Section 39

2.5.9. The Society recommends that solicitors consider the extent to which they might unwittingly commit the substantive offence of money laundering by providing a high risk legal service which requires enhanced CDD measures. Solicitors should document their thought process and detail their KYC (knowledge of client) when determining whether to provide a high risk AML-regulated legal service. The exercise of 'documenting your thought process' when ML/TF red flags are present can greatly assist a solicitor in the future should an AML-regulated legal service ever be examined by an Investigating Accountant or investigated by the CAB or the FIU.

B. STANDARD CDD

2.5.10. Under sections 33-35 of the 2010 Act as amended, Client Due Diligence (CDD) is defined as comprising the four following obligations which must be applied in accordance with the Customer Risk Assessment.

Generally, how should CDD be applied?

2.5.11. CDD must be applied in accordance with a firm's PCPs and as determined by the Customer Risk Assessment guidance which is provided earlier in this Update.

Standard CDD Measure 1 - Identifying the client and verifying the client's identity

2.5.12. Identifying the client and verifying the client's identity on the basis of documents, data or information (which the solicitor has reasonable grounds to believe can be relied upon to confirm the identity of the customer including documents from a Government source (section 33(2)(a)). The 2018 Act introduces a new standard CDD requirement to verify that any person purporting to act on behalf of the customer is so authorised, together with the need to identify and verify the identity of that person along the normal lines (section 33(2A)).

Identification or verification?

2.5.13. Identification of a client or a beneficial owner means establishing a client's identifying details, such as their name and address.

2.5.14. The statutory obligation is to verify identity. Verification of identity means obtaining some evidence which supports a client or beneficial owner's claim of identity.

What does identification mean?

2.5.15. Identification is simply the process whereby a solicitor obtains from a client the information s/he considers necessary to know who the client is. The identity of an individual has a number of aspects: e.g. name (which of course may change), date of birth etc.. Other facts about an individual accumulate over time e.g. family circumstances and addresses, employment and business career, contacts with the authorities or with designated persons, physical appearance. The identity of a corporate client is a combination of its constitution, its business, and its legal and ownership structure.

What does verification mean and what sources of evidence can be used?

2.5.16. Verification is the process through which the solicitor establishes that the information obtained in relation to the client's identity is correct on the basis of satisfactory evidence provided by the client or obtained by the solicitor him/herself.

2.5.17. Evidence of identity can take a number of forms. Evidence of identity can be obtained in documented or electronic format. In respect of individuals, "identity documents", such as passports and driving licences, are often the best way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a client's identity based on other forms of confirmation including, in appropriate circumstances, written or otherwise documented assurances from persons or organisations that have dealt with the client for some time. Recommendations of the Society as to best practice identity documents are set out in Chapter 6 of the 2010 Guidance.

2.5.18. The quantity of evidence required to verify a client's identity is dependent upon the risk category to which the client has been allocated by the solicitor.

2.5.19. Verification is possible using either documentary or electronic format, or a combination of both where appropriate. This guidance is not intended to suggest that documentary verification must be corroborated by electronic verification or vice versa. Examples of risk-based identification and verification procedures are included in Chapter 6 of the 2010 Guidance.

2.5.20. There is no prohibition on the acceptance of faxed or scanned copies of documentation.

2.5.21. Where the interaction with the client is on a face-to-face basis, the solicitor should have sight of the original document(s) and appropriate details should be recorded.

2.5.22. In cases where a client produces non-standard documentation to meet the identification and verification requirements, the solicitor may consider instituting enhanced monitoring arrangements over the client's activities utilising a risk-based approach.

2.5.23. Where other professionals use your services in their capacity as a professional rather than a private individual, you may consult their professional directory to confirm the person's name and business address. It will not be necessary to then confirm the person's home address. You may consult directories for foreign professionals, if you are satisfied it is a valid directory, e.g. one produced and maintained by their professional body and, if necessary, you can translate the information unless you already have a sufficient understanding of what it says.

When must identification and verification be undertaken?

2.5.24. Section 33(1) requires that the verification of the identity of the client and, where applicable, the beneficial owner must take place prior to the establishment of a business relationship or the carrying out of a transaction or service.

2.5.25. Verification of the identity of the client and, where applicable, the beneficial owner, may be completed during the establishment of a business relationship if:

- This is necessary not to interrupt the normal conduct of business; and
- There is no real risk of money laundering or terrorist financing occurring, provided that the verification is completed as soon as practicable after the initial contact.

2.5.26. The assessment of when it might be appropriate for a solicitor to establish a business relationship in accordance with the paragraph above is a matter for each solicitor, according to the nature of the services being provided. However, where a solicitor enters into a business relationship in advance of verification of identity, he/she should be extremely careful regarding the acceptance of any funds from the client, including the return of any funds transferred by the client to the solicitor prior to the completion of verification. The Society's best practice guidance is that solicitors complete CDD prior to agreeing to provide an AML-regulated legal service – this will be in the firm's best interest from a risk management perspective.

2.5.27. Section 33(1)(c), substituted by the 2013 Act, requires that identification and verification take place prior to carrying out any service for a customer if there are reasonable grounds to suspect ML/TF with regard to specific statutory factors. In such circumstances, solicitors must be mindful of the risk of committing ML/TF and consider whether they are in a position to proceed with the AML-regulated legal services and any potential requirement to make a report (see Chapter 8 of the Guidance Notes).

2.5.28. Section 33(1)(e), inserted by the 2018 Act, requires that verification of identity take place "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." The Society's best practice recommendation is to complete a Customer Risk Assessment for every new legal AML-regulated legal service and ensure AML CDD is in compliance with the 2018 Act.

2.5.29. Solicitors should also have regard to the advice in Section 1 - Introduction of this Updated Guidance which deals with the transitioning of existing clients, AML-regulated legal services already in train and future AML-regulated legal services.

What are the requirements where contact is non face-to-face?

2.5.30. The 2018 Act now lists, in Schedule 4, non-face-to-face business relationships or transactions as potentially higher risk. Solicitors must now consider the presence of any factor specified in Schedule 4 in their customer risk assessment required under section 30B.

2.5.31. Where a client approaches a solicitors' firm remotely (by post, telephone or over the internet), this may be an indicator of product, service, transaction or delivery channel risk.

2.5.32. Paragraph 6.20 of the 2010 Guidance already highlights non-face-to-face risks:

"Any mechanism (e.g. post, telephone, or electronic) that avoids face-to-face contact between a solicitor and a prospective new client inevitably poses challenges for client identification. Legal services conducted on the Internet adds a new dimension to risks and opens up new mechanisms for fraud and money laundering"

2.5.33. If, following the Customer Risk Assessment, the solicitor is satisfied that there is no risk of ML/TF, the solicitor may decide to follow the previous section 33(4) statutory requirement and carry out non face-to-face verification, either electronically, and/or by reference to documents in accordance with the requirements, although the Law Society would emphasise the inherent risks in doing so.

2.5.34. Where the client has not been physically present for identification purposes, section 33(4) had previously suggested by way of examples that one or more of the following measures could be undertaken:

a) Ensuring that the client's identity is established by additional documents, data or information,

Examples of a):

- Telephone contact with the client prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise).
- Communicating with the client at an address that has been verified (such communication may take the form of a direct mailing of documentation/terms of engagement to him which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- Electronic verification via a commercial agency where electronic verification has not been used to originally verify the client.

b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by another designated body covered by the legislation;

c) verification of the client's identity on the basis of confirmation received from an acceptable third party that the client is, or has been, a client of that third party;

d) ensuring that one or more of the following transactions is carried out through an account in the client's name with an acceptable institution that is a credit institution in the EU:

i. the first payment made by the client to the solicitor for the provision of a service;

ii. in the case of a financial transaction or a transaction relating to land, the first payment made by the client in respect of the transaction.

2.5.35. Should the solicitor decide to provide the AML-regulated legal service to non-face-to-face clients, the extent of the CDD required will depend on the assessed money laundering risk presented by the client and documented in the solicitor's customer risk assessment. Enhanced CDD may be prudent.

2.5.36. There are some circumstances where the client is typically not physically present which would not in itself increase the risk attaching to the transaction or activity. For example, a person normally resident in Ireland might be temporarily working abroad and instruct a solicitor in a conveyance. In some circumstances this would increase risk but, depending on the solicitors knowledge of the client, non-face-to-face instruction may be acceptable. A solicitor should take account of such cases in developing their systems and procedures. Where third parties are relied upon to carry out CDD and meet the client, in line with the statutory requirements and guidance in Chapter 7 of 2010 Guidance, this may be viewed as face-to-face identification for the purposes of the solicitor's risk assessment.

2.5.37. Additional measures would also include assessing the possibility that the client is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances. Solicitors should be particularly wary where they are approached to provide a service, e.g. debt collection, which subsequently does not proceed but it is proposed that the debt will still be 'collected' through the solicitor's client account and a fee deducted by the solicitor.

2.5.38. In an increasingly global and technologically advanced environment, it is sometimes the case that you may act for clients without meeting them. You should include this as a factor when you carry out your practice-wide risk assessment.

2.5.39. In addition, you should consider the systems and procedures that you have implemented to mitigate the risks associated with acting for clients you do not meet. When you act for clients without meeting them you must be satisfied that it makes sense in all the circumstances not to do so and you must be comfortable that you can mitigate the risks of identity fraud. Further non-face-to-face guidance is provided under Enhanced CDD below.

What is electronic verification?

2.5.40. A number of commercial agencies which access many data sources are accessible online to designated persons, and may provide a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list.

2.5.41. Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required. Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information can reduce the risk of impersonation fraud.

2.5.42. Before using a commercial agency for electronic verification, it is advisable that firms become satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate and they should document the outcome of this assessment.

2.5.43. In addition, a firm may wish to confirm that a commercial agency has processes that allow the enquirer to capture and store the information they used to verify an identity.

2.5.44. Given the higher risk of exposure to impersonation when using electronic verification, solicitors should also undertake one or more of the following checks:

- Telephone contact with the client prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the client before the business relationship starts, using it to verify additional aspects of personal identity information that have been previously provided during the taking of initial instructions;
- Communicating with the client at an address that has been verified (such communication may take the form of a direct mailing of terms of engagement documentation to him which, in full or in part, might be required to be returned completed or acknowledged without alteration).

What about using electronic verification providers?

2.5.45. This will only confirm that someone exists, not that your client is the said person. Solicitors should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that the client is not the person they say they are. Solicitors may choose to mitigate risk by corroborating electronic verification with some other CDD material. When choosing an electronic verification service provider, solicitors should look for a provider who:

- has proof of registration with the Data Protection Commissioner's Office to store personal data
- can link a user to both current and previous circumstances using a range of positive information sources
- accesses negative information sources, such as databases on identity fraud and deceased persons
- accesses a wide range of 'alert' data sources
- has transparent processes enabling the solicitor to know what checks are carried out, the results of the checks, and how much certainty they give on the identity of the subject
- allows the solicitor to capture and store the information used to verify an identity.

2.5.46. When using electronic verification, solicitors are not required to obtain consent from the client, but clients should be informed that such checks may take place.

2.5.47. Where verification is to be undertaken using electronic verification, it is recommended that the designated person uses as its basis the client's full name and date of birth or full name and current address.

How can the identity of different types of clients be verified?

2.5.48. Chapter 6 contains the Society's recommendations as to how solicitors can best meet their obligation to verify the identity of a wide variety of clients on the basis of varying types of documents.

New requirement to identify persons acting on behalf of the client introduced by the 2018 Act

2.5.49. The 2018 Act introduced a new standard CDD requirement to verify that any person purporting to act on behalf of the customer is so authorised, together with the need to identify and verify the identity of that person along the normal lines (section 33(2A)).

2.5.50. Section 33(2A) provides:

"When applying the measures specified in subsection (2), a designated person shall verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person in accordance with subsection (2)."

2.5.51. Accordingly, where a person purports to act on behalf of your client, solicitors should:

- verify that the representative is authorised to act on your client's behalf
- identify the representative
- verify the identity of the representative on the basis of documents and information from a reliable source

2.5.52. In correspondence with the Law Society, the Department of Justice and Equality and the Department of Finance have indicated that this obligation is confined to agents. Section 33(2A) does not introduce an obligation to identify co-advisors or other professional service providers who are not in the chain of instruction between client and solicitor.

Standard CDD Measure 2 - Identifying the beneficial owners and taking measures reasonably warranted by the ML/TF risk to verify their identity

2.5.53. This requires: (1) Identifying the beneficial owners, as defined by the Act, connected with the customer or service concerned and (2), **taking measures reasonably warranted by the risk of ML/TF** to (i) **verify their identity** so that the firm is satisfied that it knows who the beneficial owner is and (ii) in the case of a legal entity or legal arrangement defined by sections 26 to 30 **understands the ownership and control structure of the client.** The 2018 Act amends the relevant definitions of beneficial owners in sections 26, 27, 28 and 30. In addition, the 2018 Act requires that, when beneficiaries of trusts or similar legal arrangements are designated by particular characteristics, the solicitor must be satisfied that they will be able to establish the identity of the beneficiary at the time of the payout/exercise by the beneficiary of its vested rights (section 33(7D)).

2.5.54. You will also need to consider the identity of beneficial owners where you cannot apply simplified due diligence.

What is the obligation to identify beneficial owners? Also, what must be verified for beneficial owners?

2.5.55. Section 33(2)(b) (a requirement which has been in place since 2010) obliges solicitors, in accordance with the Customer Risk Assessment (new in the 2018 Act), to take steps:

"identifying any beneficial owner connected with the customer or service concerned, and **taking measures reasonably warranted by the risk of money laundering or terrorist financing—**

(i) to **verify the beneficial owner's identity to the extent necessary** to ensure that the person has reasonable grounds to be satisfied that the person knows who the beneficial owner is, and

(ii) in the case of a legal entity or legal arrangement of a kind referred to in section 26, 27, 28 or 30, to **understand the ownership and control structure** of the entity or arrangement concerned.

2.5.56. Section 24(1) provides that the term "beneficial owner" has the meaning assigned to it by sections 26 to 30. These sections define the term "beneficial owner" in the context of various types of entities.

What are the different definitions of "beneficial owner"?

2.5.57. Beneficial owner in relation to bodies corporate – section 26 as amended and by reference to the Fourth Directive:

(a) *"in the case of corporate entities:*

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with [European] Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council (3);

(ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;"

2.5.58. Beneficial owner in relation to partnerships – section 27 as amended provides:
""beneficial owner", in relation to a partnership, means any individual who—

(a) ultimately is entitled to or controls, whether the entitlement or control is direct or indirect, more than a 25 per cent share of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership, or
(b) otherwise controls the partnership."

2.5.59. Beneficial owner in relation to trusts – section 28 as amended provides:

"(2) (a) any individual who is entitled to a vested interest in possession, remainder or reversion, whether or not the interest is defeasible, in the capital of the trust property;

(b) in the case of a trust other than one that is set up or operates entirely for the benefit of individuals referred to in paragraph (a), the class of individuals in whose main interest the trust is set up or operates;

(c) any individual who has control over the trust;

(d) the settlor;

(e) the trustee;

(f) the protector.

(3) For the purposes of and without prejudice to the generality of subsection (2), an individual who is the beneficial owner of a body corporate that—

(a) is entitled to a vested interest of the kind referred to in subsection (2)(a), or

(b) has control over the trust,
is taken to be entitled to the vested interest or to have control over the trust (as the case may be).

(4) Except as provided by subsection (5), in this section "control", in relation to a 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 trust property;

(b) vary the trust;

(c) add or remove a person as a beneficiary or to or from a class of beneficiaries;

(d) appoint or remove trustees;

(e) direct, withhold consent to or veto the exercise of any power referred to in paragraphs (a) to (d).

(5) For the purposes of the definition of "control" in subsection (4), an individual does not have control solely as a result of the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are at least 18 years of age, have full capacity and (taken together) are absolutely entitled to the property to which the trust applies."

2.5.60. Beneficial owner in relation to estates of deceased persons is unchanged by the 2018 Act – section 29 provides:

"in relation to an estate of a deceased person in the course of administration, means the executor or administrator of the estate concerned."

2.5.61. While there is no amendment in the 2018 Act to the section 29 definition, a new section 33(7D) requires that:

"in addition to verification measures for customers and beneficial owners, in the case of beneficiaries of trusts or similar legal arrangements that are designated by particular characteristics or class, a designated person shall obtain sufficient information concerning the beneficiary to satisfy the designated person that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights."

2.5.62. Accordingly, when writing to any beneficiary under a Will, discretionary or otherwise, and where there are no ML/TF concerns, solicitors should always ask the beneficiary to send in a photocopy of current passport or driver's licence and a recent utility bill.

2.5.63. Other persons who are beneficial owners – section 30 (as amended) provides: –

"*(1) In this Part, "beneficial owner", in relation to a legal entity or legal arrangement, other than where section 26, 27 or 28, applies, means—*

(a) if the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from the property of the entity or arrangement,

(b) if the individuals who benefit from the entity or arrangement have yet to be determined, the class of such individuals in whose main interest the entity or arrangement is set up or operates, and

(c) any individual who exercises control over the property of the entity or arrangement

(d) any person holding a position, in relation to the legal entity or legal arrangement that is similar or equivalent to the position specified in paragraphs (d) to (f) of section 28(2) in relation to a trust.

(2) For the purposes of and without prejudice to the generality of subsection (1), any individual who is the beneficial owner of a body corporate that benefits from or exercises control over the property of the entity or arrangement is taken to benefit from or exercise control over the property of the entity or arrangement.

(3) In this Part, "beneficial owner", in relation to a case other than a case to which section 26, 27, 28 or 29, or subsection (1) of this section, applies, means any individual who ultimately owns or controls a customer or on whose behalf a transaction is conducted."

2.5.64. Therefore, the 2018 Act deletes "at least 25 per cent of" from sections 30(1)(a) and (b) and inserts a new section 30(d).

2.5.65. If identification of the ultimate beneficial owner is not possible for whatever reason, consideration must be given to making a report to the Gardaí and the Revenue Commissioners.

2.5.66. In due course, supplemental guidance will be issued as part of an update of Chapter 6 of 2010 Guidance to provide solicitors with suggestions for CDD on different types of clients including beneficial owners and trusts.

Standard CDD Measure 3 - Obtaining information reasonably warranted by the risk of ML/TF on the purpose and intended nature of the business relationship

2.5.67. Since the 2010 Act, solicitors have been required to obtain information reasonably warranted by the risk of ML/TF on the purpose and intended nature of the business relationship prior to the establishment of the relationship (section 35(1)). While there has always been a prohibition on providing the service until such information is supplied (section 35(2)), the 2018 Act provides welcome clarification that this prohibition does not apply to non-AML regulated legal services (section 33(8A).

2.5.68. The obligation to obtain information from a client on the purpose and nature of the business relationship is one that must be applied to all clients seeking AML-Regulated Legal Services with whom a solicitor is entering into a business relationship. However, in most cases, this will be self-evident given the nature of the transaction being undertaken or service being provided or may be easily clarified by discussing with the client what they are seeking from the relationship.

2.5.69. Where a solicitor proposes to enter into a business relationship with a client and the solicitor's assessment of the risk associated with the client or with the nature of the transactions or services to be provided to the client indicate a higher than standard risk of money laundering or terrorist financing, then the solicitor should obtain the following information during the establishment of the business relationship:

- Nature and details of the business/occupation/employment of the client;
- The expected source and origin of the funds to be used in the transaction;
- The various relationships between signatories and with underlying beneficial owners; and
- The anticipated level and nature of the activity that is to be undertaken through the relationship.

2.5.70. A key aspect of understanding the purpose and nature of the business relationship is to collect information on clients, in particular those in higher risk categories. Aside from the statutory requirement, it assists solicitors in deciding whether they are in a position to provide the AML-regulated legal service. Over time, the solicitor should develop a greater understanding of the business or nature of the activities undertaken by the client. While it is necessary to obtain information on the purpose and nature of the business relationship at the outset of the relationship, the reliability of this profile will only increase over time as the solicitor learns from experience what the client is about.

Do I need to obtain evidence or "determine" the source of funds/wealth?

2.5.71. Solicitors often enquire whether they must obtain evidence of source of funds/wealth. If a client is eligible for standard CDD with low/medium ML/TF risk, the goal will likely be to obtain information about the source or origin of funding. This generally involves asking questions about where funding will come from and how the client came to have the funds. Standard CDD does not require solicitors to "determine" the source of funds/wealth. All that is required is that the information being provided about source of funds/wealth is consistent with the solicitor's customer risk assessment and there are no potential red flags for ML/TF (e.g. funding from third parties).

2.5.72. For each retainer, it is important to have an understanding of where the funds to finance the

transaction are coming from. That information will then help you to decide the level of scrutiny, if any, required of that source. You are not required to question a wealthy private client about their entire financial history, nor are you required to undertake detailed due diligence of a business. The Society's guidance is that you should consider whether the source of funds is consistent with the risk profile of the client, the retainer and their business.

2.5.73. However, it may be prudent, even when standard CDD is applicable, to ask for some supporting evidence to confirm the information provided. Where such supporting evidence is provided, it is important that you look at that evidence to see if it is actually consistent with the client's explanation or whether it throws up more questions. If an explanation is consistent with the client's risk profile, is consistent with the type of retainer being undertaken, and you do not have other AML concerns about the transaction, you should simply note the explanation on the file and request accounts staff to check that the funds are coming from the bank accounts the client has said they would come from.

2.5.74. If the transaction is higher risk and enhanced CDD may be applicable or you have determined it is prudent to ask for supporting evidence in standard CDD, you may ask for supporting evidence, possibly in the form of:

- bank statements
- recently filed business accounts, or
- documents confirming the source, such as a sale of a house, sale of shares, receipt of a personal injuries award, a bequest under an estate or a win from gambling activities.

2.5.75. Where cash is involved it becomes more challenging, as a bank statement showing a large withdrawal does not mean that the cash the client is now in possession of was actually the money withdrawn. Equally, a bank statement showing a large cash deposit does not provide you with information about where the cash came from in the first place.

2.5.76. There can also be situations where a client cannot or will not produce any paperwork to back up their account of where the funds have come from. Does this mean that you automatically suspect money laundering? Not everyone is efficient at keeping paperwork and the funds may have arisen some time ago.

2.5.77. In addition, please note that source of funds is different from source of wealth. Source of funds means where the client's funds are received from – an Irish bank account for example. Source of wealth means how the client came to have the funds in question via inheritance, house sale, or investment windfall for example. Source of wealth is fundamental to money laundering risk assessment. If you are clear about the legitimacy of a client's source of wealth, the risk of money laundering is significantly reduced.

2.5.78. The obligation to "determine" or obtain evidence about the source of funds/wealth is an enhanced CDD measure. See also "Establishing source of wealth and funds" later in this section. It is only a statutory requirement when there is a high risk of ML/TF and, in such circumstances, the Society recommends that solicitors consider the extent to which they might unwittingly commit the substantive offence of money laundering by providing a high risk legal service which requires enhanced CDD measures. Solicitors should document their thought process and detail their KYC (knowledge of client) when determining whether to provide a high risk AML-regulated legal service. The exercise of 'documenting your thought process' when ML/TF red flags are present can greatly assist a solicitor in the future should an AML-regulated legal service ever be examined by an Investigating Accountant or investigated by the CAB or the FIU.

2.5.79. This approach allows solicitors to place all relevant circumstances in context and, should the need

arise in the future, enables solicitors to demonstrate their level of knowledge and rationale for proceeding with a legal service or not. By documenting your thought process, solicitors can follow the FATF's (Financial Action Task Force) recommended method for interpreting red flags/indicators of suspicion as follows:

> "...the methods and techniques used by criminals to launder money may also be used by clients with legitimate means for legitimate purposes. Because of this, red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation. These red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements of knowing who their client and the beneficial owners are, understanding the nature and the purpose of the business relationship, and understanding the source of funds being used in a retainer. **Where there are a number of red flag indicators, it is more likely that a legal professional should have a suspicion that ML or TF is occurring.**" See page 77 of the FATF 2013 Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals."

2.5.80. Ask yourself the following questions:

- Is this consistent with what I know about the client?
- Do I have information which makes me suspicious of ML/TF?

2.5.81. If the retainer is consistent and you do not suspect that existing criminal property is involved, you don't have to go further to prove that the funds are clean. Remember that you are not a member of An Garda Síochána investigating potential crime; you are simply taking steps to protect your firm from being used to launder funds. You need to make your own decision about the consistency of the source of funds with what you know about the client and whether there is information on which you can form a suspicion of money laundering or not.

2.5.82. If, after the explanations and the supporting documents are received, you are still concerned about the source of funds, you will need to consider whether the proceeds of crime/ML/TF is involved. It is important to remember that documentation about source of funds (e.g. copy bank statements) may never adequately negate the inherent ML/TF risk.

2.5.83. You may be suspicious because you have information about a specific offence, such as tax being avoided, benefits being received which should not have been, or press articles which show a client has been charged with drug offences. Alternatively, you may be suspicious because this is the logical conclusion to be drawn due to the manner of the handling of the funds in the transaction. In those circumstances, you should consider whether you have an obligation to report your suspicion to the authorities. Guidance about the reporting obligation is provided in Chapter 8 2010 Guidance and also in information about the FIU's goAML online reporting system.

2.5.84. Accordingly, the Society encourages solicitors to ascertain the precise details of what is being proposed when considering whether to provide an AML-regulated legal service. It is best for solicitors and their potential future clients, that the solicitor collates information about the purpose and nature of an AML-regulated legal service before deciding whether they are in a position to provide that service. Solicitors also need to be cautious about purchases of property where no financing is required and/or financing is being provided from outside the EU. In particular, the Society recommends that solicitors ascertain if a proposed legal service will necessitate the transfer of funds into their client account and from whom and what country those funds will originate having particular regard to proposed transfers from third parties or from outside the EU financial system.

Standard CDD Measure 4 - Conducting ongoing monitoring

2.5.85. Conducting ongoing monitoring (to the extent reasonably warranted by the risk of ML/TF) of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the firm's knowledge of the client, the business and risk profile including, where necessary, the source of funds.

2.5.86. Ongoing monitoring is required by section 35(3) of the 2010 Act and the 2018 Act uses a slightly different approach to monitoring:

"A designated person shall monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of money laundering or terrorist financing."

2.5.87. Section 24(1) provides a definition of "monitoring":

""*monitoring", in relation to a business relationship between a designated person and a customer, means the designated person,* ***on an ongoing basis—***

(a) scrutinising transactions, and the source of wealth or of funds for those transactions, ***undertaken during the relationship*** *in order to determine if the transactions are consistent with the designated person's knowledge of—*

(i) the customer,

(ii) the customer's business and pattern of transactions, and

(iii) ***the customer's risk profile (as determined under section 30B)****, and*

(b) ***ensuring that documents, data and information on customers are kept up to date in accordance with its internal policies, controls and procedures adopted in accordance with section 54;"***

How can ongoing monitoring of the business relationship be conducted?

2.5.88. The obligation to monitor clients applies to those clients with whom the solicitor has established a business relationship as defined.

2.5.89. The objective of the ongoing monitoring obligation imposed by the legislation is firstly, to identify activities of clients during the course of the business relationship which are not consistent with the solicitor's knowledge of the client, the Customer Risk Assessment for the client, or the purpose and intended nature of the business relationship, and which need to be assessed for the possibility that the solicitor may have grounds to report a suspicion of money laundering or terrorist financing. Secondly, to ensure, on the basis of that assessment, that the documents, data or information held about the client are kept up-to-date in accordance with the firm's PCPs. Records should be kept up-to-date based on information gathered during the normal course of business.

2.5.90. Solicitors are not required to:

- conduct the whole CDD process again every few years
- suspend or terminate a business relationship until they have updated data, information or documents, as long as the solicitor is still satisfied he/she knows who the client is, and keeps under review any request for further verification material or processes to get that material

- use sophisticated computer analysis packages to review each new client file for anomalies.

2.5.91. Internationally, many practices operate a system of regular review and renewal of CDD as good practice.

2.5.92. Ongoing monitoring will normally be conducted by fee earners handling the client file, and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material. A high degree of professionalism and scrutiny is expected from legal professionals – see R v Griffiths & Pattison (2007) CA which confirmed that legal professionals are expected to fulfil these obligations 'up to the hilt'.

2.5.93. For example, a solicitor may have acted for a client in preparing a Will and purchasing a modest family home. They may then receive instructions to purchase a holiday home, the value of which appears to be outside the means of the client's financial situation as had been previously been advised in earlier transactions. While a solicitor may be satisfied that he/she still knows the identity of the client, as a part of ongoing monitoring obligations it would be appropriate in such a case to ask about the source of the funds for this purchase. Depending on the client's willingness to provide such information and the answer they provide, a solicitor would need to consider whether he/she was satisfied with that response, wanted further proof of the source of the funds, or needed to discuss making a report to the MLRO, or consider making a report to the authorities.

2.5.94. To ensure that CDD material is kept up-to-date, solicitors should consider reviewing it:

- when taking new instructions from a client, particularly if there has been a gap of over three years between instructions
- when a firm receives information of a change in identity details
- when instructions change, in particular, when funding is being provided by sources other than the client

2.5.95. Relevant issues may include:

- the risk profile of the client
- whether the solicitor holds material on transactional files which would confirm changes in identity
- whether electronic verification may help to find out if the client's identity details have changed, or to verify any changes

2.5.96. In circumstances where no subsequent action was taken/change effected as a result of the obligation to conduct ongoing monitoring through the lifecycle of a transaction, it is suggested that practices should record:

- that they considered this issue,
- that they took no action, and
- the reasons for that decision.

C. SIMPLIFED CDD

2.5.97. Simplified client due diligence (SCDD) means that a solicitor can determine the extent to which they must apply the CDD measures under sections 33(2) and 35 because they determine the legal services are at a low risk of ML/TF. This no longer applies on the basis of a client falling into a specific category. The solicitor must obtain sufficient information about the client to satisfy itself that the client meets the statutory criteria for SCDD to be applied.

What is the statutory criteria for SCDD eligibility?

2.5.98. Solicitors should read in full the specific statutory requirement for SCDD eligibility in section 34A: *"34A.— (1)Subject to section 33(1)(c) and (d), a designated person may take the measures specified in sections 33(2) and 35 in such manner, to such extent and at such times as is reasonably warranted by the lower risk of money laundering or terrorist financing in relation to a business relationship or transaction where the designated person—*

(a) identifies in the relevant business risk assessment, an area of lower risk into which the relationship or transaction falls, and
(b) considers that the relationship or transaction presents a lower degree of risk.

(2) For the purposes of identifying an area of lower risk a designated person shall have regard to—
(a) the matters specified in section 30A(2),
(b) the presence of any factor specified in Schedule 3, and
(c) any additional prescribed factor suggesting potentially lower risk.

(3) Where a designated person applies simplified due diligence measures in accordance with subsection (1) 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 designated person to detect unusual or suspicious transactions...

(5) For the purposes of subsection (1), a business relationship or transaction may be considered to present a lower degree of risk if a reasonable person having regard to the matters specified in paragraphs (a) to (f) of section 30B(1) would determine that the relationship or transaction presents a lower degree of risk of money laundering or terrorist financing."

What does section 34A mean in practice for solicitors?

2.5.99. In specific prescribed circumstances, where a reasonable person would consider a low ML/TF risk arises, solicitors can determine themselves the extent to which they need to apply statutory CDD measures.

2.5.100. All of the following statutory circumstances must be present:

- There are no reasonable grounds to suspect ML/TF having regard to the types of customer, business relationship, service and the purpose, value or product and the source of funds – section 33(1)(c)
- There are no grounds to doubt the veracity/adequacy of identity documents – section 33 (1)(d)
- The client/AML-regulated legal service falls within a lower area of risk identified in the firm's Business Risk Assessment and the solicitor considers the instruction to present a lower degree of risk – section 34A(1)(a) and (b)
- Section 34A(2) requires that lower risk must be identified by having had regard to:

    a. matters specified in section 30A(2) of the Business Risk Assessment requirement which are
        i. information about legal sector risk in the National Risk Assessment – (see further the Business Risk Assessment Section)
        ii. guidance about risk issued by a competent authority – (see further the Business Risk Assessment Section)

b. the presence of a Schedule 3 low risk factor

- If a reasonable person, having regard to the statutory ML/TF factors which must be considered in the customer risk assessment (see further the Customer Risk Assessment Section), would determine that the relationship or transaction presents a lower degree of risk of ML or TF - Section 34A(5))

2.5.101. Section 34A(3)(a) requires solicitors who apply SCDD to keep a record of the reasons for determining SCDD could be applied and the evidence on which that determination was based. In addition, section 34A(3)(b) requires solicitors to ensure they carry out sufficient monitoring of the instruction to be able to detect unusual/suspicious indicators or ML/TF red flags.

D. ENHANCED CDD

2.5.102. In situations which, by their nature, give rise to a higher risk of money laundering or terrorist financing, all designated persons, including solicitors, are obliged to undertake enhanced client due diligence measures above and beyond normal measures.

2.5.103. As mentioned earlier, the Society recommends that, before applying enhanced measures, solicitors consider the extent to which they might unwittingly commit the substantive offence of money laundering by providing a high risk legal service requiring enhanced CDD. Solicitors should document their thought process and detail their KYC (knowledge of client) when determining whether to provide a high risk AML-regulated legal service. The exercise of 'documenting your thought process' when ML/TF red flags are present can greatly assist a solicitor in the future should an AML-regulated legal service ever be examined by an Investigating Accountant or investigated by the CAB or the FIU.

2.5.104. The extent of additional information sought, and of any monitoring carried out in respect of any particular client, will depend on the money laundering or terrorist financing risk that is assessed to be present to the solicitor or firm.

2.5.105. The legislation now prescribes four specific circumstances when enhanced due diligence measures must be applied.

1. Complex/Unusual transactions - Section 36A
2. Risk that client involved in ML/TF then ascertain PEP status - Section 37
3. Client is established or resides in a high-risk third country - Section 38A
4. Business relationship (client or AML-regulated legal service) is High Risk for ML/TF - Section 39

Enhanced CDD Duty 1 - Complex/Unusual transactions - Section 36A

2.5.106. In accordance with a firm's AML Policies, Controls and Procedures, examine the background and purpose of complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

2.5.107. In such circumstances solicitors should increase the degree and nature of monitoring of a business relationship in order to determine whether transactions appear suspicious.

Enhanced CDD Duty 2- Risk that client involved in ML/TF, ascertain PEP status - Section 37

2.5.108. This enhanced due diligence duty requires solicitors to **take steps**, which are **reasonably warranted**

by the risk of a client being involved in money laundering or terrorist financing, to determine if that client is a PEP with new measures to be applied to all PEPs.

2.5.109. Section 37 contains the amended PEP obligations.

2.5.110. Section 37(1) and (3) requires solicitors to take steps, which are reasonably warranted by the risk of a client being involved in money laundering or terrorist financing, to determine if that client is an international or domestic PEP.

2.5.111. Sections 37(1)(a) and (b) clarify that clients include customers, beneficial owners connected with the customer/service and beneficial owners of the beneficiary.

2.5.112. The timing of when a solicitor must determine whether a client is a PEP is clarified in section 37(2) as being prior to establishing the business relationship.

2.5.113.The measures to be applied to all PEPs are specified in sections 37(3) and (4):

"(3) The steps to be taken are such steps as are reasonably warranted by the risk that the customer, or beneficiary or beneficial owner (as the case may be) is involved in money laundering or terrorist financing.

(4) If a designated person knows or has reasonable grounds to believe that a customer residing in a place outside the State is, or has become, a politically exposed person or an immediate family member or close associate of a politically exposed person, the designated person shall—

(a) ensure that approval is obtained from senior management of the designated person before a business relationship is established or continued with the customer,

(b) determine the source of wealth and of funds for the following transactions—

(i) transactions the subject of any business relationship with the customer that are carried out with the customer or in respect of which a service is sought, or

(ii) any occasional transaction that the designated person carries out with, for or on behalf of the customer or that the designated person assists the customer to carry out,

and

(c) in addition to measures to be applied in accordance with section 35(3), apply enhanced monitoring of the business relationship with the customer."

Who is a PEP?

2.5.114. The legislation (section 37) requires designated persons to apply enhanced measures to PEPs that are resident outside of Ireland and, since the 2018 Act, also PEPs resident in Ireland ('domestic PEPs'). Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position makes them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put a client into a higher risk category. Under the definition of a PEP, an individual ceases to be so regarded after he has left office for one year.

2.5.115. Under section 37(10), a PEP is an individual who is or has been entrusted with prominent public functions, or an immediate family member, or a known close associate of such a person. The

definition includes persons holding a prominent position in European Union and international bodies such as the UN, World Bank or IMF. Solicitors should note the amended definition as follows:
""politically exposed person" means an individual who is, or has at any time in the preceding 12 months been, entrusted with a prominent public function, including either of the following individuals (but not including any middle ranking or more junior official):

(a) a specified official;
(b) a member of the administrative, management or supervisory body of a state-owned enterprise;
"specified official" means any of the following officials (including any such officials in an institution of the European Communities or an international body):

(a) a head of state, head of government, government minister or deputy or assistant government minister;
(b) a member of a parliament or of a similar legislative body;
(bb) a member of the governing body of a political party;
(c) 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;
(d) a member of a court of auditors or of the board of a central bank;
(e) an ambassador, chargé d'affairs or high-ranking officer in the armed forces;
(f) a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation."

2.5.116. Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, solicitors should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

2.5.117. Immediate family members include:

- Parents;
- Spouse;
- Equivalent spouse;
- Child;
- Spouse of a child;
- Equivalent spouse of a child; and
- Any other family member of a PEP.

2.5.118. Persons known to be close associates include:

- Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- Any individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a person de facto who is a PEP.

2.5.119. Having to obtain knowledge of such a relationship does not presuppose active research by the solicitor in order to obtain knowledge of such a relationship.

What do I have to do if my client is a PEP?

2.5.120. Under section 37, solicitors are required to take the following steps prior to establishing a business relationship with a PEP or carrying out a transaction:

- Have appropriate **risk-based** procedures to determine whether a client or beneficial owner residing outside or inside the State, is a PEP;
- Obtain Senior Management/MLRO approval prior to establishing a business relationship with

such a client;
- Take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- Conduct enhanced ongoing monitoring of the business relationship.

2.5.121. The steps taken by a solicitors' firm to identify a PEP's source of funds and to monitor the ongoing business relationship should be in accordance with the ECDD measures outlined below.

2.5.122. A firm's Business Risk Assessment will ascertain the nature and scope of the services provided by a particular solicitors' firm and will, therefore, generally determine whether the existence of PEPs in their client base is an issue for the firm, and whether or not the firm needs to screen all clients for this purpose in the customer risk assessment. In the context of both of these risk assessments, it would be appropriate if the firm's resources were focused in particular on transactions and/or services that are characterised by a high risk of money laundering.

2.5.123. Establishing whether individuals or legal entities qualify as PEPs is not always straightforward and can present difficulties. Where solicitors need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. If there is a need to conduct more thorough checks, or if there is a high likelihood of a solicitor having PEPs as clients, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

2.5.124. Clients may not initially meet the definition of a PEP. The solicitor should, as far as practicable, be alert to public information relating to possible changes in the status of its clients with regard to political exposure.

2.5.125. Obtaining approval from Senior Management/MLRO for establishing a business relationship does not imply obtaining approval from the partners, but from the immediately higher level of authority to the person seeking such approval. The 2018 Act provides a definition of "senior management" as an officer/employee with sufficient knowledge of the firm's ML/TF risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

2.5.126. Guidance for the legal sector in Britain suggests that for law firms, senior management for the purposes of compliance with AML legislation may be:
- the head of a practice group
- another partner who is not involved with the particular file
- the partner supervising the particular file
- the nominated officer or, if different, the officer responsible for compliance with the Regulations, and
- the managing partner.

2.5.127. In any case, it is recommended that you advise those responsible for monitoring risk assessment in your firm that a business relationship with a PEP has begun or may be about to begin, to help their overall monitoring of the practice's risk profile and compliance.

Establishing source of wealth and funds

2.5.128. Generally, this simply involves asking questions of the client about their source of wealth and the source of the funds to be used with each retainer. When you know a person is a PEP, their salary and source of wealth is often publicly available on a register of their interests. This may be relevant for higher risk retainers.

2.5.129. The question of 'determining' or evidencing source of wealth should be addressed on a risk sensitive basis. There is no 'one-size-fits-all' answer to this question; certain evidence may be sufficient in some circumstances, though insufficient in others. In cases identified as lower-risk, you should minimise the amount of information relating to source of wealth that you seek to collect directly from clients and make use of information which is readily available. When assessing what evidence will be sufficient to address this issue, solicitors should take a global view of the risk factors relevant to the situation and consideration of the client's source of wealth should be central to this assessment. Whatever actions are taken or not taken, those actions and the reasons for them should be clearly recorded. See also 'Do I need to obtain evidence or 'determine' the source of funds/wealth' earlier in this section.

2.5.130. In addition, please note that source of funds is different from source of wealth. Source of funds means where the client's funds are received from – an Irish bank account for example. Source of wealth means how the client came to have the funds in question via inheritance, house sale, or investment windfall for example. Source of wealth is fundamental to money laundering risk assessment. If you are clear about the legitimacy of a client's source of wealth, the risk of money laundering is significantly reduced.

How can PEPs be identified?

2.5.131. Solicitors are not required to conduct extensive investigations to establish whether a person is a PEP, but should have regard to information that is in their possession or publicly known.

2.5.132. To assess a firm's PEP's risk profile, you must take into account your Business Risk Assessment, the level of risk of money laundering or terrorist financing inherent in your business and the extent to which that risk would be increased by a business relationship with a PEP and the firm's existing client base, taking into account how many clients are currently known to be a PEP.

2.5.133. If the risk of a firm acquiring a PEP as a client is low, a firm may simply wish to ask clients as a matter of course whether they fall within any of the PEP categories. Where they say no, a solicitor may reasonably assume the individual is not a PEP unless anything else within the retainer, or of which a solicitor otherwise becomes aware, gives rise to a suspicion that they may be a PEP.

2.5.134. Where a firm has a higher risk of having PEPs as clients or a solicitor has reason to suspect that a person may actually be a PEP contrary to earlier information, the solicitor should consider conducting some form of electronic verification. Firms may find that a web-based search engine will be sufficient for these purposes, or may decide that it is more appropriate to conduct electronic checks through a reputable international electronic verification provider.

2.5.135. It should be noted that the range of PEPs is wide and constantly changing, so electronic verification will not give 100% certainty. Solicitors should remain alert to situations suggesting the client is a PEP. Such situations include:

- receiving funds in the retainer from a government account
- correspondence on official letterhead from the client or a related person
- general conversation with the client or person related to the retainer linking the person to a PEP
- news reports suggesting the client is a PEP or linked to one.

2.5.136. Where a solicitor suspects a client is a PEP but cannot establish that for certain, the solicitor may decide on a risk-sensitive basis to apply aspects of the enhanced due diligence procedures, as provided for in section 39 to manage and mitigate risk. A lack of clarity as to whether a person is a PEP could, in and of itself, be indicative of a heightened risk of money laundering.

Enhanced CDD Duty 3 - Client is established or resides in a high-risk third country - Section 38A

2.5.137. Solicitors must apply additional measures including enhanced monitoring to manage and mitigate the risk of money laundering and terrorist financing where a customer is established or resides in a high-risk third country.

2.5.138. Section 38A(2) and (3) provide limited exemptions and criteria.

2.5.139. Under the 2018 Act a high risk third country is defined as a country which has been identified by the European Commission under Article 9 of the 4th Directive.

2.5.140. Article 9.2 empowers the European Commission to identify 'high risk third countries' with strategic deficiencies in their national anti-money laundering and counter financing of terrorism regimes that pose significant threats to the financial system of the European Union.

Who is on the list?

2.5.141. At the time of publication (November 2018) there are 15 countries that have been identified as 'high risk third countries'. They are:

- Afghanistan
- Bosnia and Herzegovina
- Guyana
- Iraq
- Lao PDR
- Syria
- Uganda
- Vanuatu
- Yemen
- Ethiopia
- Sri Lanka
- Trinidad and Tobago
- Tunisia
- Iran
- Democratic People's Republic of Korea

2.5.142. The original list can be accessed here.

2.5.143. It has been amended by two subsequent delegated regulations which can be accessed here and here.

2.5.144. The Fifth EU Money Laundering Directive, which was published in the Official Journal on 19 June 2018, has broadened the criteria for the European Commission in assessing high risk third countries. As such, it is likely that the current list will be expanded in future.

Can a country pose a higher ML/TF Risk but not be designated as a "high-risk third country"?

2.5.145. **Even where a client is not based in one of the listed high risk third countries you should consider the individual money laundering and terrorist financing risks posed by that particular client and matter.** In determining whether it is appropriate to apply enhanced CDD you should take into account geographic risk factors, such as whether the country in which the client or transaction is based:

- has deficient anti-money laundering legislation;
- has high levels of acquisitive crime or corruption;
- is considered to be an offshore financial centre or tax havens; and/or
- permits nominee shareholders to appear on the share certificate or register of owners.

2.5.146. In addition, to effectively manage the money laundering risks that your firm faces you should:

- be aware of which jurisdictions are on the European Commission list and information about financial sanctions provided by the Central Bank;
- be alert to unexpected instructions to undertake transactions relating to one of those jurisdictions where this is outside of your normal practice;
- be alert to unexpected increases in instructions to undertake transactions relating to one of those jurisdictions or where the instructions are unusual given your understanding of normal practice in those jurisdictions;
- be alert to large asset transfers out of those jurisdictions;
- consider undertaking further due diligence checks if you are not sure who you are dealing with and ask more questions about the source of funds and purpose of the transaction; and
- have a process for checking clients against the sanctions lists where they have a connection with a jurisdiction which is on the sanctions list

2.5.147. A good rule of thumb is to always be cautious of proposed legal services which will involve the routing of funds from outside of the EU into the EU financial system via a solicitor's client account. Solicitors must question the ML/TF risk posed by allowing their client account to be used as an entry point for money into the EU financial system.

Other useful resources

2.5.148. In addition to the European Commission's list of high risk third countries, you may wish to consult the following useful resources when considering geographic money laundering risk factors:

- FATF statements on unsatisfactory money laundering controls in overseas jurisdictions
- HM Treasury and OFSI's list of financial sanctions targets by regime and consolidated list of asset freeze targets
- The International Bar Association's summary of money laundering legislation around the world
- Transparency International's corruption perception index

Enhanced CDD Duty 4 - Business relationship (client or AML-regulated legal service) is High Risk for ML/TF - Section 39

2.5.149. Solicitors must apply enhanced measures, additional to existing measures to business relationships which present a higher degree of risk including those listed in Schedule 4 and any others prescribed by the Minister. However, the Society recommends that, before applying enhanced CDD measures, solicitors must consider the risk of unwittingly committing the offence of money laundering and the potential that a report may be required. Accordingly, if high risk ML/TF circumstances arise, solicitors should first consider the dangers inherent in providing the proposed AML-regulated legal service, even with enhanced CDD measures.

2.5.150. Section 39(2) clarifies that business relationships/transactions shall be considered to present a higher degree of risk if a reasonable person, having regard to the Customer Risk Assessment, would determine high risk.

2.5.151. Where solicitors identify these high risk scenarios, then ECDD measures must be applied to manage and mitigate the risk of ML/TF if it is the case that the legal service can be provided by the firm. In these circumstances, where a solicitor considers that a client presents a higher than standard risk of money laundering or terrorist financing, and enhanced due diligence is therefore necessary, increased monitoring of the client's activities may be a more appropriate alternative, based on the solicitor's risk assessment, to further identification and verification of the client additional to those applied to normal risk clients.

2.5.152. In terms of potential types of enhanced measures which might be used to manage and mitigate higher risk, regard can be had to the enhanced measures required for PEPs described above.

High risk circumstances requiring enhanced CDD where non face-to-face clients

2.5.153. Where a client is a natural person and they are not physically present for identification purposes, you must take this into account when assessing whether there is a high risk of money laundering or terrorist financing and the extent of any EDD measures you should take.

2.5.154. A client who is not a natural person can never be physically present for identification purposes and will only ever be represented by an agent. Although the fact that you do not have face-to-face meetings with the agents of an entity or arrangement is specified as a risk factor in Schedule 4, this does not automatically mean that enhanced due diligence must be undertaken. You should consider your risk analysis, the risks associated with the retainer and the client, assess how well standard CDD measures are meeting/might meet those risks and decide whether further CDD measures are required before proceeding/continuing to proceed.

Blackhall Place
Dublin 7

T +353 1 672 4800
F +353 1 672 4801

E aml@lawsociety.ie
W www.lawsociety.ie