Anti- Money Laundering, Policy, Controls and Procedures (PCP’s)

General Comments -

* This is a template/precedent document only. It should be tailored as appropriate to suit the needs of each individual firm. (this cover page should not be included)
* All sections should be included and implemented.
* The LQSI cannot accept any responsibility for any errors or omissions contained in this template document.
* The document should be reviewed on an annual basis, or as required.

Specific Comments –

* Firms are required to complete any sections outlined in red italics and to tailor this policy to reflect each firm’s own practices.
* Firms should note that sample Law Society Business and Customer Risk Assessment Forms have been appended to this template.
* Practitioners should be aware of the Solicitor’s (Money Laundering and Terrorist Financing) Regulations 2020 as they apply to the inspection of law firms by the Law Society;
  + Replace 2016 regulations, now revoked.
  + Operative date of 1 November 2020
  + No new obligations on solicitors
  + No new powers conferred on the Law Society
* Reminder – failure to comply.
  + Requirement to take remedial action.
  + Requirement to attend a meeting of the Regulation of Practice Committee to explain failure to comply; and
  + Requirement to complete an independent AML audit
  + Referral to Legal Practitioner’s Disciplinary Tribunal
* Practitioners should be aware of the provisions of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 which strengthens the risk-based approach to AML compliance. Key changes are referenced within this document and practitioners and staff should be updated on its provisions. Training records should be updated accordingly.
* This policy was revised in February 2023 to clarify obligations in respect of Business Risk Assessments, Customer Risk Assessments and CDD.
* This policy was revised and updated in February 2024 to ensure that law firms give due consideration to sanctions when considering AML compliance and customer/business due diligence requirements. Remember that it is a criminal offence not to comply with sanctions.
* This policy was updated in March 2025 to include at Appendix 5, a form for completion in respect of identification and verification for corporate clients. Firms should ensure that a Customer Risk Assessment is first completed to identify the risk level to be assigned which will determine the level of CDD to be applied to that client.
* This policy was updated in March 2025 to note the statutory duty under the 2021 Act to confirm that information concerning the beneficial ownership of a customer is entered in the relevant registers.

The Legal Quality Standard of Ireland

Updated March 2025

INDEX

**Contents**

[Anti-Money Laundering Policy, Controls & Procedures 3](#_Toc128567978)

[AML-regulated legal services 4](#_Toc128567979)

[Business Risk Assessment 5](#_Toc128567980)

[Customer Risk Assessment 5](#_Toc128567981)

[Customer Due Diligence Procedures (CDD) 7](#_Toc128567982)

Identification and verification………………………………………………………………………………….10

[Reporting of ML/TF Suspicions 12](#_Toc128567984)

[MLRO/Compliance Officer Responsibilities 13](#_Toc128567985)

[AML Record Keeping 14](#_Toc128567986)

[Reliance 14](#_Toc128567987)

[Staff Training 15](#_Toc128567988)

[Examples of ML/TF Red Flags 16](#_Toc128567989)

APPENDICES

1. Business Risk Assessment
2. Customer Risk Assessment/Document Your thought process forms
3. Low risk factors
4. High risk factors
5. Identification and Verification – Documents Required for Corporate Entities

[FIRM NAME]

Section 1

# Anti-Money Laundering Policy, Controls & Procedures

*(Insert firm name)* takes a zero-tolerance approach to being involved in illegal/illicit activity and will fully comply with all relevant sections of the Criminal Justice (Money Laundering and Terrorist Offences) Act 2010 (‘the 2010 Act’), the Criminal Justice (Money Laundering and Terrorist Offences) (Amendment) Act 2018, the Solicitor’s (Money Laundering and Terrorist Financing) Regulations 2020) and the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 (“the 2021 Act”).

It is important that *all* staff are aware of the serious consequences of failure to comply with statutory AML duties when the firm provides an AML-regulated legal service. It is a crime not to comply with statutory AML duties. It is equally important for all staff to ensure that they do not unwittingly commit the offence of money laundering by not being alert to money laundering red flags.

Statutory requirements under the legislation (2018 Act) include: -

1. Business Risk Assessments
2. Policies, Controls and Procedures (PCPs)
3. Customer Risk Assessments to determine the extent of Customer Due Diligence (‘CDD’) measures.
4. CDD measures
5. Reporting of suspicious transactions to the Gardai and the Revenue Commissioners.
6. Maintain records in respect of client identity and of all relevant transactions.
7. Ensure staff training and awareness.

Customer, or Client, Due Diligence is the process whereby information is obtained on the client and on the nature of the intended business relationship between the designated person and the client.

Subject to the specific provisions in the 2018 Act, the level of due diligence required is determined using a ‘risk-based approach’ so that the measure employed to mitigate money laundering and terrorist activity is commensurate with the risk of such activity. The 2021 Act strengthens this risk-based approach to AML compliance.

In general Customer Due Diligence should be carried out prior to the establishment of the business relationship.

It is the policy of this firm to ensure that the correct level of due diligence checks have been applied to the client and any beneficial owners. We also carry out checks to verify the source of funds and complete the appropriate records following our agreed procedures, our statutory obligations, Law Society guidelines and specific training on the subject.

In order to ensure that the regulations are fully implemented by the firm*, [NAME e.g., principal/partner or office manager]* has been appointed the firm’s Money Laundering Reporting Officer (“MLRO”). The MLRO will maintain and have full responsibility for the practice money laundering identification file upon which all client identification records will be kept. There is annexed to this policy a copy of the Law Society’s 2010 guidance notes entitled “Guidance Notes for Solicitors on Anti-Money Laundering Obligations”. There is further annexed to this policy the Law Society’s 2018 AML Guidance, this guidance being supplemental to the 2010 guidance notes.

All staff members are obliged to familiarise themselves with the guidance notes. A copy of this policy and the notes should be kept at each fee earners desk.

What is money laundering?

Money laundering is the process by which the proceeds of crime (which could be money or an equivalent benefit or asset) and/or the true ownership of those criminal proceeds are disguised so that they appear to come from a legitimate source.

Chapter 9 of the 2010 Law Society Guidance Notes (pages 66-71), as attached, note a non-exhaustive list of potentially suspicious circumstances which may give rise to a suspicion of money laundering. Each staff member is required to review this chapter and familiarise themselves with it.

Section 2

# AML-regulated legal services

The AML obligations outlined above 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), 2018 Act as a solicitor who carries out any of the following services:

1. the provision of assistance in the planning or execution of transactions for clients concerning any of the following:
2. Buying and selling real property or business entities.
3. Managing money or other assets.
4. Opening or management of banks, savings or security accounts.
5. Organisation of contributions necessary for the creation, operation or management of a company.
6. Creation, operation or management of a trust company or similar corporate structures.
7. Acting in any financial or real-estate transaction for the client.

Legal activities falling outside those categories are therefore *exempt* from AML CDD.

The Law Society advises that firms should verify the identity of all clients to follow the Society’s best practice guidance. Even where solicitors provide legal services that are not regulated for AML purposes, it is the Society’s best practice guidance that solicitors should verify the identity of *every* client.

Section 3

# Business Risk Assessment

Section 54(3)(k) requires firms to detail internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date.

The Law Society advises that in light of the Covid -19 pandemic, it may be beneficial to consider the impact of the pandemic across all legal services and firms should take this into account when drafting a Business Risk Assessment.

<https://www.lawsociety.ie/globalassets/documents/members/aml/covid-19-aml.pdf>

Requirement under the Act

The Act requires the firm to carry out an assessment to identify and assess the risks of money laundering and terrorist financing involved in carrying on the firm's business, having regard to at least the following risk factors:

(a) the type of clients that the firm has. \*

(b) the products and services that the firm provides.

(c) the countries or geographical areas in which the firm operates.\*

(d) the type of transactions that the firm carries out.

(e) the delivery channels that the firm uses.

(f) any information in the national risk assessment which is of relevance to the firm; and

(g) the guidance issued by the Law Society.

\*Fee earners must consider statutory low and high- risk factors including customer and country/geographical risk which includes consideration of sanctions. Consider whether jurisdictions in which our clients (or the beneficial owners of our clients) are based (or from which they operate their businesses) may be the subject of sanctions.

Sanctions

Sanctions have been a key tool in the fight against terrorism for many years. The competent authorities for sanctions in Ireland are the Central Bank, the Department of Jobs, Enterprise and Innovation and the Department of Foreign Affairs. These organisations constantly update their websites with information about sanctions as they are enacted together with information about how everyone can comply.

The key websites are set out below:

* Central Bank

<https://www.centralbank.ie/regulation/how-we-regulate/international-financial-sanctions>

* Department of Enterprise, Trade and Employment

<https://enterprise.gov.ie/en/What-We-Do/Trade-Investment/Export-Licences/Sanctions>

* Department of Foreign Affairs

<https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures>

Fee earners should be aware of which jurisdictions are on the European Commission list and information about financial sanctions provided by the Central Bank.

Fee earners should check clients against the sanctions lists where they have a connection with a jurisdiction which is on the sanctions list.

Of particular importance in recent years are the sanctions imposed across the EU on Russia and Belarus following the invasion of Ukraine.

All fee earners should familiarise themselves with the Law Society recommended approach to ensuring compliance with sanctions on Russia and Belarus over Ukraine by following the five steps outlined below;

1. Learn more about the scope and impact of sanctions
2. Consider whether legal services or payments have been, or about to be provided to clients or third parties from or connected to Russia/Belarus. Document the outcome.
3. If our firm may be exposed to Russia/Belarus, check sanctions lists, identify relevant law and ensure you comply if any hits are found. Document the steps taken.
4. Ensure all relevant staff are aware of and fully understand their obligations in respect of the sanctions regime.
5. Keep up to date as new sanctions emerge.

To access the in-depth Law Society guidance, follow the link below.

<https://www.lawsociety.ie/Solicitors/rules-legislation/sanctions>

Information about legal sector ML/TF Risk

The firm has considered the National Risk Assessment (NRA) and the Law Society guidance on the Act. The National Risk Assessment (NRA) of Money Laundering and Terrorist Financing 2019 assessed the ML/TF threats in Ireland and the vulnerabilities of certain sectors to ML/TF. The overall ML/TF risk in the legal services sector was judged to be medium-high under the NRA. The NRA states that while awareness of and compliance with AML/CFT obligations has improved across the legal services sector, the nature of services provided by legal professionals, the scale and variety of their sector and the low level of STR reporting all tend to increase the overall money laundering risk.

The Business Risk Assessment prepared by the firm identifies and records the money laundering risks faced by the various areas of our business, the clients/countries we serve, the services we deliver and the transactions we carry out.

Section 4

# Customer Risk Assessment

Section 54(3)(a) requires the firm to have policies, controls, and procedures (PCPs) relating to “identification, assessment, mitigation and management” of ML/TF risk factors.

In addition, section 54(3)(d) requires the firm to enable 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.”

Section 54(3) requires the firm to include measures to be taken “to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity.”

How is a Customer Risk Assessment carried out?

All new clients must undergo a risk assessment which should be carried out before the client is accepted. All existing clients, the subject of a customer risk assessment carried out within the last three years, should undergo a review of the risk assessment when a new matter is accepted, during a transaction where required, or when there is a significant change in circumstances for the client, e.g., a change in ownership structure, movement of principal place of business to another jurisdiction etc. If an existing client has not previously been subject to a customer risk assessment, that client should be treated as a new client.

All clients must have a risk categorisation applied. The risk categories which must be applied by the firm are Low Risk, Standard Risk and High Risk. The risk category applied to the client will determine the level of CDD to be applied to that client.

Low Risk Clients

Schedule 3 to the CJA sets out a non-exhaustive list of indicators that a client may be low risk (see Appendix 3).

The following clients may potentially be assessed as low risk:

* A credit or financial institution that carries on business in the State, or another EU Member State, or in a place which is not a high-risk country, supervised or monitored for compliance with equivalent requirements.
* A company listed on a Regulated Market (e.g., the Irish Stock Exchange Official List).
* Public bodies in the State which are subject to the Freedom of Information Act e.g., HIQUA, Pensions Board, certain hospitals, government departments, local authorities, health boards.

High Risk Clients

Schedule 4 to the CJA sets out a non-exhaustive list of indicators that a client may be high risk.

The following clients may potentially be assessed as high risk:

* Non-face-to-face natural person clients.
* All clients subject to UN or EU financial sanctions. – see section on Sanctions above
* All Politically Exposed Person clients (PEPs).
* Clients whose beneficial owner(s) are PEPs.
* All High-Risk Country Affected Clients.
* All clients involved in High-Risk industries.
* High Risk Industry Affected Persons.
* All clients requiring High Risk Services.

A list of potentially high-risk clients is set out at Appendix 4.

Standard Risk Clients

All clients that do not fall into the category of Low or High Risk, should be categorised as Standard Risk.

The Law Society has developed two sample Customer Risk Assessment Forms to assist solicitors. A “Risk Factor Questionnaire” and a “Document your thought Process Form”. These forms are attached at Appendix 2 and should be completed for both new and existing clients and stored on the file, either in hard or soft copy in order to state the risk level the fee earner attributed to the file.

Section 5

# Customer Due Diligence Procedures (CDD)

Section 54(3)(b) requires details of the firm’s CDD measures.

The outcome of the Customer Risk Assessment will inform the type and extend of CDD applied.

* STANDARD

Typically, most of the firms’ clients will require standard CDD.

The standard 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 – so that the firm knows who the beneficial owner(s) is.

A “beneficial owner” is defined as the individual(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. A shareholding of 25% plus one share or an ownership interest of more than 25% in the entity held by an individual is an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25% in the entity held by a corporate entity, which is under the control of an individual(s) is an indication of direct ownership. (The European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016 (the “2016 Regulations”)

1. Obtaining information reasonably warranted by the risk of ML/TF on the purpose and

intended nature of the business relationship. In most cases, this will be self-evident from a

discussion with the client.

In relation to 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 wealth/funds. All that is required is that the information being provided about source of funds/wealth is consistent with the solicitors CRA and there are no potential red flags (e.g., funding from third parties). The Law Society guidance is that you should consider whether the source of funds is consistent with the risk profile of the client, the retainer and the business. However, it may be prudent to ask for some supporting evidence possibly in the form of bank statements, recently filed business accounts or documents confirming the source, such as sale of a house, sale of shares, receipt of a personal injuries award, a bequest under an estate or a win from gambling activities.

1. Conducting ongoing monitoring of the business relationship.

* SIMPLIFIED

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 based on specific statutory criteria.

This means that the identity of the client does not have to be fully verified, information on the purpose or intended nature of the business relationship does not have to be obtained and, where relevant, details on the beneficial ownership of the client do not have to be obtained. However, checks must be carried out to ensure that the client is in fact a Low Risk Client and qualifies for simplified due diligence. The solicitor must obtain sufficient information about the client to satisfy itself that the client meets the statutory criteria for SCDD to be applied.

* ENHANCED

Enhanced due diligence applies to all High-Risk clients.

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

1. Complex/unusual transactions
2. Risk that client is involved in ML/TF, ascertain PEP status
3. Client is established or resides in a high-risk third country.
4. Business relationship (client or AML-regulated legal service) is high risk for ML/TF

In addition to the standard due diligence requirements as outlined above, further information, documents and monitoring are required to satisfy the enhanced due diligence requirements. The extent of the additional information and any monitoring carried out on the client will depend on the outcome of the risk assessment process that has been carried out.

MLRO approval must be sought and obtained before commencing a business relationship with a High-Risk client.

Information on the financial background of the client/beneficial owner(s) must be obtained for all High-Risk clients.

PEPs

The legislation requires the firm to apply enhanced measures to PEPs, both domestic and non-domestic.

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. Examples of PEPs include Heads of State, Heads of Government, Ministers and Deputy Ministers, TDs, Members of Parliament or similar legislative body, members of a governing body of a political party, members of high-level judicial bodies, members of courts of auditors, members of boards of central banks, members of management, administrative or supervisory bodies of state-owned enterprises and persons holding a prominent position in European Union and international bodies such as the UN, World Bank, IMF.

Immediate family members include;

* Parents
* Spouse
* Equivalent spouse
* Child
* Spouse of a child
* Equivalent spouse of a child
* Any other family member of a PEP

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

Identifying a PEP

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 is publicly known.

The following are some indicators of the possibility that a client is a PEP;

* Funds received from a government account
* Correspondence originating from a government source with corresponding email account or letterhead
* General conversations/media reports/ discussion with the client indicating this

Steps to take if a client is a PEP

* Ensure that MLRO approval is obtained in advance of onboarding the client
* Take measures to establish the source of wealth and source of funds for the client – source of funds is different from source of wealth. Source of funds means where the clients funds are sourced from. Source of wealth means how the client came to have the funds in question.
* Conduct ongoing monitoring of the business relationship

Section 6

# Identification and verification procedures

Evidence of personal identity can be by:

* Current valid passport or driving licence (Irish or International)
* Current National Identity Card
* Current identification with photo signed by a member of the Gardai.
* Social Welfare Card with photo ID
* National Age Card
* EU member state identity card
* Current photocard driving license.

Address

Documentary evidence of address can be:

* Current documentation issued by the Revenue Commissioners showing the name of the person and their PPS number.
* Current documentation issued by the Department of Social Protection showing the name of the person and their PPS number.
* Instrument of a court appointment (such as a liquidator or a grant of probate)
* Current Local Authority document (including those printed from the internet)
* Medical card for over 18s with intellectual disability
* Confirmation from electoral register
* Recent utility bill/bank statement/ mortgage statement with current address
* Recent Tax notices from the Revenue

In cases where the above could not be reasonably expected, the following would suffice:

* Examination of the electoral register (including online version):
* Examination of a local telephone directory or available street directory:
* Confirmation of identity by a local employer; and
* Garda Siochana Community Age card

Documents that are received directly from the client, where the originals cannot be viewed by a fee earner, should be certified copies of originals.

Individual clients:

* Certified copy photographic ID
* Certified copy non-photographic ID

Corporate Entities:

In relation to incorporated entities, the firm should obtain the following information:

* Full name
* Registered number
* Registered office address in country of incorporation; and

And in addition, for private companies and unlisted companies –

* A full list of names of the directors
* The names of beneficial owners with greater than 25% of the shares or voting rights or who otherwise exercise control
* Verify the identity of at least one director and at least one of those authorised to act on behalf of the corporate entity

Partnerships:

* Full legal name and proof of existence
* Partnership Deed Agreement or equivalent
* List of Partners
* List of Beneficial Owners
* Verify the identity of at least one Partner and at least one of those authorised to act on behalf of the Partnership
* Verify that any person acting on behalf of the Partnership is so authorised

Solicitors are referred to Chapter 6 of the Law Society Guidance Notes on the 2010 Act pgs 40-50 for further guidance in relation to identification and verification methods in respect of pension schemes, other trusts, foundations and similar entities, clubs and societies, public sector bodies, governments, state-owned companies and supranationals.

See Appendix 5 for corporate identification checklist.

Identifying beneficial owners

The procedures above should be adopted for the purposes of identifying any beneficial owners who are not the client. These may be persons who have at least a 25% shareholding in an unlisted company; or have at least a 25% interest in a partnership; or have at least a 25% interest of trust property and/or relevant classes of trust beneficiaries; and/or anyone who has management control of such an entity.

Under section 35(3A) and 35(3C) of the Criminal Justice (Money Laundering and Terrorist Financing)(Amendment) Act 2021, solicitors are required “prior to the establishment of a business relationship with a customer” to “ascertain that information concerning the beneficial ownership of the customer is entered” on the relevant central register.

The people requiring to be identified should visit the office with the relevant documentation so that copies can be taken.(See note below on alternative methods to verify client identity)

If it is not possible for these parties to call to the office, alternative arrangements will need to be made to enable us to comply with the legislation. This may involve reliance upon a third party who should verify and

Certify a copy of the passports/driving license. Such certification should be by: -

* A solicitor
* A notary public
* Garda officer
* Embassy/Consulate staff
* Senior bank official

The adoption of alternative methods to verify client identity to keep pace with technological developments adopted during the Covid-19 pandemic is outlined in detail by the Law Society and include video conferencing and the use of encrypted email.

<https://www.lawsociety.ie/globalassets/documents/members/aml/covid-19-aml.pdf>

In addition to the long-standing duty on solicitors to identify beneficial owners and take measures reasonably warranted by the ML/TF risk to verify their identity, sections 35(3A) and 35(3C) of the 2021 Act, require solicitors, “prior to the establishment of a business relationship with a customer”, to “ascertain that information concerning the beneficial ownership of the customer is entered” on the relevant central register.

Clients who are entities subject to beneficial ownership registration requirements have a duty to (1) maintain their own internal registers of beneficial owners and (2) ensure those beneficial owners are also notified to central registers. Ultimately, the requirement to gather and register beneficial ownership information rests with the entity (the trust or the company) to whom a solicitor provides legal services. ~~By late 2021, registers will have been established for companies, certain financial vehicles, and relevant trusts.~~

In addition, the relevant statutory instruments impose duties on designated persons to report any non-compliance or discrepancy they find between information in the relevant central register and information that comes to their knowledge from other sources when carrying out customer due diligence on an entity, or otherwise. The duty is to report discrepancies to the relevant Registrar.

If a client identifies a Senior Managing Official (SMO) as the beneficial owner of an entity, a new duty under the 2021 Act requires that the SMO’s identity be verified. Regulation 2 of SI 110 of 2019 defines a "senior managing official" as including a director and a chief executive officer.

Section 7

# Reporting of ML/TF Suspicions

All partners and staff have a personal statutory legal obligation to make a Suspicious Transaction Report to FIU Ireland and the Revenue Commissioners where they know, suspect or have reasonable grounds to suspect, on the basis of information obtained in the course of carrying on business as a Designated Person, that another person has been or is engaged in an offence of money laundering or terrorist financing. Failure to report a suspicious transaction is a criminal offence.

In the event of such a suspicion arising, the matter must be immediately reported to the firms’ MLRO, and the appropriate form should be completed.

*(Sample internal reporting form is annexed to the 2018 Law Society Guidelines.)*

From June 2017, STRs submitted to the Garda Siochana Financial Intelligence Unit (FIU) must be made via goAML which requires designated persons to submit STRs electronically. Prior to being able to submit an STR via goAML, the firm must register on the goAML website.

The firms MLRO is responsible for:

* Scrutiny of unusual transactions highlighted by staff
* Deciding if a client can be taken on where there is a high risk of money laundering
* Reviewing suspicions from employees and deciding whether a report must be made

The MLRO shall ensure that comprehensive records of suspicions and reports are kept. These records may be necessary in the future in potential criminal proceedings and must be securely maintained due to their sensitivity/confidentiality. Such records should 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 Gardai/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

Exception

There is an exception to the reporting obligation. It does not require the disclosure of information that is subject to Legal Professional Privilege (LPP)

Tipping Off

It is an offence where a member of staff, knowing or suspecting that a report has been made to FIU Ireland and the Revenue, makes a disclosure likely to prejudice any investigation arising from the making of a report into whether a money laundering or terrorist financing offence has been committed. For this reason, where an STR has been filed, staff should not alert or otherwise disclose or allow a client to become aware of such an STR.

Section 8

# MLRO/Compliance Officer Responsibilities

* *The MLRO and/or Compliance Officer of the Firm is/are……*
* In addition to dealing with reports of ML/TF suspicions, they are responsible for….
* Ensuring all staff are trained to a level appropriate to their role
* Reviewing the firm’s Business Risk Assessment and this AML policy, controls and procedures.

The MLRO will ensure ongoing monitoring and managing of compliance with and the internal communication of the firms’ AML policies, controls, and procedures. Policies will be reviewed on at least an annual basis. Written records of any changes will be made following such a review.

The MLRO will also maintain a written record of any steps taken to communicate AML the firm’s policies, controls, and procedures (and any changes) to staff.

Monitoring compliance will assist in assessing whether the policies, controls, and procedures that the firm has implemented are effective in identifying and preventing money laundering and terrorist financing opportunities.

Paragraph 10.9 of the Society’s 2010 Guidance suggests that a review for the purposes of monitoring effectiveness should 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

1. Reports to be provided to senior management/MLRO on compliance
2. How to rectify lack of compliance, when identified
3. How lessons learnt will be communicated back to staff and fed back into the risk profile of the practice

In that regard, the firm shall ensure that AML checks are carried out during the peer file review procedures audit. The firms file review form includes a check on compliance with AML procedures. The MLRO shall review the file review forms on a quarterly basis to ensure documented AML compliance procedures are adhered to.

**Section 9:**

# AML Record Keeping

Section 54(3)(h) requires the firm to address record keeping.

The firm uses [insert case management system] to onboard new clients and matters.

*Firm to outline how records of AML documents relating to each client and matter are saved. Include reference to completion of file opening forms in hard/soft copy and customer risk assessments.*

*The following records are maintained by the firm.*

* *AML Policies, Procedures, Manuals*
* *Risk Assessments – Business Risk Assessment and Client Risk Assessments*
* *CDD/KYC material*
* *Evidence of staff training*
* *Suspicious Activity Reports* and notes and correspondence relating to internal decision making

AML records must be kept for a minimum of 5 years (and no longer) after the relationship has ended or the transaction has been concluded.

See Chapter 11, 2010 Guidance and ‘Reliance and record keeping’ in Section 3 of 2018 Guidance.

Section 10:

# Reliance

In certain circumstances, the firm may rely on “relevant third parties” to complete part of our CDD requirements. However, it should be noted that responsibility for meeting CDD obligations still rests with the firm as the designated person.

An example of where we may rely on a Relevant Third Party is where we enter into a business relationship with a client through a third party who is acting as an intermediary for the client, e.g. a law firm in another jurisdiction.

A relevant third party is defined as

1. A person, carrying on business as a designated person in the State-
2. That is a credit institution
3. That is a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides foreign exchange, or money transmission, services)
4. Who is an external accountant or auditor and a member of a designated body
5. Who is a tax adviser and is a member of a designated accountancy body, the Irish Taxation Institute or the Law Society of Ireland
6. Who is a relevant independent legal professional
7. Who is a trust or company service provider, and who is also a member of a designate accountancy body or of the Law Society of Ireland or authorised to carry on business by the Central Bank and Financial Services Authority of Ireland, or
8. A person carrying on business in another EU Member State where supervised and monitored for compliance with the 4th Money Laundering Directive and is
9. A credit institution authorised to operate as a credit institution under the laws of the Member State
10. A financial institution (other than an undertaking that is a financial institution solely because the undertaking provides foreign exchange, or money transmission, services) and authorised to operate as a financial institution under the laws of the Member State , or
11. An external accountant, auditor, tax adviser or legal professional , trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the other Member State

(c ) A person who carries on business in a place designated under Section 31 of the 2010 Act , is supervised or monitored in the place for compliance with requirements equivalent to those specified in the 4th Money Laundering Directive, and is

1. A credit institution authorised to operate as a credit institution under the laws of the place
2. A financial institution (other than an undertaking that is a financial institution solely because the undertaking provides foreign exchange, or money transmission, services) and authorised to operate as a financial institution under the laws of the place , or
3. An external accountant, auditor, tax adviser or legal professional , trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the place

Section 11

# Staff Training

* All staff members have been provided with the Law Society Guidance (2010 and 2018) to read.
* *The following training has been provided to staff members as follows.*

*(Firm to provide details of CPD hours, seminars/courses attended and any other relevant training –* ***the firm must keep records of all AML training****)*

* *The firms’ MLRO has been provided with the following training:*

*(Firm to provide details)*

* + *Which staff require what training (specific to role).*
  + *What form the training will take?*
  + *How often training should take place?*
  + *How staff will be kept up-to-date or emerging risk factors/new developments for the firm*
* *Firm to detail any other relevant training provided:*

Section 12

# Examples of ML/TF Red Flags

STAFF SHOULD NOTE THAT THIS LIST IS NON-EXHAUSTIVE

Chapter 9 of the Society’s 2010 Guidance Notes details non-exhaustive red flags/indicators of suspicion.

Highlights include:

* Activities which have no apparent purpose, make no obvious economic sense, involve unusual losses, are unnecessarily complex, involve non-resident accounts, companies or structures, activities are without reasonable explanation/out of the ordinary range of services/inconsistent with client (paragraph 9.5)
* Excessively obstructive/secretive clients, clients who insist transactions be done inordinately quickly, use aliases, recent new relationships with financial entities, legal fees paid by third parties or in cash, avoids providing identification for group of companies by offering agent identification only (paragraph 9.6(a))
* Transactions involving areas outside of Ireland/no apparent ties to Ireland/crosses many international lines/involves wire transfers/foreign currency exchanges with locations of concern/known to facilitate money laundering/secretive banking and corporate law/illicit drug production/no effective AML system (paragraph 9.6(f))
* Property transactions where client arrives at a closing with a significant amount of cash/property purchased in the name of nominees (associates/relatives)/requests for name not to be connected with property/requests for different names to be used on different documents/last minute name substitutions/property below market value with an additional “under the table” payment/deposits paid by a third party/cash deposits/unusual source or offshore bank deposit/corporate veil purchases when inconsistent with ordinary business practice of client/property purchases without inspecting property/multiple property purchases in short time period with few concerns about location, condition/rent paid or amount of a lease in advance using a large amount of cash (paragraph 9.6(h)
* Cash (large payments in actual cash/lodged to accounts) (paragraph 9.14 to 9.16)

In addition, the Guidance Notes highlight potential issues with companies and non-face-to-face transactions as follows:

* “It is … generally recognised that the use of companies, even when fronted by legitimate trading companies, are the most likely vehicles for large scale money laundering” (paragraph 6.21)
* “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” (paragraph 6.20)

Signed:

Date:

Date of next review:

APPENDIX 1

Business Risk Assessment – Law Society of Ireland Sample Form – Version 1

Instructions

* The Law Society has developed this sample Business Risk Assessment to assist solicitors in complying with their section 30A obligation to carry out a business risk assessment.
* This sample must be adapted by firms to suits their firm’s individual needs. No two Business Risk Assessments will be the same.
* See **Section 2 – 2018 Guidance** for comprehensive information about what section 30A requires.
* The statutory requirement to complete a Business Risk Assessment only applies to the AML-regulated legal services provided by solicitors’ firms. However, solicitors’ firms may wish to risk assess and develop PCPs to mitigate the ML/TF risk of sham/fraudulent litigation or debt collection.
* The factors outlined within this sample can be considered when assessing the inherent ML/TF risk to which your firm is exposed. Inherent ML Risk is not the same as actual ML risk and is the risk inherent in your business before any mitigating factors or controls (policies, training, CDD etc.) are deployed. This document should be completed on that basis – i.e., do not note any controls your firm deploys to mitigate its ML/TF risk in this document. Instead document your robust AML controls tailored to suit your firm’s inherent ML/TF risks in your PCPs (sample provided separately).
* The factors outlined below are non-exhaustive– there may be other important risk factors which should be considered, dependent upon the size and nature of your firm.
* Business risk assessments must be reviewed and kept up to date in tandem with PCPs.
* **Colour key:**
* Text in black can be used in your firm’s Business Risk Assessment.
* **Text in red can be adapted and developed by firms to suit their specific compliance needs.**

FIRM NAME: MLRO NAME:

VERSION CONTROL:

|  |  |  |
| --- | --- | --- |
| Date | Change | Name of person reviewed by |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **General Overview of Firm & Legal Sector ML/TF Risk** | | |
| General Overview of Firm | Include a general paragraph regarding the overall size and nature of your firm and provide information about the following.   * No. of partners/staff * Is there a high staff turnover at the firm? * Type of Firm – E.g., Niche corporate firm, specialist services, full-service, high-volume conveyancing firm * Types of Work undertaken – regulated/non-regulated? Mostly Property? Litigation? Probate? Wills? * Type of clients * Geographical location of the firm – rural, urban, ~~high levels of crime~~? * International element to your business? * Any other ML/TF risks specific to your firm? | |
| Credible sources of information about legal sector ML/TF risk | Section 30A requires that regard is had to specific sources of information about risk factors particular to the legal sector. These are currently detailed in ‘Step 1 – Develop your knowledge of ML/TF risks inherent in legal services’ Section 2 – 2018 Guidance.  Include here:   * a list of the sources of information about legal sector ML/TF risk (and update should new risks emerge) * in general terms, your firm’s exposure to legal sector ML/TF risk set out in credible sources of information.   You can provide detail below about specific inherent ML/TF risk factors to which your firm is exposed. | |
| **Specific Inherent ML/TF Risk Factors** | | |
| Customer Risk Factors | | Information about the firm’s assessment of ML risk inherent in its customer base.  Include here a note of your assessment of Customer Risk Factors. Ensure you reach an overall conclusion e.g., does your customer base pose a high, medium, or lower inherent ML risk? Depending on your firm’s size and business, you may be able to categorise types of customers into varying categories of risk to be mitigated differently in your PCPs.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * Do you provide your clients/customer with AML-regulated legal services? * High turnover of clients (higher risk) or a stable existing client base? (Lower risk) * High proportion of one-off clients/deals? (Higher risk) * Do you know your clients personally? If not, what additional steps do you take to mitigate the risks that this poses? * Mostly face-to-face or non- face-to-face contact with clients? (non-face-to-face = higher risk) * Act for clients across both criminal and civil matters? (Higher risk) * Does the firm have clients who are eligible for simplified due diligence, such as public authorities? (Lower risk) * Does the firm have a significant number of non-EU-based clients (where AML regulation may not be as tight) or any high-risk third countries? (Higher risk) * Does the firm have clients who run high cash turnover businesses or high value goods businesses, or operate in higher risk sectors? (Higher risk) * Does the firm undertake work for corporate clients who have complex or multiple layers of ownership, or have links to international/offshore jurisdictions? (Higher risk) * What is the source of clients – referrals, walk-in or from internet advertisements? |
| Product/Service Risk Factors | | Information about the firm’s assessment of ML risk inherent in the products/services it provides.  Include here a note of your assessment of Product/Service Risk Factors. Ensure you reach an overall conclusion e.g., do the products or services your firm provides pose a higher, medium, or lower inherent ML risk? Depending on your firm’s size and business, you may be able to categorise types of products/services into varying categories of risk to be mitigated differently in your PCPs.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * Consider whether any services you provide are attractive to money launderers such as: * the sale or purchase of real property * creation of trusts\*, companies\* and charities * management of trusts\* and companies\* * sham litigation (e.g., fraudulent debt collection/invoices) * Consider whether the services you offer could expose your client account to abuse or misuse? * Does the firm offer any services which may attract a higher level of risk such as large volume/high value conveyancing, tax mitigation strategies, work involving offshore jurisdictions or the creation and/or management of specialist entities? (Higher risk) * Does the firm receive requests to provide services outside of the EU as part of its usual area of coverage (higher risk)? * Does the firm undertake work which may be of lower AML risk (executry/wills)? * Does the firm provide non-AML-regulated legal services, criminal defence, or litigation for example (lower risk)? |
| Countries/  Geographical Risk Factors | | Information about the firm’s assessment of ML risk inherent in its areas of practice/customer base.  Include here a note of your assessment of Geographical Risk Factors. Ensure you reach an overall conclusion e.g., do geographical risk factors present a higher, medium, or lower inherent ML risk? Depending on your firm’s size and business, you may be able to categorise clients/AML-regulated legal services into varying categories of geographical risk to be mitigated differently in your PCPs.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * Could the jurisdictions in which your clients (or the beneficial owners of your clients) are based (or from which they operate their businesses): * have deficient anti-money laundering legislation, systems and practice * have high levels of acquisitive crime or higher levels of corruption * be situated in ‘offshore financial centres or tax havens * be subject to sanctions. * Does the firm provide AML-regulated legal services with non-EU aspects (because AML regulation may not be as tight) or with a nexus to any high-risk third countries? (Higher risk) * Does the firm receive funds in from non-EU countries (where AML regulation may not be so tight) (higher risk) or from any high-risk third countries? (Higher risk) * Does the firm have a specific client-base, niche or undertake work for clients from outside the EU (where AML regulation may not be so tight) (or from any high-risk third countries? (Higher risk) |
| Transaction Type Risk Factors | | Information about the firm’s assessment of ML risk inherent in the transaction connected to the legal services it provides.  Include here a note of your assessment of Transaction Type Risk Factors. Ensure you reach an overall conclusion e.g., do transaction type risk factors present a higher, medium, or lower inherent ML risk? Depending on your firm’s size and business, you may be able to categorise clients/AML-regulated legal services into varying categories of transaction type risk to be mitigated differently in your PCPs.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * How frequently do you carry out higher risk transactions? Are there any features in transactions delivered by the firm which may represent higher risk? * 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. * Is the firm regularly involved in transactions which are undertaken at short notice, within short timescales, quick turnaround, or high volumes? (Higher risk) * Is the firm involved in more complex work involving trust or other legal entity company formation, management, or service provision? (Higher risk) * Is the firm involved in more complex, high value property transactions? (Higher risk) * Does the firm undertake work for clients where the source of funds or the parties to the transaction frequently change? (Higher risk) * Does the firm undertake transactions which are longer term in nature, or where funds are locked in for substantial periods of time (lower risk)? * Does the firm undertake transactions which are publicly funded? (Lower risk) |
| Delivery Channel Risk Factors | | Information about the firm’s assessment of ML risk inherent in the delivery channels through which it provides legal services.  The way legal services are delivered can enhance or reduce ML/TF risk.  Include here a note of your assessment of Delivery Channel Risk Factors. Ensure you reach an overall conclusion e.g., do delivery channel risk factors present a higher, medium, or lower inherent ML risk? Depending on your firm’s size and business, you may be able to categorise clients/AML-regulated legal services into varying categories of delivery channel risk to be mitigated differently in your PCPs.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * Do you provide services to clients you have not met face-to-face? (Higher risk) * Does the firm conduct a large percentage of its business on a non-face-to-face basis? (Higher risk) * Does the firm always meet all clients face-to-face? (Lower risk) * Does the firm always meet/have a relationship with the underlying client? (Lower risk) * Does the firm undertake work which is conducted through intermediaries or other third parties? (Higher risk) |
| Overall Conclusion | | Include here a note of your overall conclusion.  A (non-exhaustive) list of questions to ask yourself in completing this section:   * A note of the firm’s responses to risk factors, what is the overall conclusion/summary regarding the inherent ML/TF risk applicable to the firm? * Does the nature, scale and complexity of the AML-regulated legal services provided by the firm put it at a higher, medium, or lower risk of being used for the purposes of money laundering? Why? |

**\***In relation to trusts and company services, the Society's regulatory obligations do not extend to bodies corporate providing trust and company services where such bodies corporate are owned and controlled by solicitors.  A separate requirement exists for trust and company service providers to register with the relevant competent authority for trust and company service providers, namely the Department of Justice and Equality’s Anti-Money Laundering Compliance Unit.  Further information is available at [www.antimoneylaundering.gov.ie](http://www.antimoneylaundering.gov.ie). See further [MOU with the Department of Justice and Equality on TCSPs](http://www.antimoneylaundering.gov.ie/en/AMLCU/AMLCU-MOU%20with%20Law%20Society.pdf/Files/AMLCU-MOU%20with%20Law%20Society.pdf).

*The Society accepts no responsibility for any compliance failures or loss incurred as a result of reliance on this sample adaptable Business Risk Assessment. Solicitors’ firms must always ensure they are in compliance with all of their statutory AML obligations. The Law Society is grateful to the Law Society of Scotland on whose template this sample document is based, adapted for the Irish legislative framework.*

Appendix 2

Risk Factor Questionnaire – Law Society Sample Form – Version 1

Instructions

* The Law Society has developed this sample adaptable Questionnaire to assist solicitors when assessing ML/TF risk particular to the legal sector.
* The questionnaire is designed to be used in conjunction with the sample adaptable ‘Document your Customer Risk Assessment’ Forms.
* This questionnaire details risk factors and questions which can be considered when assessing the risk of an AML-regulated legal service. Please use the notes column to summarise observations/assessment of risks involved where the issue is applicable to the client/transaction being considered.
* **Not all questions will be relevant or applicable to all situations. Conversely, the questions outlined are non-exhaustive – there may be other pertinent risk factors which should be taken into account, dependent upon the nature of the client/transaction being considered.** The Law Society recommends that all employees in solicitors’ firms develop their knowledge of legal sector ML/TF risks by accessing the comprehensive resources in ***‘Step 1 – Develop your knowledge of ML/TF risks inherent in legal services’*** in Section 2 – 2018 Guidance.
* Chapter 9 of the Society’s 2010 Guidance Notes also details non-exhaustive red flags/indicators of suspicion. Highlights include:
* Activities which have no apparent purpose, make no obvious economic sense, involve unusual losses, are unnecessarily complex, involve non-resident accounts, companies or structures, activities are without reasonable explanation/out of the ordinary range of services/inconsistent with client (paragraph 9.5)
* Excessively obstructive/secretive clients, clients who insist transactions be done inordinately quickly, use aliases, recent new relationships with financial entities, legal fees paid by third parties or in cash, avoids providing identification for group of companies by offering agent identification only (paragraph 9.6(a))
* Transactions involving areas outside of Ireland/no apparent ties to Ireland/crosses many international lines/involves wire transfers/foreign currency exchanges with locations of concern/known to facilitate money laundering/secretive banking and corporate law/illicit drug production/no effective AML system (paragraph 9.6(f))
* Property transactions where client arrives at a closing with a significant amount of cash/property purchased in the name of nominees (associates/relatives)/requests for name not to be connected with property/requests for different names to be used on different documents/last minute name substitutions/property below market value with an additional “under the table” payment/deposits paid by a third party/cash deposits/unusual source or offshore bank deposit/corporate veil purchases when inconsistent with ordinary business practice of client/property purchases without inspecting property/multiple property purchases in short time period with few concerns about location, condition/rent paid or amount of a lease in advance using a large amount of cash (paragraph 9.6(h)
* Cash (large payments in actual cash/lodged to accounts) (paragraph 9.14 to 9.16)
* In addition, the Guidance Notes highlight potential issues with companies and non-face-to-face transactions as follows:
* “It is … generally recognised that the use of companies, even when fronted by legitimate trading companies, are the most likely vehicles for large scale money laundering” (paragraph 6.21)
* “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” (paragraph 6.20)
* See Law Society guidance referenced in the firms PCP’s regarding the pragmatic approach to be adopted to the non-face-to-face red flag.
* Solicitors should refer to section 4 of 2018 Guidance for complete guidance about Customer Risk Assessments. In summary, solicitors have a statutory duty, when assessing ML/TF risk of each AML-regulated legal service, to have regard to:

1. their firm’s Business Risk Assessment,
2. information about legal sector risk in the National Risk Assessment
3. guidance about risk issued by the Law Society
4. any relevant risk variables, including at least the following:
5. the purpose of an AML-regulated legal service
6. the level of assets/size of transactions undertaken
7. the regularity of transactions or duration of the business relationship
8. the presence of any potentially low risk factor specified in Schedule 3
9. the presence of any potentially high-risk factor specified in Schedule 4

After you have completed the questionnaire, the next step is to ‘document your thought process’ in one of the Customer Risk Assessment Forms relevant to the current stage of the instruction.

|  |  |
| --- | --- |
| *CLIENT RISK* | *NOTES* |
| **STATUS OF CLIENT**   * How well do you know your client and background? * Is your client known to you personally/existing client, or new business relationship? * Is your client a PEP? * Has your client been introduced to you by a 3rd Party? Is the instruction from your client channelled through a 3rd party? If so, why? * Are you aware of your client having any links to criminality? |  |
| **FACE-TO-FACE CONTACT**   * Have you met with your client face-to-face or is it a non-face-to-face transaction? Non-face-to-face is a factor suggesting potentially higher risk. * If non-face-to-face, are you comfortable there is a legitimate reason for this and what is the reason? |  |
| **LOCATION OF CLIENT**   * Where is your client based? Locally/Ireland/EU/other international location? * Is your client based/resident/linked to a high-risk jurisdiction/high risk third country? Is your client linked to a country the subject of sanctions? * Does your client have connections to a jurisdiction where ML controls may not be as tight as in the EU? Are funds being sent to/from any of these places? |  |
| **ID & ADDRESS VERIFICATION**   * Has your client provided acceptable standard ID and address verification? * Has your client provided acceptable non-standard ID and address verification? * Have you been able to confirm the authenticity/professional status of the certifier of any copies of ID/address verification? * Has your client been cooperative in the process, or have they delayed providing ID and address verification / appeared reluctant to do so? * Have electronic methods been utilised to verify client identity? If so, please outline. |  |
| **FINANCIAL PROFILE OF CLIENT**   * Does the stated source of wealth / source of funds and the amount of money involved stack up with what you know of your client, for example given their age and occupation? (If no, or other ML/TF risks arise, enhanced CDD may require establishing source of wealth and source of funds) * Is your client involved in / run a high risk or high cash turnover business? Is there the potential that the funds are from untaxed income? Is there a potential the funds are the proceeds of fraud/social welfare fraud? |  |

|  |  |
| --- | --- |
| *AML-REGULATED LEGAL SERVICE RISK* | *NOTES* |
| TYPE OF LEGAL SERVICE   * Could the type of transaction be used for the purposes of money laundering or is it at a higher risk of money laundering?   - E.g., Will / Power of Attorney - lower risk  - Estate Agency / Conveyancing / Commercial Property - higher risk   * Does the transaction make sense or is it overly complex given the underlying nature of the business being conducted? * Does it make sense that your client has asked your firm to carry out this type of transaction? (e.g., is it within your area of expertise/local geographical area?) |  |
| **VALUE OF LEGAL SERVICE/ASSET/TRANSACTION**   * Does the value of the transaction appear to fall within the financial means of your client, given their income and savings? |  |
| **SOURCE OF FUNDS**   * Is the source of funds clear and identifiable? * Are funds coming from a recognised financial/credit institution (e.g., a loan or mortgage) or are they personal funds? If no loan or mortgage, enquire into the source of wealth. It may be prudent to ask for some supporting evidence to confirm the information provided and then reconsider the ML/TF risks involved. * Is any funding coming from overseas? From where? From whom? Connection to client? * Are any of the funds being paid by a third party otherwise unconnected to the transaction? * Does your client seek to change the source of funds at the last minute? * Has your client paid excess funds into your client account? Why/How? * Is it being proposed that funds come from outside the EU and gain entry to the EU financial system for the first time via your client account? * Could the client be trying to route funds through the solicitor without an underlying transaction? [N.B. This would be contrary to the Solicitors' Accounts Regulations and solicitors’ firms should not provide a banking service for their clients: *“Client accounts should only be used to hold client money for legitimate transactions for clients, or for another proper legal purpose. Money-launderers will seek to route ‘dirty’ money through a solicitor’s client account in order to ‘clean’ it, either by asking for the money to be returned or by purchasing a clean asset with the funds.”* (Paragraph 9.13 – 2010 Guidance)]   *N.B. Standard CDD requires solicitors to understand the client’s source of funds/wealth. Evidence of source of funds/wealth is only required if there is a high ML/TF risk and, in such circumstances, solicitors must consider whether any documentation could possibly negate the risk that the solicitor might themselves unwittingly commit the substantive offence of ML/TF by proceeding. Please see further ‘Do I need to obtain evidence or “determine” the source of funds?’ and ‘Establishing source of wealth and funds’ in Section 5 - 2018 Guidance* |  |
| **DESTINATION OF FUNDS**   * Has your client requested that proceeds of a transaction be paid to someone other than a lender or themselves? * Are proceeds of a transaction to be paid to an overseas account? |  |

Reminder - After you have completed the questionnaire, complete the relevant ‘’document your thought process’ form (provided separately) to document your thought process for individual ML/TF Customer Risk Assessment, CDD measures and any other compliance decisions.

*The Law Society accepts no responsibility for any compliance failures or loss incurred as a result of reliance on this sample questionnaire. Solicitors’ firms must always ensure they are in compliance with all of their statutory AML obligations.* *The Law Society is grateful to the Law Society of Scotland on whose template form this questionnaire is based, adapted for the Irish legislative framework*

Document Your Thought Process – Law Society of Ireland Sample Form – Version 1

Instructions

* The Law Society has developed three sample forms to help solicitors ‘document their thought process’ process for Customer Risk Assessments, concerns about ML/TF or red flags, decisions about CDD measures applied and any other compliance decisions.
* The forms are designed to be used in conjunction with the Risk Factor Questionnaire (provided separately) and are best completed **after** the Risk Factor Questionnaire for Customer Risk Assessment (provided separately).
* These examples can be adapted by firms to suit their firm’s individual needs. They can be tailored by solicitors across the life cycle of an AML-regulated legal service as they assess and document risk. For example, Form 1 can be used to guide and document decisions about whether to provide an AML-regulated 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 and the rationale for the CDD applied. This also allows solicitors to follow the FATF’s 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.”

* If you have assessed the risk as **high** at any point during an AML-regulated legal service, have any reservations or concerns or have observed ML/TF red flags, please refer to **[the Managing Partner, the MLRO]** before continuing to act for the client. 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.

FORM 1

|  |  |
| --- | --- |
| INITIAL ASSESSMENT OF RISK: | LOW MEDIUM HIGH  (Standard CDD) (Standard CDD) (Do not proceed or  Enhanced CDD) |
| Please note below reasons for your initial ML/TF risk assessment:  Please document the CDD measures to be applied, have been applied and any compliance decisions taken:  NB If there is a risk client is involved in ML/TF, ascertain whether they have PEP status and, if they are a PEP, apply section 37 enhanced CDD. | |
| SIGNED BY: | DATE: |

FORM 2

|  |  |
| --- | --- |
| INTERIM/ONGOING RISK ASSESSMENT –IF ANY RISK FACTORS CHANGED? | LOW MEDIUM HIGH  (Standard CDD) (Standard CDD) (Do not proceed or  Enhanced CDD) |
| Please note below reasons for your assessment:    *(If no chance, quick note stating such, signed and dated – this provides evidence that a review has been undertaken and consideration given)*  Please document the CDD measures to be applied, have been applied and any compliance decisions taken: | |
| SIGNED BY: | DATE: |

FORM 3

|  |  |
| --- | --- |
| FINAL RISK ASSESSMENT – HAVE THERE BEEN ANY LAST-MINUTE CHANGES THAT GIVE CAUSE FOR CONCERN? | LOW MEDIUM HIGH  (Standard CDD) (Standard CDD) (Do not proceed or  Enhanced CDD) |
| *(Ideally, should be undertaken before monies are transacted/enter the client A/C)*  Please note below reasons for your assessment:    *(If no change, quick note stating such, signed and dated – this provides evidence that a review has been undertaken and consideration given)*  Please document the CDD measures to be applied, have been applied and any compliance decisions taken: | |
| SIGNED BY: | DATE: |

*The Society accepts no responsibility for any compliance failures or loss incurred as a result of reliance on these sample forms. Solicitors’ firms must always ensure they are in compliance with all of their statutory AML obligations. The Law Society is grateful to the Law Society of Scotland on whose template forms this document is based, adapted for the Irish legislative framework.*

Appendix 3

The following is a non-exhaustive list of factors suggesting potentially lower risk, as per the CJA.

(1) Customer/client 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) clients that are resident in geographical areas of lower risk

(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 clients, 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.

Appendix 4

The following is a non-exhaustive list of factors suggesting potentially higher risk, as per the CJA.

(1) Client risk factors:

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

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

(c) non-resident clients;

(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.”.

Appendix 5

Identification and Verification – Documents Required for Corporate Entities

(Firms should note the statutory duty to confirm that information concerning teh beneficial ownership of a customer is entered in the relevant registers)

Client:

Matter Reference:

1. Private company - (standard risk)

|  |  |  |
| --- | --- | --- |
|  | Yes/No | Comment |
| Company Printout |  |  |
| Internet Search |  |  |
| Certificate of Incorporation |  |  |
| Most recent annual return |  |  |
| The names of all Beneficial Owners with greater than 25% of the shares or voting rights or who otherwise exercise control. |  |  |
| Identification and verification documents for at least one Director |  |  |
| Verify that any person purporting to act on behalf of the client is so authorised |  |  |

Private Company (high risk) – all of the above together with the following:

|  |  |  |
| --- | --- | --- |
|  | Yes/No | Comment |
| MLRO Approval |  |  |
| Identification and verification of all Beneficial Owners with greater than 25% of the shares or voting rights or who otherwise exercise control |  |  |
| Identification and verification of two directors (or equivalent) or one director of the company and one individual with authority to act on behalf of the company |  |  |

2. Charities/Trusts

If incorporated – same as above

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes/No | Comment | |
| Full name of the trust, foundation or other similar entity |  |  |
| Nature and purpose of the trust, foundation or other entity |  |  |
| Country of establishment |  |  |
| Names and addresses of all trustees or equivalent persons |  |  |
| Copies of any and all instruments establishing and governing the trust |  |  |

3. Entities Regulated by an Approved Regulator

Subject to a risk assessment, simplified due diligence may be applied to regulated entities that are Low Risk Clients. All documents for this type of client should be available from approved public sources.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes/No | Comment | |
| Identification and verification of client – full legal name |  |  |
| Confirmation client is regulated |  |  |
| Evidence from competent authority website that the client is authorised and supervised |  |  |

4.Partnership – (standard risk)

|  |  |  |
| --- | --- | --- |
|  | Yes/No | Comment |
| Constitutional document |  |  |
| Partnership Deed, Agreement or equivalent |  |  |
| Names of Partners |  |  |
| The names of all Beneficial Owners with greater than 25% of the shares or voting rights or who otherwise exercise control. |  |  |
| Verify the identity of at least one partner and at least one individual with authority to act on behalf of the partnership |  |  |
| Verify that any person purporting to act on behalf of the client is so authorised |  |  |

Partnership – (High Risk) – all of the above together with the following:

|  |  |  |
| --- | --- | --- |
|  | Yes/No | Comment |
| MLRO Approval |  |  |
| Identification and verification of all Beneficial Owners with greater than 25% of the shares or voting rights or who otherwise exercise control |  |  |
| Identification and verification of two Partners |  |  |