[PRACTICE NAME] Anti-Money Laundering Policies and Procedures (PCPs)

Date:

Last Updated:

Version control:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Change | Name | Senior Management/Board Sign off |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Overview 3](#_Toc126840553)

[Obligations 4](#_Toc126840554)

[MLRO 4](#_Toc126840555)

[The MLRO should be: 4](#_Toc126840556)

[Risk Assessment 5](#_Toc126840557)

[Practice Wide Risk Assessment (PWRA) 5](#_Toc126840558)

[Client/Matter-Level Risk Assessment 5](#_Toc126840559)

[Client Due Diligence 6](#_Toc126840560)

[Source of Funds (SoF) 7](#_Toc126840561)

[Source of Wealth (SoW) 8](#_Toc126840562)

[Simplified Due Diligence 8](#_Toc126840563)

[Ongoing Monitoring 9](#_Toc126840564)

[Reliance 10](#_Toc126840565)

[Enhanced Due Diligence (EDD) 10](#_Toc126840566)

[When to apply EDD 10](#_Toc126840567)

[Enhanced Ongoing Monitoring 11](#_Toc126840568)

[EDD Measures - Understanding a clients Source of Wealth (SoW) 12](#_Toc126840569)

[Politically Exposed Persons (PEP’s) 12](#_Toc126840570)

[Who is a PEP? 13](#_Toc126840571)

[Identifying a PEP 13](#_Toc126840572)

[Suspicious Activity Reporting 15](#_Toc126840573)

[Seeking consent/Defence against Money Laundering 15](#_Toc126840574)

[Tipping off 16](#_Toc126840575)

[Technology 16](#_Toc126840576)

[Training 17](#_Toc126840577)

[What should be included in training? 17](#_Toc126840578)

[Internal Controls & Governance 17](#_Toc126840579)

[Record keeping & Data Protection 18](#_Toc126840580)

[Retention Periods 18](#_Toc126840581)

[Proliferation Financing 19](#_Toc126840582)

**Useful information:**

The **black text** within this document is static and can remain as is

The red text within this document **must** be changed to reflect the details of your Practice – e.g., practice name etc.

The purple text contains guidance and considerations for your practice to consider and **must also** be amended to fit with your Practices approach to each section. The practice must consider these questions and text and amend/delete/incorporate responses in line with the circumstances, size, and nature of your Practice.

# Overview

[PRACTICE NAME] take a zero-tolerance approach to being involved in illegal/illicit activity and will fully comply with all relevant sections of the Money Laundering Regulations 2017 (as amended), the Proceeds of Crime Act 2002 (POCA), the Terrorism Act 2000 (TACT) as well as the Legal Sector Affinity Group guidance (LSAG guidance).

* [The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (legislation.gov.uk)](https://www.legislation.gov.uk/uksi/2017/692/contents)
* [Proceeds of Crime Act 2002 (legislation.gov.uk)](https://www.legislation.gov.uk/ukpga/2002/29/contents)
* [Terrorism Act 2000 (legislation.gov.uk)](https://www.legislation.gov.uk/ukpga/2000/11/contents)
* Legal Sector Affinity Guidance ([lsag-aml-guidance-final-version-2-january-2021.pdf) (lawscot.org.uk)](https://www.lawscot.org.uk/media/370276/lsag-aml-guidance-final-version-2-january-2021.pdf)

*Please note that the above is subject to change and it is your responsibility to ensure that your PCPs are amended/updated in line with any legislative, regulatory or supervisory-related changes.*

All partners and employees of the practice are under an obligation and duty to comply with the above.

This policy and any related procedures aim to help partners and staff fulfil these responsibilities, by providing a clear framework, along with setting out the practices key principles and obligations.

All staff are encouraged to report to the practices MLRO any action or inaction which they suspect may represent a breach of these policies or involve an attempt to launder money through the practice. The MLRO has a duty to disclose knowledge or suspicion, or reasonable grounds for suspicion, of money laundering to the National Crime Agency (the ‘NCA’).

Failure to fulfil the responsibilities as per this Policy may result in disciplinary action and may also result in criminal sanctions for the staff involved. Breaches may also be reportable to our AML Supervisor (The Law Society of Scotland). Further information on this can be found:

[lsag-breach-reporting-note.docx (live.com)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.lawscot.org.uk%2Fmedia%2F372545%2Flsag-breach-reporting-note.docx&wdOrigin=BROWSELINK)

[AML FAQs | Law Society of Scotland (lawscot.org.uk)](https://www.lawscot.org.uk/members/regulation-and-compliance/financial-compliance/anti-money-laundering/aml-faqs/)

# Obligations

R.19(3) states that a Practices PCP’s must include:

* Risk management practices (LSAG guidance sections 5 and 6)
* Internal controls (R.21-24 and LSAG guidance section 9)
* Customer Due Diligence (CDD) including the nature and extent of identification of checks to be done under simplified, standard, and enhanced DD (R.27-38 and LSAG guidance section 6)
* Reliance and Record keeping (R.39-40 and LSAG guidance 6 and 10)
* The monitoring and compliance with, and the internal communication of the PCP’s (LSAG guidance sections 8 and 9)

Please see LSAG guidance 4.8 for an overview of other items which must be included.

Key responsibilities of staff include (but are not limited to):

* Conducting an adequate risk assessment and appropriate due diligence (CDD) on clients and transactions, including PEP and sanctions checking
* Monitoring all clients/transactions on an ongoing basis for potential money laundering or terrorist financing activity
* Reporting any suspicious activity in respect of the client or transactions, to the MLRO in accordance with the practices Suspicious Activity Report (SAR) procedure
* Avoiding discussing any potential or actual SARs with clients or any third parties. If you do so, you could be guilty of an offence under POCA s333A or TACT s39
* Referring any Police/Law Enforcement queries or requests to the MLRO
* Undertaking any AML-related training provided by the practice
* Keeping appropriate records of all AML related activity – including how PCPs are communicated to staff.

## MLRO

**LSAG guidance 4.3**

The MLRO is ultimately responsible for ensuring that information leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the National Crime Agency (NCA).

The MLRO has a personal responsibility to ensure they fulfil their duties and may be subject to conviction under s.331 of the Proceeds of Crime Act 2002, for a failure to disclose information to the NCA.

Where appropriate, the MLRO should also submit an (at least) annual “MLRO Report” to the Board setting out key information relating to the AML Compliance of the Practice. Further information can be found in LSAG Guidance s.4.3.3.

### The MLRO should be:

* Of sufficient seniority to make decisions on reporting which can impact your practice's business relations with your clients and your exposure to criminal, civil, regulatory, and disciplinary sanctions
* In a position of sufficient responsibility to have access to all client files and business information. This will allow them to make decisions on the basis of all information held by the practice
* Supported and empowered in the carrying out of their duties by the Board
* The appointment should be documented, along with the rationale behind the appointment

# Risk Assessment

**LSAG guidance section 5.6**

## Practice Wide Risk Assessment (PWRA)

R.18 requires the practice to document a PWRA.

[PRACTICE NAME] has established its own risk profile as per R.18 and has considered the following factors (please see separate PWRA for further details on each factor):

* Client Risk Factors (LSAG guidance 5.6.1)
* Client Turnover (LSAG guidance 5.6.1.1)
* Politically Exposed Persons - PEPS (LSAG guidance 5.6.1.2)
* Clients in higher risk sectors (LSAG guidance 5.6.1.3)
* Clients with cash intensive businesses (LSAG guidance 5.6.1.4)
* Geographic Risk (LSAG guidance 5.6.2)
* Higher Risk Jurisdictions (LSAG guidance 5.6.2.1)
* Product or Service Risks (LSAG guidance 5.6.3)
* Delivery Channel Risk (LSAG guidance 5.6.4)
* Transaction Risk (LSAG guidance 5.6.5)

*Consider: Your PWRA should be used to influence your PCP’s. AML PCPs should be tailored to mitigate the risk as noted above. I.e., if your Practice Wide Risk Assessment indicates conveyancing as a high-risk area of your business, it may be appropriate to place stronger/more stringent AML procedures in place within this area of your business, compared to lower risk areas.*

Based on consideration of the above factors, Senior Management believe [PRACTICE NAME] is at an inherently [low/medium/high risk] of being used to launder the proceeds of crime.

## Client/Matter-Level Risk Assessment

Detail your Practices approach to the Client and Matter Risk Assessment (RA), including:

* Who is responsible for completing the RA and how is it undertaken?
* Factors to be considered at all levels of risk assessment (LSAG Guidance 5.6)
* Client Risk Assessment (LSAG guidance 5.10) – a written assessment on each new client. This assessment should include all of the key risk factors outlined within LSAG guidance 5.10
* Matter Risk Assessment (LSAG guidance 5.11) – a written assessment on each matter undertaken. This assessment should out line all the key risk factors outlined within LSAG guidance 5.11
* When/how often/in what circumstances is the RA reviewed through the course of the transaction?
* The Practices position of risk factors/red flags and what action this leads to. E.g., what standard of due diligence should be applied (SDD/CDD/EDD) and what this entails
* The Practices position/policy on international clients/matters or funds coming in from overseas (particularly locations of increased money laundering risk)
* How these Risk Assessments are recorded and documented

*The PCPs should make reference to key flag indicators/risks and detail what employees should look for, as well as what steps should be taken do to mitigate against these red flags/risks. Please see LSAG guidance section 18.2 for assistance with this.*

# Client Due Diligence

**LSAG guidance section 6**

Undertaking appropriate Customer Due Diligence (CDD) is required under R.27 and R.28.This is one of the key controls in order to protect the Practice from Money Laundering and Terrorist Financing risks.

CDD is the collective term for the checks we must complete on our clients, which may differ depending on the circumstances.

**CDD is holistic in nature and is wider than simply undertaking identification and verification of clients**.

Key information regarding understanding the nature and purpose of a relationship may include:

* The nature and details of the business/occupation/employment
* Source of funds and source of wealth information
* Anticipated levels and nature of activity to be conducted

**The individual responsible for collecting CDD should detail the background and nature of the client and the matter.**

In this section you **must** document the Practices PCPs which cover the below points:

* CDD procedures (including procedures to identify the ownership and control structures of non-natural persons)
* ID&V procedures in relation to the Ultimate beneficial owners of non-natural clients (and those purporting to act on behalf of a client)
* Procedures to facilitate a clear understanding of the client’s source of funds (SoF) and source of wealth (SoW) in relation to a transaction and the level of evidence required, in line with the risk profile of the client/matter
* Procedures to facilitate reporting of discrepancies between Beneficial Ownership information obtained through DD checks and what is held on the Companies House register (R.30A)
* The practice’s position on the use and application of Simplified Due Diligence
* The timing of any due diligence procedures
* The practice’s position on the use of R.39 Reliance and any related procedures
* The ongoing monitoring of clients and their matters
* The identification of instances where it is required or appropriate to re-apply or renew CDD or EDD on a client
* Identification and scrutiny of any complex or unusually large transactions, or an unusual pattern of transactions, or those which serve no apparent economic or legal purpose
* Any additional measures to prevent products/transactions that support anonymity being used for ML/TF
* Identification of PEP’s, their relatives or close associates and the control of any associated risks

Specific CDD/ID&V measures should also be set out include, but are not limited to the following:

**Natural Persons (LSAG guidance 6.14.4)**

* Clients unable to produce standard documentation (LSAG 6.14.7)
* Professionals (LSAG 6.14.8)
* Persons acting on behalf of the client (LSAG 6.14.9)

**Non-natural Persons (LSAG 6.14.10)**

* Companies (LSAG 6.14.11)
* Trusts (LSAG 6.14.12)
* Partnerships, limited Partnerships, Scottish limited Partnerships and UK LLP’s (LSAG 6.14.13)

## Source of Funds (SoF)

**LSAG guidance 6.17.2**

*This section should detail the practices procedures in relation to understanding and evidencing Source of Funds – this should be based on the information below.*

Source of Funds refers to the funds that are being used to fund the specific transaction

in hand – i.e., the origin of the funds used for the transactions or activities that occur within the business relationship or occasional transaction.

The question you are seeking to answer should not simply be, “where did the money for the transaction come from,” but also “how and from where did the client get the money for this transaction or business relationship.”

**It is not enough to know the money came from a UK bank account or financial institution.**

The types of data and documents that we use for verification of SoF will vary depending on the circumstances.

**Understanding the clients SoF is not limited to collating bank statements**.

**It should also not be simply limited to checking that the client’s name matches the name on the account**.

Documentation we could request to *assist us* with understanding and evidencing a clients SoF include, but are not limited to:

* Bank statements
* Documentation from a regulated financial institution or professional showing proceeds of asset sale/divestment
* Wills
* Full payslips
* Audited financial accounts showing funds disbursed to the client
* Sales/purchase agreements

Further detail the steps your practice takes to understand your clients SoF. This is not the same as Source of Wealth (SoW) and the difference between the two should be detailed.

## Source of Wealth (SoW)

SoW describes the economic, business and/or commercial activities that generated, or significantly contributed to, the client’s overall net worth/entire body of wealth. This should recognise that the composition of wealth generating activities may change over time, as new activities are identified, and additional wealth is accumulated.

A holistic approach should be taken when establishing a clients SoW. Questions we could ask include, “what is the origin of the client’s entire body of assets?”, rather than just looking at what has funded a specific scenario.

Your practices approach to establishing and documenting a clients SoW should be included within your PCPs. The level of detail will depend on the risk rating for that particular client/matter. Further information on SoW can be found within the Enhanced Due Diligence section below.

*N.B. The Law Society of Scotland has also published a Frequently asked Questions document on the difference between Source of Funds and Source of Wealth which can be found here:*

[AML FAQs | Law Society of Scotland (lawscot.org.uk)](https://www.lawscot.org.uk/members/regulation-and-compliance/financial-compliance/anti-money-laundering/aml-faqs/)

## 

# Simplified Due Diligence

**LSAG guidance 6.20**

Under R.37, we may be allowed to relax the type, timing and extent of measures undertaken under CDD where a matter is eligible for Simplified Due Diligence (SDD). We must continue to monitor the relationship and transactions to ensure that SDD continues to be appropriate. We must carry out sufficient monitoring of the relationship or transaction to enable us to detect any unusual or suspicious transactions.

SDD may be considered when your client is:

* A public administrator or a publicly owned enterprise
* An individual resident in a geographic area of lower risk
* A credit or financial institution which is subject to requirements in national legislation
* A company listed on a regulated market (including majority owned subsidiaries) and the location of the regulated market

SDD is the lowest permissible form of due diligence and must only be used where we have determined that the client presents a low risk of money laundering or terrorist financing.

You must record your reasoning for why you have determined that it is appropriate to use SDD via your client or matter risk assessment. It may be that due to factors recognised in your PWRA, it may not be appropriate for us to use SDD at all.

You must clearly document within your PCPs how SDD is undertaken in the context of your practice and under what circumstances this would be acceptable.

## Ongoing Monitoring

**LSAG guidance 6.21**

R.28(11) requires that we should conduct ongoing monitoring of business relationships and throughout the course of a transaction. Ongoing monitoring is defined as:

* Scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with your knowledge of the client, their business, and their risk profile
* Undertaking reviews of existing records and keeping the documents, or information obtained for the purpose of applying CDD, up to date

Ways in which we can comply with R.28(11) are:

* Renew and re-evaluate CDD at appropriate intervals, including during the course of a transaction
* Suspend or terminate a business relationship until we have updated information or documents, though this may be excessive if we are satisfied, we know who our client is, and keep under review any request we have made for information or documents
* Use technology to aid our ongoing monitoring.

CDD must be reapplied for existing clients on a risk-based approach and when we become aware that the material circumstances of the client or the source of funding have changed. Questions we should ask ourselves include, but are not limited to:

* Throughout the course of the transaction, have the source of funds changed?
* Have any third-party funds been introduced?
* Has the client or beneficial ownership changed?

Each time ongoing monitoring is conducted, we should record:

* What was considered
* The action taken (if any)
* The reason for the decision made
* Who undertook the ongoing monitoring and the date in which it was applied

The practice must clearly document within the PCPs how ongoing monitoring is undertaken in the context of your practice. This should be tailored to suit depending on the size/nature of your practice.

## Reliance

LSAG guidance 6.23

Under R.39, in certain circumstances, we may rely on another person to conduct CDD for us, subject to their agreement.

Reliance goes further than solely obtaining certified copies of documentation from other regulated professionals.

The Practice remains liable for any non-compliance with CDD requirements and therefore not all practices will choose to exercise their right to use Reliance.

Should your practice decide to exercise your right to use Reliance, this must be clearly documented within your PCP’s. including how this is undertaken in the context of your practice and what steps should employees take to ensure they comply with Regulations.

Should you decide not to exercise your rights to use Reliance as a form of CDD, this must also be clearly documented within your PCP’s.

# Enhanced Due Diligence (EDD)

**LSAG guidance 6.18**

*This section should clearly outline your Practices approach to EDD, when it would be applied and what steps employees should take to comply with the regulations and LSAG guidance.*

The Regulations specify that we must take measures to examine the background and purpose of the transaction and to increase the monitoring of the business relationship where Enhanced Due Diligence (EDD) is required. The Regulations are not prescriptive about exactly what must be included in EDD, with the exception of PEP’s (please see separate section on PEPs within this document for further information).

EDD is required where there is a higher risk of money laundering or terrorist financing. In determining whether there is a higher risk of money laundering or terrorist financing in each case, we must consider the risk factors set out in R.33(6), along with the outcomes of the practice-wide, client and matter risk assessments.

HM Treasury released an Advisory notice which came into force on 22 January 2024, this note amended the definition of HRTC. It removes Schedule 3ZA containing the list of HRTCs in the MLRs. Instead of referring to a separate schedule, Regulation 33(3)(a) will now define an HRTC as:

* a country named on either of the following lists published by the Financial Action Task Force (FATF) as they have effect from time to time—

1. High-Risk Jurisdictions subject to a Call for Action;
2. (ii) Jurisdictions under Increased Monitoring

In order to keep abreast of which countries are HRTCs, relevant persons will now have to refer directly to lists published by the Financial Action Task Force (‘FATF’) of ‘Jurisdictions Under Increased Monitoring’ and ‘High-Risk Jurisdictions subject to a Call for Action’. These lists are updated three times a year, on the final day of each FATF Plenary meeting, held every February, June and October.

## When to apply EDD

**LSAG guidance 6.19**

EDD **must** be applied in the following circumstances:

* Regulation 33(1)(b) requires businesses to apply enhanced customer due diligence and enhanced ongoing monitoring in any business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country. This means that relevant persons are obliged to carry out enhanced customer due diligence and enhanced ongoing monitoring on all customers, new and existing, established in high-risk third countries.
* If the customer has been deemed to be of PEP status (please see section on PEPs for further details)
* In any case where it has been discovered that the client has provided false or stolen ID documents.

And in any case where:

* A transaction is complex or unusually large
* There is an unusual pattern of transactions
* The transaction(s) have no apparent economic or legal purpose
* In any other case whereby, its nature can present a higher risk of money laundering or terrorist financing.

R.33(6) – Risk Factors you must consider when determining whether to apply EDD

* Customer Risk Factors (R.33(6)(a)
* Product, service, transaction, or delivery channel risk factors (R.33(6)(b)
* Geographic risk factors (R.33(6)(c)

Depending on the requirements of the case, the EDD measures required may include, among other things:

* Seeking additional independent, reliable sources to verify information provided or made available to the relevant person
* Taking additional measures to understand background, ownership, and financial situation of the client (this includes both SoF and SoW), and other parties to the transaction
* Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
* Increasing the monitoring of the business relationship, including greater scrutiny of transactions
* Obtaining the approval of senior management/MLRO for establishing or continuing the business relationship
* Conducting enhanced monitoring of the client relationship by increasing the number and timing CDD applied
* Examining beneficial owners with less than 25% ownership if you have concerns regarding the ownership structure or feel that the ownership structure is a pertinent risk factor, to fully understand control and ownership interests in the client.

### Enhanced Ongoing Monitoring

**LSAG guidance 6.18.4**

Enhanced ongoing monitoring is automatically required whenever EDD is applied. One way to achieve this is to ensure that transactions are in line with the CDD information held on the client, as well as information contained in the client and matter risk assessments.

Ways to apply ongoing monitoring may include:

* Requiring a greater level of information and explanation from the client when activity diverts from that addressed in their client risk assessment
* Greater frequency of checks on transactions, particularly SoF
* Undertaking more frequent due diligence checks on your client.

Further information on ongoing monitoring can be found within the ongoing monitoring section below.

### EDD Measures - Understanding a clients Source of Wealth (SoW)

**LSAG 6.18.3**

*This section should detail the practices procedures in relation to understanding and evidencing Source of Wealth (in addition to Source of Funds) in EDD situations – this should be based on the information below.*

*The Law Society of Scotland has also published a Frequently asked Questions document on the difference between Source of Funds and Source of Wealth which can be found here:*

[AML FAQs | Law Society of Scotland (lawscot.org.uk)](https://www.lawscot.org.uk/members/regulation-and-compliance/financial-compliance/anti-money-laundering/aml-faqs/)

An important additional EDD measure should include understanding the financial situation of your client. This means taking additional measures to understand the SoW as well as the SoF of our client.

A question to ask yourself is: “why and how does the individual have the amount of overall assets they do – and how did they accumulate/generate these?”

*Within your PCPs you should have a clear and documented approach to how your Practice deals with understanding your client’s SoW. This should be holistic in nature.*

# Politically Exposed Persons (PEP’s)

**LSAG guidance 6.19.3**

*Within this section you must detail your practices approach regarding PEPs. Should onboarding PEPS fall outside of your risk appetite, this should be clearly documented within your PCPs.*

PEPs present risks as they have the opportunity to use their political position to enrich themselves through corrupt activities.

In order to treat PEPs in a risk-based manner, it is a precondition that we can correctly identify them.

EDD must be applied and Senior Management approval given. **This is not optional.**

## Who is a PEP?

**LSAG guidance 6.19.3.1**

A PEP is a person who has been entrusted within the last year (or for a longer period if you consider it appropriate to address the risks in relation to that person) with one of the 93 following prominent public functions by a public institution, an international body, or a state, including the UK.

**Listing of PEP roles R.35(14)**

* Heads of state, heads of government, ministers and deputy or assistant ministers
* Members of parliament or similar legislative bodies
* Members of governing bodies of political parties
* Members of supreme courts, of constitutional courts, or any judicial body whose decisions are not subject to further appeal, except in exceptional circumstances
* Members of courts of auditors or of the boards of central banks
* Ambassadors, charges d'affaires and high-ranking officers in the armed forces
* Members of the administrative, management or supervisory bodies of state-owned enterprises
* Directors, deputy directors and members of the board of equivalent function of an international organisation.

In addition to the primary PEPs listed above, a PEP also includes (R.35(12)):

* Family members of a PEP – spouse, civil partner, children, their spouses or partners, and parents
* Known close associates of a PEP – persons with whom joint beneficial
* Ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity arrangement set up by the primary PEP

Further information on PEPs is contained within the FCA guidance – [FG17/6: The treatment of politically exposed persons for anti-money laundering purposes (fca.org.uk)](https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf)

## Identifying a PEP

**LSAG guidance 6.19.3.2**

*How this is undertaken will depend on the size and nature of your Practice.*

*If you have decided not to engage with clients who meet the definition of a PEP, the rationale behind this must be clearly documented within your PCPs.*

R.35(1) requires us to have appropriate risk management systems and procedures to determine whether a client or beneficial owner is a PEP.

[PRACTICE NAME] take a risk-based approach to identifying PEP’s.

In Practices where undertaking work on behalf of a PEP is unlikely or rare, it may be acceptable to use publicly available or open sources to assist with identifying a PEP.

Simple measures may include:

* Asking the client or their representative (as appropriate) whether the person is a PEP, as a part of client onboarding
* Performing an internet search to check whether the individual may hold any position that qualifies them as a PEP
* Reviewing the information, they submit to you carefully to determine whether any information you have access to, suggests they may be a PEP

*If PEPs are identified the practice must have a clear, written procedure in place to perform the requisite EDD in line with r.35 as well as detailing how that relationship/client should be managed.*

It is important to note that if a PEP relationship is established, the Regulations specify that we **must** take the following steps to deal with the heightened risk:

* Have senior management approval for establishing a business relationship with a PEP or an entity beneficially owned by a PEP
* Take adequate measures to establish the SoF and SoW which are involved in the business relationship or occasional transaction
* Conduct closer ongoing monitoring of the business relationship
* Consider which aspects of your EDD protocol are appropriate for the PEP in question

Questions we should ask regarding PEP Status:

• What role(s) does the individual hold?

• What is the nature and context of business relationship?

• What services or products does the PEP wish to use?

• What is the potential for the product to be misused for the purposes of corruption?

• Do you know if they have close family members or known associates and if so, what roles do they hold?

• What level of public scrutiny, exposure, governance, disclosures, or accountability in their role is the PEP subject to?

• Are their accompanying geographic risks associated with the PEP relationship?

• If you have identified a PEP, were they helpful in providing this information and if not, should and how would this impact my assessment of the risk present?

• Does the nature of their PEP status impact in the level of EDD that needs to be applied, and if so, how?

*Dependant on the size/nature of the Practice, a PEP register should be considered, and regularly updated/reviewed.*

# Suspicious Activity Reporting

**LSAG Guidance Section 11.**

*Within this section your PCPs must cover all your practices approach to how and when an internal SAR should be submitted to your MLRO.*

*You should also outline whether your practice has a template for reporting suspicions to the MLRO. Information on what should be included can be found within LSAG guidance 11.9.*

*Further assistance can also be found on the Law Society of Scotland’s website:* [Suspicious Activity Reports | Law Society of Scotland (lawscot.org.uk)](https://www.lawscot.org.uk/members/regulation-and-compliance/financial-compliance/anti-money-laundering/suspiciousactivityreports/) *and* [introduction-to-sars-v10.pdf (lawscot.org.uk)](https://www.lawscot.org.uk/media/371634/introduction-to-sars-v10.pdf).

All persons within the regulated sector have obligations under POCA 2002 and TACT 2000 to make disclosures of suspicions of money laundering and terrorist financing and terrorist property offences. MLRO’s have specific additional obligations. Any individual working within the regulated sector must make an internal disclosure to their MLRO if they know or suspect to have reason to know or suspect money laundering or terrorist financing is taking place.

An internal SAR **must** be submitted to the MLRO:

* If you know, suspect or have reasonable grounds for knowing or suspecting money laundering or terrorist financing where that information has come to you from work in the regulated sector (subject to privilege)
* If you are proposing to engage in a prohibited act under sections 327 to 329 of POCA and require a defence against money laundering.

This internal SAR must be submitted to your MLRO as soon as is practical after you have formed this knowledge or suspicion.

Failure to report your suspicions may result in a criminal offence being committed by the colleague involved.

Should the MLRO decide not to submit a SAR to the NCA, the MLRO will ensure that the reason for this is documented and recorded appropriately.

## Seeking consent/Defence against Money Laundering

**LSAG guidance 11.10**

The NCA can also provide a defence against Money Laundering (DAML), commonly known as consent.

If the MLRO is seeking consent, it is important to specify whether you are seeking it for yourself,

for your client, or both. The request should make clear who is seeking consent for each

prohibited act.

Please see LSAG guidance 11.10.1 and 11.10.2 for further information and assistance on DAML.

## Tipping off

**LSAG guidance 11.11 and 16.8**

You must not say anything about an internal disclosure or SAR which could prejudice an investigation. If you do so, you could be guilty of an offence under POCA s333A or TACT s39, punishable with up to two years imprisonment.

It is an offence to disclose the fact that an investigation into a possible money laundering offence is being considered or carried our id that disclosure is likely to prejudice that investigation.

# Technology

**LSAG guidance Section 7**

There is a large range of regulatory and compliance-related technology available to legal Practices. These tools assist with Electronic ID&V (EID&V) and may also encompass/ assist with PEP screening, adverse media checks and corporate register checks.

[PRACTICE NAME] has decided to make use of technology to help fulfil our obligations under the Regulations.

These include (delete as appropriate):

* Electronic ID&V systems and Source of Funds checking tools
* Corporate registries
* PEP, Sanctions, Adverse media screeners

The PCPs should then make reference to Technology where used, covering the following:

* Is an electronic EID&V tool used? If so, what role does the tool take?
* What circumstances should the tool be used?
* What are the benefits of the tool?
* What are the limitations of the tool?

If a tool is used the following should also be documented within your PCPs:

* The tools name
* What it’s used for? (ID&V, Screening, Corporate Registry)
* Who at the Practice has access to the tool?
* Who is responsible for interpreting results?
* How should results be interpreted
* What lists does the tool screen against

# Training

**LSAG Guidance Section 8**

*Within this section, you should tailor the below to your practice. Ensuring that the relevant points are covered and clearly documented within your PCP.*

Employees are [PRACTICE NAME]’s most effective defence against the Practice becoming inadvertently involved in Money Laundering or Terrorist Financing. Providing employees with adequate training, in order to equip them with appropriate AML awareness, skills and knowledge is a key part of AML controls, and an important way to mitigate the risks the Practice faces.

The practice must have clearly documented PCPs based on their PWRA, which cover the following:

* What training is completed – by the MLRO, Fee Earners, Partners and other employees – commensurate with their role and responsibilities
* Who is responsible for keeping training records up to date?
* Does the training cover off the AML responsibilities held by each employee?
* How often is AML training completed?
* How is this training recorded?

## What should be included in training?

**LSAG Guidance Section 8.3**

Your AML/CTF training programme should enable employees and agents to identify and

detect when risk indicators are present and relevant or material changes in client activity, nature or circumstances

The training should include:

* An explanation of the relevant law within the context of the services and products your practice supplies
* AML/CTF ‘red flags’, risk assessment and an explanation of the risks identified in your PWRA.
* AML/CTF policies, controls, and procedures, including CDD and EDD as applied in your practice
* Identifying suspicious activity, tipping off and the processes for internal reporting
* Record Keeping and Data protection requirements.

You should take a risk-based approach to how often training should take place, however some form of high-level basic AML awareness/refresher training should be completed annually across all relevant employees.

# Internal Controls & Governance

**LSAG guidance Section 9**

Dependent on the size and nature of your practice, it may be necessary to evidence you have adequate controls in place to audit the adequacy and effectiveness of your PCPs.

The purpose of an independent audit function is to examine, evaluate and make recommendations regarding the adequacy and effectiveness of your PCPs.

This section should also include information on employee screening – both at pre-employment and on an ongoing basis.

To ensure [PRACTICE NAME]’s compliance with LSAG guidance section 9, we take a risk-based approach to our audit requirements.

Detail in full the practices approach to this, including who undertakes the audit, what knowledge, skills, and competency they have, and the process by which independent audit is undertaken in your practice.

Please see LSAG guidance 9.3 onwards to assist with this.

# Record keeping & Data Protection

**LSAG Guidance Section 10.**

To ensure [PRACTICE NAME]’s compliance with regulations, the implementation of rigorous record keeping procedures is vital.

All Practices must be able to demonstrate to their supervisor that they have adopted a risk-based approach to the management of AML/TF risk within their businesses. This means retaining documents and records to demonstrate this.

Key areas for Record Keeping within the PCP will include:

* Risk Assessments
* Customer Due Diligence and Enhanced Due Diligence
* Policies, Controls and Procedures
* Training
* Internal Controls
* Record Keeping
* Reliance
* Data Protection

It is important to note that you must be able to demonstrate to your supervisory authority (The Law Society of Scotland) that the extend of the measures you have taken to satisfy R.28 are appropriate based on the risks of money laundering and terrorist financing.

You must also ensure that sufficient supporting records are kept in order to allow the transaction to be reconstructed as per r.40 and LSAG 10.3.

## Retention Periods

**LSAG guidance 10.4**

The records must be retained for five years beginning on the date on which you know, or have reasonable grounds to believe:

* that an occasional transaction is complete
* that the business relationship has come to an end for records relating to any transaction which occurs as part of a business relationship, or CDD measures taken in connection with that relationship.

# Proliferation Financing

In September 2022 [The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022](https://www.legislation.gov.uk/uksi/2022/860/made) came into force and saw the introduction of the requirement for practices to identify and mitigate the risk of Proliferation Financing (PF)

All practices in scope of the regulations are asked to consider the definition of PF under r.16A and to (dependent on size and nature) incorporate PF into their existing Practice Wide Risk Assessment (PWRA) (r.18) and use this to inform the PCPs in line with r.18A and r.19A.

Practices are also asked to consider the risk of PF across all regulatory requirements, including (but not limited to) client/matter risk assessments, CDD/EDD, relevant staff training, internal controls and record keeping.

We ask that practices make themselves familiar with these compulsory additional requirements and continue to monitor and update their PCPs accordingly.

Additional resources regarding Proliferation Financing, it’s background and context:

• [FATF’s Guidance on Proliferation Financing Risk Assessment and Mitigation](file:///C:/Users/bclark/Downloads/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation%20(2).pdf)  
• [HMT’s National Risk Assessment of Proliferation Financing](https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing)