CILEx Regulation Sectoral Risk Assessment - October 2024

1. Introduction

CILEx Regulation (CRL) is one of the supervisors responsible for monitoring compliance with anti-money laundering (AML) legislation. To ensure the effectiveness of its monitoring and to reduce the potential for such economic crime, CRL must understand the current and potential risks faced by the community it supervises.

1.1 The purpose of the CRL Sectoral Risk Assessment

Regulation 17 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended (MLR) require CRL as a supervisory authority to identify and assess the international and domestic risks of money laundering and terrorist financing that its supervised sector faces.

Money laundering covers a wide range of activity but is basically concealing the origin of money obtained from criminal activity. Terrorist financing is the provision or collection of funds from legitimate or illegal sources with the intention or knowledge that these funds are used to fund terrorism.

CRL also monitors the risk of the supervised sector becoming involved in proliferation financing (the funding of services used for the manufacture, acquisition, transfer of weapons or the materials used to produce those weapons).

The purpose of the Sectoral Risk Assessment is to ensure that these risks are identified, so that CRL as a supervisory body, can:

- Target its supervision to address the risks.
- Advise the supervised community how to mitigate the risk.

We also monitor the activities of our wider regulated community to identify whether their activities bring them within the scope of the MLR.

This document is the latest CRL Sectoral Risk Assessment.

1.2 Who should read the Sectoral Risk assessment?

The Sectoral Risk Assessment is designed to meet the needs of several different audiences all of which play a vital role in tackling money laundering and wider economic crime. It is there to inform:

- CRL staff as they perform their regulatory functions many of which will overlap with elements of AML supervision. It assists CRL with its risk-based approach to regulation.
- The CRL supervised community, the firms and individuals whose legal service provision brings them within the scope of the MLR.
- The CRL regulated community, which is not within the scope of the MLR, to enable it:

- comply with Economic Crime and broader AML legislation, such as the Proceeds of Crime Act 2002, the Terrorism Act 2000 and Proliferation Financing, and
- avoid becoming an enabler in wider economic crime.

We recommend that this assessment is read as part of everyone's annual AML training.

This assessment should also be taken into consideration when a supervised firm is drafting or updating its own Regulation 18 Practice-wide Risk Assessment (PWRA). We recommend that firms not strictly falling within the scope of the MLR should carry out a PWRA to provide context in risk assessing individual client matters and inform the drafting of the firm's policies and procedures.

2.0 CRLs methodology for assessing risk

CRL needs to have processes in place to identify the risks and potential risks faced by its supervised community and correctly identifies others that should be within that supervised community.

The supervised community consists of those individuals and firms providing services as:

- A Tax Adviser, as defined in Regulation 11(d) of the MLR.
- An Independent Legal Professional, as defined in Regulation 12(1) of the MLR.
- A Trust or Company service Provider, as defined in Regulation 12(2) of the MLR.

2.1 How we identify the risks currently faced by firms

To understand the money laundering, terrorist financing and proliferation financing risks faced by our supervised sector, CRL first considers the risks faced by each individual firm.

This information comes from a range of sources:

- The AML Statement the firm is required to complete each year which is specific to money laundering and wider economic crime.
- The Annual Return that regulated firms need to complete.
- Inspections and reviews.

In risk assessing the firms CRL looks a wide set of factors, including but not confined to:

- Trading history and complaints.
- The services being provided, as some services are more susceptible than others.
- The type of client, their location and how the firm is interacting with them.
- Financial information such as turnover and the level of client money held.
- Staffing levels and training.
- Policies, procedures and the firm's own risk assessment.

2.2 How we identify potential risks that could affect our supervised community

In identifying new and emerging threats that could affect its supervised community CRL is aided by information coming from a wide range of sources including but not restricted to:

- The Legal Sector Affinity Group and sub-groups as well as information from the Joint Money Laundering Intelligence Taskforce and the National Economic Crime Centre.
- The National Risk Assessment.

- Reports from firms.
- Complaints about firms.

3.0 The risk factors that need to be considered.

The National Risk Assessment[1] recognised that the legal sector is at low risk of terrorist financing but at high risk of abuse for money laundering purposes. The services most at risk of exploitation by criminals and corrupt elites for money laundering purposes continue to be conveyancing, trust and company services and client accounts.

The risk factors we consider when looking at individual firms are:

- Services
- Clients
- Location
- Financial transactions
- Training and Governance

These risk factors are covered in the following sections and highlight the findings from our risk assessments of the firms we supervise and the wider set of firms we regulate.

3.1 Services

The firms in our supervised sector provide specialist services rather than providing a broader range of services, with most firms providing probate and or estate administration services. Whilst estate administration can be viewed as being a higher risk activity because these services are more likely to manage larger value transactions, careful checks on the source of funds and clients / beneficiaries can greatly reduce the risks. Furthermore, the fact that the service must be linked to the estate of a deceased person limits the opportunity for money laundering.

Only one firm in our supervised sector is currently authorised for conveyancing limited to transactions directly linked to a probate estate. The risk level for these services has been assessed as lower than for mainstream conveyancing work.

One firm offers trust and company services provider services, but since this is a very small part of its work as it has not formed any new companies in recent years, the risk is assessed as low.

One firm although not holding client money, does provide tax advice which brings it into AML supervision. Again, with limited scope for money laundering, this has been assessed as low risk.

Based on this information we have scored this risk factor for our supervised sector as low risk.

3.2 Clients

Most firms in our supervised sector deal solely with individuals on a face-to-face basis. The one firm dealing with corporate clients is dealing primarily with local SME firms recovering business to business debts. There are no complicated ownership structures.

[1] An updated National Risk assessment is due to be published shortly

The supervised sector has reported it has not dealt with any PEPs or individuals subject to the sanctions regime in the last year.

Within the supervised sector the initial interaction with clients tends to be on a face-to-face basis, aiding the application of identity checks and verification.

Even within the wider regulated set of CRL firms the services they provide tend to be for individuals but there is a slightly increased number dealing with corporate clients. Where there are corporate clients these tend to be either micro companies[2] or small companies[3] that have established service contracts with the CRL firm.

Again, for the wider set of regulated CRL firms, none reported dealings with PEPs in the last year, and none provided services to sanctioned individuals.

Based on this information we have scored this risk factor for our supervised sector as being low risk.

3.3 Location

This risk factor is closely related to the client risk factor but considers other persons (including beneficiaries) the firms are dealing with eg overseas connections particularly with high-risk jurisdictions, and payments received from, made to or linked to high-risk jurisdictions.

Since the firms we supervise tend to see their client in person, it was not surprising that the clients were all located in the UK. In previous years there have been a small number of overseas clients or beneficiaries, but these are very much in the minority, and the firms concerned have taken steps to identify and carry out appropriate checks on these individuals.

In the reporting period there were no reported dealings with individuals from or linked to high-risk jurisdictions.

Based on this information we have scored this risk factor for our supervised sector as being low risk.

3.4 Financial transactions

As recorded in the National Risk Assessment, the holding of client money increases the risk of a firm being targeted by those involved in money laundering, terrorist financing or proliferation financing. But these risks in law firms are mitigated by the requirement in the Accounts Rules for each firm to deliver an Accountant's Report each year. Moreover, before CRL will authorise or supervise a firm it needs to be satisfied that the firm has suitable controls in place for the management of client money. This includes controls on the receipt of payments and to whom and when client account details are provided.

[2] if it has any 2 of the following:
- a turnover of £632,000 or less
- £316,000 or less on its balance sheet
- 10 employees or less (Source)

[3] if it has any 2 of the following:
- a turnover of £10.2 million or less
- £5.1 million or less on its balance sheet
- 50 employees or less (Source)

Of the supervised firms 50% will not take cash payments and of the remainder none accept cash payments of over £1,000. This again, makes these firms less attractive to criminals.

Source of funds checks carried out by supervised firms have broadly been found to be less than adequate. Some firms have treated as low risk funds received through a high street bank and have not carried out their own checks to identify the true source of the funds and the clients source of wealth.

Based on this information we have scored this risk factor for our supervised sector as medium risk.

3.5 Training and Governance

Training addressing the key aspects of anti-money laundering needs to be regularly delivered to staff.

It should cover 'red flag' matters that prompt the firm to carry out enhanced due diligence and the nature of those higher level of checks.

Whilst some firms maintain records of AML training that includes all relevant members of staff and covers the wider aspects such proliferation funding, other firms did not have proper training records as required by Regulation 24.

In undertaking this analysis three other governance related risks have been identified:

- Firms need to evidence regular monitoring of AML risks throughout the matter (not just at the outset and /or at the end of the matter). This needs to be evidenced in the Client/ Matter Risk Assessment.
- Firms need to demonstrate they have extended their Regulation 18 PWRA to include proliferation financing.
- The verification checks carried out where the firm is not meeting the client face-to-face basis needs to be more comprehensive. Risk Assessment forms should detail specifically the electronic verification that has been used and explain how this identification links to the individual they are dealing with.

Based on this information we have scored this risk factor for our supervised sector as being medium risk.

4.0 Potential / emerging risks

Alongside the risks we have identified for our supervised community there are other risks that need to be monitored and flagged if firms change the services they provide, their operating procedures or staffing.

4.1 Changes in service provision

Under the Economic Crime and Corporate Transparency Act, Companies House will be required to verify the identity of anyone submitting information to the public register, including those acting on behalf of a company. Whilst this may reduce the overall number of firms providing TCSP services, it is possible that CRL will need to supervise firms owned by CILEX members providing TCSP services which are not currently regulated as CRL firms.

There are early indications that the risk appetite of insurers is changing which may result in a greater willingness to provide professional indemnity cover to newly established conveyancing firms. If so, the risk profile of our supervised community would also change.

4.2 Changes in operating practices

The increased likelihood of remote working underlines the importance of firms being sure that they are dealing with the person to which any verified identity relates. Equally, high quality fake identity and banking documents can now be produced relatively easily.

As they start accepting crypto-currency payments CRL firms need to have suitable processes in place to verify the true source of funds.

4.3 Changes in staffing

Although there are relatively low levels of staff turnover, firms have to be sure that induction training on AML is provided promptly as part of the firm's induction process.

Equally staff changes must not impact compliance arrangements, in particular the responsibilities of the Money Laundering Reporting Officer and/or the Money Laundering Compliance Officer must be performed at all times.

5.0 Overall risk score

CRL has assessed the overall money laundering, terrorist financing and proliferation financing score for its supervised community as being low risk. The risk can and should be reduced still further. By taking action on the identified risks and by continuing to review potential risks, CRL seeks to maintain this low risk score.

6.0 Advice to the supervised / regulated community

CRL has identified a number of risks, and one of the purposes of this risk assessment is to provide advice to the supervised community and ensure it is taking the necessary action to mitigate these risks.

This section provides advice on:

- Source of funds checks
- Training
- Client / Matter Risk assessments (Regulation 28)
- Practice-wide Risk Assessment (Regulation 18)
- Identity and verification checks.

6.1 Source of Funds checks

Since one of the key elements of money laundering is the existence of criminal property, law firms must identify the true source of funds. The word 'property' is defined[4] broadly in the Proceeds of Crime Act 2002 (POCA).

[4] S.340(9) Property is all property wherever situated and includes—
(a)money;
(b)all forms of property, real or personal, heritable or moveable;
(c)things in action and other intangible or incorporeal property.

All law firms should carry out these checks, not just those falling within the scope of MLR. Failure to carry out adequate checks may result in the firm handling criminal money which is a criminal offence.

6.1.1 Requirements of the legislation

Proceeds of Crime Act 2002 (POCA)

Section 327 - it is an offence for a person to, conceal, disguise, convert, transfer criminal property or to remove criminal property from the UK.

Section 329 - it is an offence for a person to acquire, use or possess criminal property.

Whilst there are statutory defences to both these sections, the onus is on the individual to make appropriate checks that there is no criminal property.

Money Laundering Regulations (MLR)

Regulation 28 covers the customer due diligence measures, and at 28(11)(a) requires scrutiny of the transactions undertaken throughout the course of the relationship (including the source of funds) to ensure that the transactions are consistent with your knowledge of the client, the client's business and risk profile.

Regulation 31 states that where in relation to any client you are unable to apply customer due diligence measures as required in regulation 28 you must:

- Not carry out any transaction through a bank account with the client or on behalf of the client.
- Not establish a business relationship or carry out a transaction with the client otherwise than through a bank account.
- Terminate any existing business relationship with the client.

Regulation 33 requires you to carry out enhanced due diligence and ongoing monitoring of the client if any of the following risks apply:

- You have identified there is a high risk of money laundering or terrorist financing.
- The business relationship or transaction is with a person established in a high-risk third country.
- You have identified the client or potential client is a PEP[5], a family member of a PEP or a known close associate of a PEP.
- Where you are aware the client has provided false or stolen identification documents or information, and you are continuing to deal with that person.
- Where the transaction is complex or unusually large, or there is an unusual pattern of transactions, or they have no apparent economic or legal purpose.
- In any other case which by its nature can present a higher risk of money laundering or terrorist financing.

Enhanced due diligence must comply with Regulation 33(3A)(c) by obtaining information on the source of funds and source of wealth of the client or the client's beneficial owners.

[5] Politically Exposed Person

6.1.2 What do we mean by Source of Fund checks?

When we talk about ‘Source of Funds’ we are talking about where the money being used to fund the transaction, including the payment of the firm’s fees, has come from. ‘Source of Wealth’ covers the client’s total assets and how these are derived.

In practice, source of wealth and source of funds can often be linked. Financial enquiries of the client and wider information in relation to one may well shed light on the other.

6.1.3 What constitutes an adequate source of funds / source of wealth check?

As with all aspects of due diligence you need to follow a risk-based approach. The level of checks you apply to a transaction you deem to be low or medium risk will be different to those which you have identified as being high risk and therefore subject to enhanced due diligence.

Where for example you receive a relatively small payment for the firm’s fees, there is no evidence to suggest any criminal activity and you are satisfied the client is not a PEP or related to a PEP and has an identified legitimate source of income, it would be sufficient to rely on the fact that the payment is coming through a recognised UK bank, the account of which can be linked to that of the client.

Equally in a property purchase, where a mortgage provides the bulk of the funding evidence of the mortgage from the bank or building society will be sufficient to cover that element, but you would still need to consider the source of the remainder of the purchase price. Is this through the sale of another property, savings etc? If so, the client should provide evidence of the property being sold or how the savings were derived. This could be supplemented, as appropriate, by payslips or copies of bank statements.

Where a client is not known to the firm and/or the transaction is of a higher value more detailed checks will be required. It would not be sufficient to rely solely on the fact that the payment is coming from a UK bank account. You would need evidence of the source of income, the receipt of a prize, or other legitimate source of funds. Equally, any unusual source of funds must be investigated, and documentary evidence obtained.

If the client’s wealth is derived through a business they own, you may be able to look up financial records relating to the trading history of that business. This could provide the evidence that they have the funds relating to the transaction, but it is still advisable to check the specific source of the funds being used to pay for the matter. Does the bank account link to the business or the individual.

Cash payments and overpayments are often used by those perpetrating money laundering. We recommend firms have strict controls on the amounts of cash they accept. Where cash payments are being made, it is vital that the source of the money is established, and the client questioned as to why it has not been possible to make the payment from a bank account. There may well be perfectly legitimate reasons for this, but these need to be recorded on the risk assessment.

Where a matter involves several transactions, checks need to be made that the source of the funds has not changed. Is the money coming in from a different bank account. If this is confirmed, you need establish the reason and check the new source.

6.1.3 So what do we expect of firms?

Alongside the checks themselves the most crucial element is that the checks are documented. Whilst only supervised firms are required to document the risk assessment of the client / matter (Regulation 28(16)), we expect all firms to risk assess the client / matter to ensure that they comply with the Proceeds of Crime Act 2002 and the Terrorism Act 2000. Most case management systems have the facility to record this information on a Client / Matter Risk Assessment page/ form:

- Identity checks.
- Identity verification.
- PEP and Sanction checks, normally alongside conflict checks.
- Other risk information, such as source of funds, nature of the transaction.

It is not sufficient merely to state that a check has been made. As a supervisory body we need to see evidence of what check was undertaken, when, the result of the check and how this affected the risk score.

So, when completing the client / matter risk assessment you need to include sufficient details:

- The date of each check.
- Details of the documents used to identify individuals, passport numbers, etc.
- Detail of when and how the identity was verified; face-to-face meeting etc.
- If a third-party verification is being relied on, evidence of that check.
- Details of who, when and how other checks such as PEP and Sanction checks were conducted and records of results.

The Client /Matter Risk Assessment should detail the dates and amounts of all transactions relating to the matter, what checks were undertaken, when and by whom and the results of those checks. The level of detail here will be dependent on the level of risk associated with the transaction but should always provide more detail than: *'A source of funds check was undertaken'.*

If you do not provide sufficient evidence we are not able to confirm that adequate checks have been made and would have to assess such records as non-compliant.

6.1.4 Additional sources of information

Section 6.17 Legal Sector Affinity Group - Anti-Money Laundering Guidance for the Legal Sector 2023 provides further information on 'Source of Funds' and the necessary checks.

6.2 Training

The effective implementation and maintenance of any compliance system is dependent on the training provided to those individuals setting up and running that system and those relating to money laundering, terrorist financing and proliferation financing.

In this section we look at what constitutes suitable training, who should receive it and the frequency of such training. We will also look at how records of training should be maintained.

6.2.1 Requirements of the legislation / CILEX Code of Conduct

Money Laundering Regulations (MLR)

For those firms falling within the scope of the MLR, Regulation 24(1)(a) requires the firm:

- to make relevant staff aware of the law relating to money laundering and terrorist financing and proliferation financing and the requirements of relevant data protection.
- to provide regular training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering, terrorist financing and proliferation financing.

Regulation 24(1)(b) requires the firm to maintain a written record of the measures taken under regulation 24(1)(a) and in particular the training given to its relevant employees.

In this requirement a 'relevant employee' is any employee whose role is relevant to maintaining compliance with the Regulations. The definition includes an employee who is capable of contributing to:

- the identification or mitigation of the risk of money laundering, terrorist financing or proliferation financing, or
- the prevention or detection of money laundering, terrorist financing or proliferation financing.

CILEx Regulation Continuous Professional Development (CPD) Regulations

CILEX members and CILEX Authorised Practitioners need to comply with the CILEx Regulation CPD Regulations 2021. Other authorised persons working in the firms we regulate also need to comply with their regulatory bodies CPD requirements.

These regulations define CPD as *'To maintain, improve and extend the skills and qualities necessary for the proper performance of professional and legal duties and compliance required by CILEx Regulation, so far as to ensure confidence in the professionalism and competence of CILEX members and CILEX Practitioners'.*

CILEX members and CILEX Practitioners need to familiarise themselves with the Regulations to check what they need to do. These vary dependent on the grade of membership. CPD activities must cover professional and legal duties and compliance. This supports the requirement in the MLR to have undertaken money laundering and data protection training both of which are important in maintaining the firm's compliance.

Failure to comply with these regulations may be misconduct under the CILEx Code of Conduct.

CILEX Code of Conduct

CILEX members and CILEX Authorised Practitioners must comply with the CILEX Code of Conduct, and in relation to training should ensure compliance with the following principles:

- Principle 5.1 – Maintain a high level of competence in your legal work and ensure that your legal knowledge is current and of a sufficient depth for your role.
- Principle 5.2 – Identify and address any deficiencies in your knowledge or training, or that of your staff, so as to maintain a level of competence and knowledge appropriate to the work and level of responsibility in which you or your staff are engaged.

6.2.2 So what do we require in terms of training?

The MLR sets the requirements for supervised firms in regulation 24 by requiring the training to:

- make relevant staff aware of the law relating to money laundering and terrorist financing and proliferation financing and the requirements of relevant data protection.
- provide regular training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering, terrorist financing and proliferation financing.

All regulated firms should ensure their training covers these requirements. It will also assist them avoid becoming enablers in wider economic crime and ensure they comply with their obligations under the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

Whilst there will be specific courses / training materials that cover these requirements, it is possible to use a range of sources. The important point to ensure that the training is sufficiently detailed covering both the legal requirements as well as the individual's ability to identify and where appropriate deal with incidents.

The training should be tailored to reflect the findings of your firm's Regulation 18 Practice-wide Risk Assessment, the nature of the services being provided and the risks associated with those services. Vital aspects to cover include:

- The legal obligations and offences.
- The 'Red Flag' related to the firm's services.
- The completion of Customer Due Diligence and Enhanced Due Diligence.
- The reporting of suspicious activity.

The training should not focus solely on money laundering. It also needs to capture terrorist financing and proliferation financing as well as the data protection aspects of these offences.

6.2.3 Who should receive training?

All 'relevant employees' as defined in point 6.2.1 above must receive training. You need to ensure that the training is appropriate to the member of staff receiving it and their role in the firm.

Whilst there should be more detailed training for the Money Laundering Reporting Officer (MLRO) or Money Laundering Compliance Officer (MLCO) it is also important that all staff have an understanding of the legal requirements and the firms' systems for detecting and dealing with incidents or suspected of money laundering, terrorist financing and proliferation financing.

6.2.3 What frequency of training is required?

All new staff should receive training on anti-money laundering, terrorist financing and proliferation financing during their induction. This should take place as soon as practicable after they start.

Whilst there are no set frequencies for training, this is an important element of compliance so we expect annual refresher training on AML related issues, backed up at other points by

more in-depth training. CRL would be concerned where a firm has not provided any anti-money laundering, terrorist financing and/or proliferation financing training to staff in the previous two years.

Other triggers for training include:

- Significant changes to the firm's Practice-wide Risk Assessment.
- Changes in the services being provided and the 'Red Flags' associated with those services.
- Changes in legislation or regulatory requirements.
- Changes in staffing or roles within the firm.

Ultimately it will be up to the firm to justify the frequency based on its risk-based approach.

6.2.3 What training records should we keep?

For firms within the scope of the MLR, Regulation 24(1)(b) requires the firm to maintain a written record of the measures taken under regulation 24(1)(a) and in particular the training given to its relevant employees.

There must be a documented record of the training provided, but it does not need to be just for AML, it could record all the firm's training or have separate training logs for each member of staff.

The training log needs to capture the following information for each individual:

- The date they undertook the training.
- Sufficient information to identify the training and how it was delivered, the name of the course, title of article/ webinar, etc.
- Copies of any course materials to evidence the scope of the training.
- Where applicable copies of certificates to evidence completion of the training.

6.2.4 Monitoring compliance.

CRL will normally look at a training log as part of an inspection visit. It also reserves the right to ask for the training log to be submitted at anytime as part of a desk-based review of the firm. So please ensure that it is up to date at all times.

6.2.5 Additional resources

More detail can be found in Section 8 of the Legal Sector Affinity Group Guidance for the Legal Sector 2023.

6.3 Client / Matter Risk Assessments (Regulation 28)

Whilst there will be separate risks relating to the client and those related to the matter these are normally combined into one risk assessment document or one section of the case management system. Your case management system may be different, so you need to know where the information is captured.

6.3.1 Requirements of the legislation

Money Laundering Regulations (MLR)

Alongside the requirements in Regulation 28(2) to identify the client and verify their identity, 28(2)(c) requires the firm to assess, and where appropriate to obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

In assessing the level of risk the firm must take into account (Regulation 28(13)) factors such as:

- The purpose of an account, transaction or business relationship.
- The level of assets to be deposited by the client or the size of the transaction undertaken by the client.
- The regularity and duration of the business relationship.

Regulation 28(16) requires the firm to be able to demonstrate to CRL the extent of the measures it has taken to satisfy its requirements under regulation 28 are appropriate in view of the risks of money laundering terrorist financing or proliferation financing.

6.3.2 What CILEx Regulation expects to see in the Client / Matter Risk Assessment

Each Client / Matter Risk Assessment should be documented either in the case file or in your firm's case management system and at the very minimum cover:

- Evidence flowing from the Customer Due Diligence checks the firm is required to carry out.
- Any other information about the individuals that may make them higher risk.
- Details of checks made on conflict of interest, PEP and sanctioned individuals.
- Details of the source of funds checks that have been undertaken and the findings. And where applicable details on the source of wealth (see above 6.1 Source of Funds).
- Details the assessment of risks identified for individual matters - the nature of the service being provided, how it is being provided, its complexity and the opportunity it might provide for money laundering, terrorist financing or proliferation financing.
- Highlight any potential 'Red Flags' such as, complexity, third-party involvement or unusual circumstances.
- Detail any updates to the risk assessment throughout the matter.
- The overall risk should be given a scoring (High, Medium or Low) so that higher risk matters can be easily identified.

Please remember that where a client / matter is assessed as being at higher risk of money laundering, terrorist financing or proliferation financing, Regulation 33(1) requires Enhanced Due Diligence (EDD) checks, which need to be captured in the Client / Matter Risk assessment detailing the additional checks that have been undertaken.

Just because you deem a matter to be low risk does not mean there should be less information in the risk assessment. You will need to include sufficient information to justify that low risk scoring and show that reasonable checks have been carried out.

The Risk Assessment should detail how any risks identified are being mitigated, and whether in the light of that assessment it is appropriate to proceed with the matter.

6.3.3 Assessment throughout the matter.

The time it takes to complete a legal matter will vary significantly. Some simple matters complete in days but more complex matters take months, if not years. For this reason, it is important that where applicable matters which take longer, the risk assessment is updated throughout the matter. To evidence this, the risk assessment should detail when additional

checks are undertaken, by whom, the date and the outcome. This is particularly important where these change the risk score and initiate the need for Enhanced Due Diligence.

6.3.4 Make sure your Client / Matter Risk Assessments are of a suitable standard

These Risk Assessments are important, as they help you identify potential risks and put the necessary controls in to prevent them. They also demonstrate that you have the necessary systems in place and are applying those systems.

Your Client / Matter Risk assessment must:

- ✓ Be detailed, including the action taken by whom and when.
- ✓ Demonstrate, the checks are appropriate to the risk.
- ✓ Demonstrate that the necessary risk factors have been considered.
- ✓ Detail the overall risk score and define the mitigating action where needed.
- ✓ Show risk assessment reviews and additional checks for longer matters.

Your Client / Matter Risk Assessment must not:

- × Contain bland statements such as 'Check undertaken'.
- × Fail to detail who undertook the check and on what date.
- × Fail to define the overall risk score and the mitigation for any identified risks.
- × Fail to be updated, throughout the life of the matter for longer matters.

6.4 Practice-wide Risk Assessments (Regulation 18)

6.4.1 Requirements from the Legislation

Regulation 18(1) MLR requires the firm to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which the firm is subject.

Regulation 18A MLR requires the firm to also identify and assess the risk of proliferation financing to which the firm is subject.

> Proliferation financing being defined to be: *'The act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of the relevant financial sanctions obligation'*[6].

Whilst Regulation 18A is a separate requirement, it is sensible to incorporate it as part of the production of the Regulation 18(1) risk assessment.

Regulation 18(2)(a) requires that in identifying and assessing the risks of money laundering and terrorist financing the firm must take into account information made available by its supervisory body, CILEx Regulation. This would include:

- The latest available version of the National Risk assessment
- CILEx Regulation's own Sectoral Risk assessment
- And other economic crime information that CILEx Regulation has made available.

[6] Regulation 16A(9) MLR

Alongside this information, the firm is required by Regulation 18(2)(b) to also consider the following risk factors:

- Its customers
- The countries and geographic areas in which it operates
- Its services.
- Its transactions
- Its delivery channels

Whilst the level of detail included in the risk assessment will be dependent on the size of the firm and the nature of its business, Regulation 18(4) requires all firms falling within the scope of the regulations to keep a documentary record of the steps it has taken to identify the risks and of its assessment of those risks. This is referred to in the legal sector as being the 'Practice-wide Risk Assessment'.

Regulation 18(6) goes further and makes it a requirement that the Practice-wide Risk Assessment must be available on to the supervisory authority (CILEx Regulation) on request. It is therefore sensible to combine the Regulation 18(1) and 18(A) requirements in to one Practice-wide Risk Assessment covering the firms risk being subject to money laundering, terrorist financing and proliferation financing.

6.4.2 The need for a documented Practice-wide risk Assessment

Whilst the MLR only apply to law firms falling within the scope of Regulation 11 or 12 of the MLR, CILEx Regulation recommends that all the firms it regulates produce a Practice-wide Risk Assessment. The reason being that by undertaking such a risk assessment they will have a better understanding of their firm's risk of falling victim to money laundering or of becoming an enabler of such crime. The landscape is changing, with sham litigation being used to launder money and fraudulent immigration cases being used for wider economic crime. Therefore, the preparation of a Practice-wide Risk Assessment is a fundamental building block in a firm's preparedness for the prevention of such activity.

You will need to ensure that your Practice-wide Risk Assessment, is marked with the date that it was undertaken. CILEx Regulation would recommend that the Practice-wide Risk Assessment is updated annually.

6.4.3 The steps needed to prepare your firm's Practice-wide Risk Assessment

Step 1: Do your background research

This will involve reviewing the information that CILEx Regulation has made available to you relating to money laundering, terrorist financing or proliferation financing. Some of this will be included in the bulletins it sends out, but also that contained in the money laundering and economic crime pages of the CILEx Regulation website.

We would also encourage you to undertake AML / economic crime refresher training prior to drafting your Practice-wide Risk Assessment, this may provide you with additional information and importantly for supervised firms can be used to support their compliance with the training requirements of Regulation 24 of the MLR.

Step 2: Consider each of the risk factors

Whilst these are listed in Regulation 18(2) and 18A(2) for proliferation financing, we have included some additional points you should consider when reviewing each factor:

Risk factor	There are many points to consider against each risk factor and the list below provides information on some of the key ones to consider:
Its customers	Some clients will have a higher risk profile: • Does the firm deal with PEPs, Sanctioned individuals? • Does it deal with high-net-worth individuals? • Does it have a high proportion of first-time clients? • Does it deal with corporate clients? • Does the firm deal with overseas clients or clients linked to high-risk jurisdictions? • Does the firm deal with clients linked to criminality?
The countries or geographic areas in which it operates	Alongside considering the geographic location of the client, does the firm's work regularly involve matters that see transactions involving other countries. • Does the firm deal with overseas clients? • Does the firm deal with clients linked to or resident in high-risk countries? • Do the matters relate to overseas countries? • Does the matter relate to transactions linked to a tax haven?
Its services	The National Risk Assessment (NRA) produced in 2020 highlighted the increased risk of conveyancing and the work of Trust and Company service providers. These we believe will remain higher level risks when the new NRA is published in 2025, however they are not the only risks, and it is important to note that there are risks relating to services such as civil litigation and immigration. These risks can manifest themselves in the form of sham litigation or fraudulent applications for asylum. And whilst these may be lower-level risks firms providing such services need to ensure they have the mechanisms in place to identify and report such activity.
Its transactions	Here you need to consider whether the firm deals with matters involving complex or high value transactions. These of themselves may not be a problem but they do necessitate the need for greater checks. Key to these will be checks on the source of funds involved in the matter and where necessary the source of wealth of those funding the transactions. Part of the risk assessment of this factor will consider the controls the firm has in place regarding the types of payments it will accept. For example, does the firm have a limit of the amount of any one cash payment? Does it allow payments derived from a source funded through a cryptocurrency transaction? Is the client involved in trade contracts relating to industries the products of which relate to materials that could be used in weapons production?
Its delivery channels	With more firms offering their services remotely through online service provision this factor can offer an increased risk but is one that can be mitigated by adequate due diligence checks. Aspects to consider here are: Does the firm have work referred to it by agents or others. Does it rely on third party verification? Does it allow third parties to pay for a clients services?

6.4.4 Produce an overall risk finding for the firm

The Practice-wide Risk Assessment should result in an overall risk assessment score, high, medium or low, of the firm being subject to money laundering, terrorist financing or proliferation financing. This should highlight any specific aspects that could raise the risk score and detail the mitigation that the firm is putting in place to address them.

6.4.5 Ensuring the risk assessment is updated.

It is vitally important that the firm's Practice-wide Risk Assessment (PWRA) is up to date as this is a key document in guiding its Anti-money Laundering policies and procedures.

CILEx Regulation would recommend that the PWRA is updated annually as part of the firm's refresh of its policies and procedures.

However, if the firm starts to offer new services or changes the way it operates, this will necessitate an early review and redraft of the PWRA.

6.5 Identity and verification checks

6.5.1 Requirements of the legislation

Regulation 27 MLR requires that Customer Due Diligence is carried out when the firm:

a) Establishes a new business relationship.
b) Carries out an occasional transaction that amounts to a transfer of 1,000 euros or more.
c) Suspects money laundering or terrorist financing.
d) Doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

Regulation 28 sets out the standard requirements for Customer Due Diligence:

It requires the firm to:

- Identify the client, unless the identity is known to them and has already been verified by the firm.
- Verify the client's identity unless the client's identity has already been verified by the firm. Where the client is a body corporate this would include all the beneficial owners and additional detail relating to the corporate body.
- Assess, and where appropriate obtain information on the purpose and intended nature of the business relationship or the transaction.

The MLR applies a risk-based approach when it comes to the application of Customer Due Diligence checks:

- Regulation 33 requires Enhanced Customer Due Diligence in certain circumstances including when there is a high risk of money laundering or terrorist financing.
- Regulation 37 allows for Simplified Customer Due Diligence, where the firm's Practice-wide Risk Assessment and the business relationship or transaction presents a low risk of money laundering or terrorist financing. But please remember this doesn't remove the need to comply with the requirements of Regulation 28, it just means the firm can uses a measures approach in applying the due diligence.

Please remember that under Regulation 31 if it has not been possible to apply customer due diligence, the firm must not carry out the transaction or establish a business relationship with the client and must terminate any existing business relationship with the client.

It is also important to note that Customer Due Diligence is not just an activity that takes place at the start of a client matter. Regulation 28(11) requires ongoing monitoring of the business relationship, and this will be particularly important in delivery of longer and more complex matters. This ongoing monitoring along with the initial customer due diligence checks must be captured in the Client / Matter Risk Assessment.

6.5.2 Which firms should carry out CDD

CILEx Regulation recognises that it regulates firms that fall outside the scope of the MLR because they do not provide services that involve transactional matters, do not provide tax advice and do not provide trust and company service activities.

However, CILEx Regulation expects all the firms it regulates to undertake due diligence checks. Other services, even services such as litigation and immigration, can be enable economic crime. Furthermore, these checks are a natural extension of the checks being undertaken to ensure there isn't a conflict of interest and identify whether they are dealing with a Politically Exposed Person or a sanctioned individual. Such checks are also important for establishing whether the work is something the firm believes it can provide.

We expect to see records of Customer Due Diligence checks for all matters with this information included in the Client / Matter Risk Assessment. This will either be a standalone document or a section within the client file of your firm's case management system.

6.5.3 Carrying out the identification and verification element of CDD

It is vitally important that the Customer Due Diligence checks are undertaken at the outset, as Regulation 31 will preclude the firm from carrying out the transaction or establishing a business relationship until the checks have been made.

Deciding who you need to carry out identity checks on.

This will include the client or clients. Where a client is represented by an agent, intermediary, or representative you are required to comply with Regulation 28(10), not only by checking the agent's identity but also by ensuring they have the authority to act on behalf of the client.

Where the client is a corporate body, the firm will need to identify the beneficial owners of the company.

Establishing an identity

The first stage in the process is identifying the individual. This is normally achieved by requiring the individual to provide identity documents or certified copies of identification documents, where you are not provided with the original documents.

This should include reliable source of such information. Ideally one photographic identity document such as a current passport or driver's licence. And at least one other document such as a council tax statement, utility bill, bank statement etc to check the address information. But please ensure the documents provided are up to date.

There may be occasions where such documents are not available, such as when a client is in a care home. However, remember this is a risk-based approach so a letter from the care home confirming the individual's identity may be all that is needed.

Electronic verification is a facility used by an increasing number of firms as it can be more convenient for the client, particularly when the services of the law firm are being provided remotely. The service is provided online by a third party established to undertake such identity checks, and there are many now providing this service.

Whilst we don't recommend any specific providers, the following organisations are just some of those provide this service:

- Amquis – https://amquis.co
- Compliance Assist – https://complianceassist.co.uk
- Credas – https://credas
- GBG – https://www.gbgplc.com
- Ondato – https://ondato.com
- SmartSearch – https://smartsearch.com
- Veriff – https://www.veriff.com

Such electronic verification services often have the added benefit of being able to carry out both PEP and sanctions checks, both of which can be time consuming without the use of sophisticated database analysis.

Verifying the identity

Obtaining the identity documents or receiving the electronic check is the first step to also verifying that this identity links to the person the firm is actually dealing with. This is relatively straightforward as in most cases the photographic identity can be checked either by a home visit, office meeting or more usually now by a Teams / FaceTime call.

6.5.4 Making a record of the identity check and its verification

Regulation 28(16) of the MLR makes it a requirement for the firm to be able to demonstrate to CILEx Regulation that it has undertaken the necessary due diligence. This is achieved by providing sufficient detail in the Client /Matter Risk Assessment recorded either in a standalone document or in the firm's electronic case management system.

This needs to be more than a tick box. The record must include details of when, how and by whom the checks were undertaken, referencing the documents supplied or linking to the electronic verification document.

The risk assessment must show that reasonable checks have been made, detail who undertook those checks and when and indicate what risks have been identified or explain why the risk is assessed as low.