



CLC AML Sector Risk Assessment

The CLC is obliged, under Regulation 17 of the 2017 AML Regulations, to conduct a risk assessment of its own sector regarding the international and domestic risks of money laundering and terrorist financing. This risk assessment sets out the main money laundering risks that we consider relevant to those we supervise.

Money laundering is the process of concealing the origin, ownership or destination of illegally or dishonestly-obtained money by hiding it within legitimate economic activities in order to make it appear legal. The impact of money laundering is significant as it, “...underpins and enables most forms of organised crime, allowing crime groups to further their operations and conceal their assets”. The NCA has stated that there could be hundreds of billions of pounds laundered in the UK annually¹.

Preventing money laundering can remove criminals' incentives to traffic weapons, trade drugs or engage in human trafficking, and helps to reduce corruption to create a better, safer society.

Conveyancing is a common method for disposing of or converting criminal proceeds due to criminals being able to launder large amounts of money in a single transaction. Probate services (including estate administration and related work) and trusts may also be utilised for money laundering purposes and could be vehicles to disguise assets derived from the proceeds of crime.

What is the CLC's role?

The CLC is responsible for the supervision of its regulated community's compliance with AML Regulations and the relevant CLC codes and standards. We work to identify those who may willingly help money launderers, and inform and educate those who might be unwittingly used by criminals. This AML risk assessment is updated as required to ensure it takes into account emerging risks and trends.

To comply with the legal obligations contained in the [Proceeds of Crime Act 2002](#), the [Terrorism Act 2000](#) and the [2017 AML Regulations](#)² (as amended) (MLRs), CLC regulated persons should have regard to the specific outcomes under the [CLC Code of Conduct](#) outcome 1(m) and the [CLC anti-money laundering and combating terrorist financing code](#) and [guidance](#). CLC Practices should also make use of the resources in the [CLC AML Toolkit](#), including the Treasury-approved Legal Sector Affinity Group AML Guidance.

Who needs to consider this risk assessment?

The MLRs place obligations on CLC Practices to take appropriate steps to identify and assess their risk of being used for money laundering or terrorist financing.

CLC Practices are required to carry out a written practice-wide risk assessment to identify and assess not only the risk of money laundering and terrorist financing but also to assess the risk of proliferation financing³. This should be updated at least every year and also whenever significant developments

¹ NCA National Strategic Assessment of Serious and Organised Crime 2020, p 54.

² As amended by the MLRs 2019 (The Fifth Money Laundering Directive [5MLD])

³ This requirement has been introduced by the Money Laundering and Terrorist Financing (Amendment) (No. 2)

occur (such as new AML legislation or a change in the practice's services being offered).

When practices develop their own risk assessments, they must, under Regulation 18(2)(a), take into account the risks contained in this sector risk assessment, the [National Risk Assessment](#) and knowledge of their services, clients and service delivery. We have produced a summary of the areas of the National Risk Assessment that are most relevant to CLC Practices which you can find [here](#).

Practices must also have written policies, controls and procedures that enable effective management, monitoring and mitigation of the risks that have been identified. Client and matter risk assessments are also necessary to understand the risk arising in each individual matter and determine the extent of client due diligence. The CLC has produced a template matter risk assessment which can be found here in the [CLC AML Toolkit](#).

Risk-based approach

The MLRs require you to take a risk-based approach to detecting and preventing money laundering. This means focussing resources on the areas that are most at risk of money laundering and undertaking not only a practice wide risk assessment but also client and matter risk assessments as practices must, under Regulation 28(12), ensure that their due diligence measures, "...reflect...(ii) its assessment of the level of risk arising in any particular case."

With respect to client/matter risk assessments CLC practices are expected to ensure that these risk assessments, which must be recorded, take into account relevant factors, reflect the findings of your practice wide risk assessment and come to a conclusion as to risk rating. The level of risk arising in any particular matter will determine what level of due diligence you undertake and it is recommended to conduct risk assessments not only at the outset at the transaction but also during the transaction as well.

The CLC takes a risk-based approach to supervision and targets resources at those practices considered to be higher risk which is informed by a variety of sources. This risk assessment will also take into account emerging risks such as new funding technologies (such as cryptocurrency) and proliferation financing.

Red flags/alerts

It is important to be aware of, and act properly upon, red flag indicators that a transaction may be suspicious. One red flag may provide a basis for making further enquiries of your client. Several red flag indicators together, without reasonable explanation, are more likely to provide grounds for suspicion.

You should consider which circumstances in your experience are unusual. If further enquiries do not satisfy your suspicions, you should refer the matter to your practice's Money Laundering Reporting Officer (MLRO) who will decide whether a SAR needs to be filed with the NCA.

We have published two documents which give information on red flag indicators. The lists are not intended to be a tick-list nor to be exhaustive but they may help you to consider which circumstances in your experience are unusual.

The first document outlines some of the [high level AML red flag indicators](#) as identified by the [Financial Action Taskforce](#) (FATF). The second document provides more detailed [warning signs that you may come across in conveyancing transactions](#).

National Risk Assessment 2020

The National Risk Assessment 2020 states that professional services are a crucial gateway for criminals looking to disguise the origin of their funds. The report notes that legal services, like banking and accountancy services, remain at high risk of being abused by money launderers and suggests that high-end money laundering almost always requires facilitation by legal services, even if they are unwitting.

The identification of a sector as 'high risk' means that those working in that sector *'should be vigilant towards the persistent efforts of criminals and terrorists to exploit...vulnerabilities'*.

The National Risk Assessment specifically highlights the following services to be at high risk of money laundering:

- Conveyancing
- Operation of a client account
- Trust and company service providers

To mitigate risks when providing services in these areas, you must make sure that you comply with the latest AML guidance and be aware of red flags that could cause you to have suspicions of money laundering.

We have produced a summary of the areas of the National Risk Assessment that are relevant to CLC Practices which you can find [here](#).

RISK FACTORS

The different types of risk that we consider to be relevant for CLC Practices are:

Product/service (High Risk):

- Conveyancing

Conveyancing, both residential and commercial, is a common method for disposing of or converting criminal proceeds due to being able to launder large amounts of money in a single transaction. Properties can be used to launder money by posing as rental properties to 'wash' illegitimate funds by disguising it as rental income. Remember that criminals also need somewhere to live and carry out their illegal work. Criminals may also use illegitimate monies as large and early repayments on a mortgage.

- Client account

Lawyers' client accounts can be used as a way to make illegal monies seem to have a legitimate source. Client accounts must never be used as a banking facility, or to pass funds through without a legitimate underlying legal transaction. It is good practice to withhold details of your client account until the necessary client due diligence has been completed.

Product/service (Medium risk):

- Trusts and trust related services

The kind of work which CLC practices are involved in under this service include acting or arranging for someone else to act as a trustee in the administration of an estate and/or involvement in the creation and/or management of trusts. Offshore trusts are typically considered to be higher risk and the NCA 2020 identified that whenever trusts are linked to UK criminals, they almost always involve offshore trusts. There is little evidence that UK trusts, by themselves, are used for money laundering and terrorist financing.

The CLC recently undertook a thematic review in the area of TCSPs and concluded, due to weak controls which were identified in some of the practices that participated, that the risk was medium. We would like to emphasise that client/matter risk assessments are expected on all relevant trust matters which are in scope of the AML Regulations. With adequate controls in place the risk of trust and trust related services is likely to be low.

Furthermore, trust assets need to be carefully scrutinised and understood by CLC practices and we would advise that in low to medium risk situations the practice should enquire with the client as to source of the funds (or the source of funds that were used to purchase the asset being placed into trust) and record this on file. In high-risk situations, practices should undertake further checking which may involve obtaining documentation relating to the source of funds such as bank statements or completion statements and ensuring that the client's source of wealth is understood. A comprehensive risk assessment of trusts can be found in the TCSP [thematic review](#).

Product/service (Low Risk):

- Company Service Providers

Corporate structures which enable anonymity can help to disguise the source or destination of money or assets. Law enforcement has stated that many investigations of money laundering involve opaque corporate structures that are used to hide the beneficial owner of assets. This is often used together with other services (in particular the purchase of property) to facilitate money laundering.

The CLC's thematic review into TCSP's identified that CLC practices are rarely involved in company formation however some exceptions were identified: incorporating management companies in freehold developments or forming companies for leaseholders to purchase the freehold through collective enfranchisement.

The CLC's conclusion on both of these kinds of company formation was they were low risk as they were closely linked to property, are non-complex (do not offer anonymity) and set up for a very narrow specific purpose within the UK. The complete risk assessment can be found in the TCSP [thematic review](#).

- Probate and estate administration

Although these services are not explicitly mentioned in the National Risk Assessment (NRA) the CLC recognises that they may still be exploited by money launderers. In particular estate administration involves large amounts of monies coming into regulated client accounts from a range of sources and then being paid out to beneficiaries. These monies are sometimes not checked with the same level of scrutiny as other transactions and there is a risk that they could be given the appearance of legitimacy by going through a practice's client account.

- Remortgage work

Although this service is closely linked with conveyancing, it is considered to represent a lesser risk of money laundering due to the fact that money is typically not required from the client. If there is a shortfall however, meaning that the amount the client is borrowing is not enough to repay the existing lender, then the client will be required to produce additional funds which may increase the risk.

Client risk factors

Each client is different which will be reflected in their individual risk-profiles. There are a number of factors that increase the risk of money laundering presented by clients and beneficial owners, if applicable.

- Politically Exposed Persons (PEPs)

PEPs, both domestic and in the UK, are considered higher risk as they are susceptible to bribery and corruption by virtue of their position which brings them power, influence and access. PEPs and their close families and associates must be identified and enhanced due diligence checks are required to mitigate the risks of corruption. Recent legislative changes permit a lower form of EDD for domestic PEPs vs overseas PEPs which should be carefully considered.

- Clients seeking anonymity or who cannot prove their identity

Clients who seek anonymity on behalf of themselves, a third party or beneficial owner, may be seeking to launder money. In some circumstances a client might legitimately not be able to produce identification documents in which case further investigations should be made. Clients who are evasive about proving their identity or who produce non-standard documentation might be considered higher risk if there is no good explanation for this.

- Duration and nature of client relationships

The CLC's supervisory experience has identified situations where practices have failed to undertake adequate client due diligence when there is a pre-existing business or personal relationship with the client. Assumptions which have been made about a client's source of funds in particular should be challenged robustly and practices must obtain evidence of source of funds in all situations especially when dealing with conveyancing, which is considered to be high risk in terms of AML.

Another relevant factor to consider is whether the practice undertakes high volume work with a high client turnover. This is often the case with conveyancing (as opposed to other boutique or specialist services) and can lead to a superficial understanding of a client's background - which could mean there is a greater inherent AML risk.

- Clients who are involved in high-risk businesses or industries

The LSAG Guidance lists a number of what are considered to be high-risk businesses due to their nature such as cash intensive businesses like taxi firms, restaurants, pubs and others. CLC practices can act for non-natural persons and also may encounter source of funds which are derived from such business activities. The nature of the business should always be taken into account by the practice and fully recognised within the client/matter risk assessment.

Transaction

Practices should be aware of any circumstances about a transaction which appear to be unusual or do not make commercial sense. The use of cash in a transaction suggests a higher risk, and it is a good idea to have a policy on the amount of cash you will accept and in what circumstances.

- Size and value of transaction

Criminals may seek large or high value transactions to launder as much money as possible in one go. If there is no good explanation for an unusually large transaction, or a client is seeking to make a number of linked transactions this may present a higher risk.

- Payment type

Cash and some electronic currencies/cryptocurrencies⁴ can enable anonymity and present significant

⁴ The National Risk Assessment 2020 identified 'cryptoassets' as being at medium risk of being used for money laundering.

challenges in tracing their source⁵. There may be legitimate reasons that a client wants to pay in cash or electronic currency, however this should be considered higher risk because it has not passed through the banking system and is often untraceable.

- Transactions that don't fit with the practice or client's normal pattern

If a new or existing client requests services that aren't usually offered by your practice, you might consider it suspicious if there is no obvious reason for the request.

- Services that facilitate anonymity

Practices should be alert to clients seeking services that enable anonymity and allow beneficial owners to remain hidden without a reasonable explanation.

- New services, delivery methods or technologies

Criminals might target practices moving into new areas, because of the perception that their AML policies and procedures are new and untested. Criminals might also seek to target loopholes in new technology before they are identified and protected.

- Complex transactions

Criminals can use complexity as a way of concealing the source of funds or their ownership. Practices should make sure that they fully understand the purpose and nature of a transaction.

- Red flag transactions

CLC practices should note that the Fifth Money Laundering Directive (5MLD) expanded the situations in which red flag transactions would obligate a practice or firm to undertake Enhanced Due Diligence (EDD). The changes mean that practices must apply EDD where:

- where the transaction is complex
- where the transaction is unusually large or
- where there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose (formerly both conditions had to be satisfied).

Whether a transaction is "complex" or "unusually large" should be considered in relation to the normal conveyancing/probate activity of the practice and also the normal activity of the client.

Previously EDD was necessary only where all of the above elements were satisfied and now only one element needs to be engaged for EDD to be necessary.

This broadens the scope of this particular section considerably and we would advise CLC practices to pay careful regard to this when undertaking matter risk assessments and considering the level of client due diligence to be applied.

- Proliferation financing (Emerging risk)

All CLC practices must ensure that the risk of proliferation financing is risk assessed as part of their PWRA after legislative changes in 2023. Proliferation financing relates to the act of providing funds or financial services for use in the "manufacture, acquisition, development, export, trans-shipment,

⁵ Practices should note that if client due diligence (which includes source of funds) cannot be concluded then the business relationship should be terminated. Practices should also note that some insurance providers may not extend PII cover to transactions involving cryptocurrency so practices should check the insurance position first.

brokering, transport, transfer, stockpiling of or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons.”⁶

The CLC’s view is that conveyancing services, as well as the full range of services which CLC practices offer, is at a low risk of being exposed to such funds however CLC practices are reminded to be wary of funds or clients (both natural and non-natural persons) which may have a link or connection to the weapons trade and be aware that some sectors, such as the insurance sector, shipping/maritime or military/defence, or clients established in countries subject to sanctions may represent an increased risk which should be considered carefully. There are also some particular risks to the UK which should be considered when assessing proliferation financing risks:

1. The ease of establishing companies in the UK – [The National Proliferation Financing risk assessment](#) notes that the ease in setting up a company in the UK may enable key actors to create “front companies to carry out procurement business.” It is crucial that CLC practices are alive to the need to identify beneficial owners under both the AML and sanctions regime when acting for non-natural clients.
2. The role of cryptocurrencies in facilitating proliferation financing – the risk assessment also highlights that certain state actors connected to sanctioned countries such as North Korea or Iran may exploit cryptocurrency. A recent estimate has put the amount of virtual assets stolen by North Korea alone to be in the region of \$300 million.

Delivery channel

- Remote clients

Not seeing a client face-to-face (or engaging with them only through intermediaries) increases the risk of identity fraud and may help facilitate anonymity. The risk posed by remote clients can be mitigated by the use of safeguards such as electronic signatures and e-verification. You should consider using an electronic identity system that provides you with an adequate level of assurance that the client is who they say they are. This is particularly important as remote working and transactions become more common. It should also be noted that 5MLD introduced additional high-risk factors (when considering whether to apply EDD) and one of them was “whether the firm operates without face to face meeting and without electronic identity systems to mitigate this”.

- Payments to or from third parties

Criminals may seek to disguise the source of funds by third parties making or receiving payments. This is a way of disguising assets and practices should make sure the source of funds and source of wealth are identified and verified with no gaps. There may be legitimate reasons for third party payments, for example parents gifting a house deposit to their child. You should ensure you carry out appropriate due diligence on the source of funds and wealth (and retain appropriate evidence on file as you would for a client) and the reason for the payment before accepting funds.

Geographical

- Location of client and beneficial owners

If clients, beneficial owners or third parties are based outside of the UK, you should consider applying enhanced due diligence measures, especially if dealing with countries with significant levels of corruption or other criminal activity, such as terrorism. EDD is mandated for certain countries on the UK’s list of high risk third countries which can be found on the [FATF website](#) (the “grey” and “black” lists). This list is updated at every FATF plenary meeting.

⁶ LSAG Guidance: page 33

Emerging risks:

- In addition to new technologies and proliferation financing, the CLC would also like to highlight the risks associated with Electronic Money Institutions (EMI's) which are becoming an increasingly common way for payments to be made and received and offer an alternative to more traditional banks. CLC practices should be aware that in 2019/20 almost a third of all SARs relating to suspected criminal funds came from the electronic payment sector which EMI's are a large part of. CLC practices should always carefully consider SOF and SOW in transactions – payments from one of the UK's 260 EMI's should be carefully scrutinised.

Next steps/available resources

We will regularly review this risk assessment, taking into account new information from government, law enforcement and our regulatory regime.

This report should be considered when practices are developing their own risk assessments under Regulation 18(1) MLR 2017 along with the National Risk Assessment 2020 and knowledge of their services, clients and delivery channels.

You should also consider the descriptions of risks and mitigations in the HMT-approved Legal Sector Affinity Group's AML Guidance when writing your own practice-wide risk assessment.

We review practices' written risk assessments as part of our routine monitoring and inspections, or in response to specific information we receive.

Last reviewed: March 2024