Solicitors Regulation Authority

Risk assessment

Sectoral Risk Assessment - Anti-money laundering and terrorist financing

Updated 31 July 2025

Background

Money laundering is the means by which criminals make the proceeds of crime appear legitimate. By preventing money laundering, we remove the financial motivation for criminals to engage in acquisitive offences such as drug trafficking and human trafficking—crimes that often disproportionately harm vulnerable individuals. This, in turn, helps to reduce overall crime and contributes to building a better, safer society for everyone.

The funding of terrorism can also be facilitated by the same weak controls that allow money laundering to take place.

We are responsible for the supervision of authorised firms for their anti-money laundering (AML) compliance, and we take our responsibilities very seriously. We have a responsibility to society as a whole to uphold the integrity of the legal profession by addressing both deliberate and inadvertent facilitators of money laundering.

Open all [#]

What is the purpose of this document?

The UK Government periodically undertakes a National Risk Assessment [https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2025] pulling together risk-based information from all sectors in scope of the AML requirements, law enforcement and other sources. Drawing on this, and in order to fulfil our duties under Regulation 17 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) ('the Regulations'), we also produce a risk assessment of our supervised sector. This is to help firms to better assess the risks they are exposed to.

A risk-based approach is embedded in UK legislation and AML best practice. It means that firms should assess their risks and target their resources to the areas or products that are most likely to be used to launder money. Similarly, we take a risk-based approach to directing our resources, focusing effort most on supervising the firms that are most likely to be used to launder money.

Under Regulation 18(2)(a), firms must take our sectoral risk assessment into account when drafting their own firm-wide risk assessment (FWRA). This sectoral risk assessment is not a substitute for a FWRA, which firms are obliged to draft and maintain themselves under Regulation 18.

We ask to see FWRAs and policies, procedures and controls as part of our proactive supervision programme, or in response to specific information we have received. Your FWRA should not be disclosed to customers, or third parties, because it may be useful to those who are seeking to launder money.

This document sets out information on money laundering, terrorist financing and proliferation financing risk that we consider most relevant for firms we supervise.

We will continue to refresh this sectoral risk assessment on a regular basis to keep up to date with emerging risks and trends.

Who does it apply to?

The Regulations place obligations on firms offering services that are most likely to be targeted by those wishing to launder money.

These include independent legal professionals, tax advisers and trust or company service providers as defined in the Regulations.

What to do with this information

All firms that are within scope of the Regulations must comply with all the regulatory requirements. This includes taking appropriate steps to identify, assess and maintain a written record of their risk of being used for money laundering or terrorist financing.

Firms must have regard to this risk assessment, and any updates, when creating and maintaining their own written risk assessment as required by Regulations 18 and 18A of the Regulations, along with a comprehensive knowledge of their business and clients.

We may ask to see your firm's risk assessment.

Emerging Risks

Capital flight from high-risk countries

Firms should remain aware of current world events which may present emerging risk, such as autocratic regime changes in countries which are recognised as being high-risk for money laundering, as well as other financial crimes such as bribery and corruption.

For example, information suggests the collapse of the Sheikh Hasina regime in Bangladesh has led to an exodus of politically exposed persons (PEPs) who may have purchased UK property assets with funds illicitly taken from the country. The money may have been transferred out of Bangladesh using informal value transfer systems such as hawala, also known as hundi, or via various international banking routes before reaching the UK.

Firms who deal with clients or funding from countries that may present a heightened risk, particularly those whose regimes have changed or are unstable, should make sure that:

- they run stringent checks on clients who are PEPs or may be connected to PEPs
- client due diligence is consistent, e.g. that the source of funds makes sense for a proposed property purchase
- sources and origins of funds and wealth are properly evidenced and match the value of assets being transferred.

The use of offshore companies or accounts may be used to try and conceal or obscure true beneficial ownership or origins of funding therefore robust enhanced due diligence checks clients as well as any associated parties must be a consideration.

Client account issues

We have noted an increase in poor client account practice recently. These are not necessarily indicative of money laundering itself, but could potentially facilitate it, intentionally or otherwise. This includes:

- using client accounts as a banking facility in breach of Accounts Rule 3.3 [https://upgrade.sra.org.uk/solicitors/guidance/improper-client-account-banking-facility/] , which naturally involves the risk of its origin being obscured
- retaining client funds for longer than is necessary, in breach of Accounts Rule 2.5, which could involve these monies being put to the wrong purposes
- incorrectly recording funds on client ledgers, eg cash purchase funds being described as a mortgage.

Poor CDD scrutiny

We have noted a number of matters where firms have gathered client due diligence (CDD) but failed to properly scrutinise it. If they had, they would have noticed various mismatches between what the client was telling them and what the evidence showed. Examples of this include:

- the client's appearance and age not matching the photo ID they had supplied, in one case by several decades
- the client telling the firm that purchase monies came from their salary, but this not being backed up by the payslips supplied
- a superficial reading of the source of funds of third-party funders

- over-reliance on e-verification leading to high-risk clients not being identified as such, despite indicators being present.

These examples illustrate that, in order to be effective, due diligence at any level must not only be collected but analysed.

A particular incident involved due diligence being signed off by the fee earner, partner and MLCO, but missing multiple issues of concern which were not identified or analysed. This demonstrates how diffusion of responsibility can lead to risks being missed. Every person in the process apparently thought than another person was responsible for scrutinising the documents. Firms should encourage all of their fee earners and management to see AML as their own responsibility.

Changing firm business models

We have noted an increase post-Covid in firms operating as a network of consultants with their own practices. In these cases, the consultant operates semi-independently, with their own caseload, with the benefit of the firm's systems and resources. Often the consultant lives and works some distance from the firm, and attends their offices for occasional client meetings.

These firm structures can be of benefit to firms and solicitors, but their decentralised nature can carry risks. We have noted that it is sometimes difficult for these firms to keep a central AML policy in operation, to monitor compliance, and to ensure a consistent standard across the firm. MLCOs and MLROs in these firms will need to be more vigilant and potentially more interventionist in order to make sure that the firm is not put at risk by non-compliance. Firms should also check the level of AML knowledge of new entrants to the firm and undertake training where needed. A new consultant who previously occupied a partnership role may, for example, be unfamiliar with AML processes because these were delegated to other staff.

Technology

There are similar risks in the use of new types of financial technology, for example, fund transfer systems and crowdfunding platforms. Any use of new technologies should be preceded by an assessment of the risks they may introduce and effective mitigation of these risks where possible.

We have not so far seen any evidence of the use of deepfake technology to impersonate legitimate clients. Firms should nonetheless remain alert to the potential of this new use of artificial intelligence.

This greater use of technology in all respects also heightens the importance of cyber security. Cyber security breaches could allow criminals to gain total access to both clients' sensitive data and the firm's systems, allowing them to be used for laundering money. Recently, a cyber attack involved all users of a particular case management system, affecting large numbers of firms. You can find a range of cyber security resources here [https://upgrade.sra.org.uk/solicitors/resources/cybercrime/] .

Global economic uncertainty pressures

A continuing issue which is of growing importance is the issue of sufficient resourcing of AML work. As economic conditions have continued to deteriorate and uncertainty has increased, firms are likely to be under pressure to reduce costs, and elements of businesses that are not directly revenue generating may see their budgets reduced.

Whatever decisions are made about resourcing, economic conditions do not change the requirement to comply with the Regulations. They remain a legal obligation which applies regardless of budget.

In fact, the economic conditions are more likely to increase a firm's exposure to would-be money launderers, emboldened by a perception that they are in a position of relative strength in dealing with firms. Potential clients may seek to emphasise the amount of revenue they can bring to a firm as a bargaining tactic. Poorly-resourced AML systems, or staff under pressure due to diminished headcount, could also create weak points in a firm's AML protections.

Observations from our proactive supervision work

As a part of our duties as an AML supervisor, we have been reviewing the compliance of firms we supervise, including reviewing FWRAs, policies, controls and procedures and client files. We publish our findings from recent inspections annually in the autumn.

We have published several other pieces of guidance and supporting information, also informed by this proactive work:

- warning notices on:
  - money laundering and terrorist financing [https://upgrade.sra.org.uk/solicitors/guidance/money-laundering-terrorist-financing/]
  - suspicious activity reports [https://upgrade.sra.org.uk/solicitors/guidance/money-laundering-terrorist-financing-suspicious-activity-reports/]
  - firm-wide risk assessments [https://upgrade.sra.org.uk/solicitors/guidance/compliance-money-laundering-regulations-firm-risk-assessment/]
  - client and matter risk assessments [https://upgrade.sra.org.uk/solicitors/guidance/client-and-matter-risk-assessments/]
  - sham litigation [https://upgrade.sra.org.uk/solicitors/guidance/sham-litigation/] .
- an AML topic guide [https://www.sra.org.uk/sra/corporate-strategy/sub-strategies/enforcement-practice/anti-money-laundering/] which informs our approach to enforcement
- guidance for AML officers [https://upgrade.sra.org.uk/sra/research-publications/money-laundering-governance-three-pillars-of-success/]
- guidance on sanctions [https://upgrade.sra.org.uk/solicitors/guidance/financial-sanctions-regime/]
- guidance on firm-wide risk assessments [https://upgrade.sra.org.uk/solicitors/guidance/firm-risk-assessments/] and client and matter risk assessments [https://upgrade.sra.org.uk/sra/research-publications/client-matter-risk-assessments/]
- guidance on AML training [https://upgrade.sra.org.uk/sra/research-publications/thematic-review-aml-training/] .

Weak controls

Inadvertent failures and gaps in a firm's AML compliance can introduce real and dangerous vulnerabilities into their ability to protect themselves from would-be money launderers.

For example, weak screening controls put firms at risk of being used or infiltrated by organised crime gangs. Individuals posing as solicitors, or solicitors that are being controlled by criminal elements, can use the structures of a firm (particularly the client account) to provide a veil of legitimacy to the proceeds of crime.

The most common weaknesses we have observed included inadequate:

- source of funds checks
- independent audits
- screening of staff and
- matter risk assessments.

We have also observed that while larger firms may have greater resources to protect them from money laundering risks, they will often silo off risk-based information in a compliance team or system. This can mean that those working on a file may:

- lack ready access to the underlying risk assessment and due diligence documentation and information and
- be prevented from conducting effective ongoing monitoring of risk.

Firms should remain vigilant and make sure their policies, controls and procedures adequately protect the firm against the risk of money laundering and terrorist financing.

Developing a culture of compliance is vital. Firms' outcomes are improved if staff understand the reasons for preventing economic crime, and their role in doing so, rather than seeing it as the job of a compliance team or an AML officer. Importantly, comprehensive and relevant AML training leads to better regulatory outcomes for firms.

Politically Exposed Persons (PEPs) and higher risk jurisdictions

We have found that some firms are potentially taking an overly simplistic approach to risks associated with PEPs and higher risk jurisdictions.

The UK economy is highly integrated with the rest of the world, and services offered in the UK are attractive to those in high risk jurisdictions who wish to make the proceeds of crime seem legitimate. A blanket assumption that PEPs would not instruct your firm, or that your firm would never accept instructions from a PEP, is not a sufficient protection against the risks they present. Neither approach would itself satisfy the requirement at Regulation 35(1) to have measures in place to identify PEPs.

It is for firms to decide their own risk appetite, but their policies should be realistic. With the proper policies, controls and procedures, there is nothing to prevent a firm taking on PEP clients. If a firm has an overly restrictive PEP policy, it is at risk of:

- turning away clients for no good reason, restricting access to legal services
- being counter-productive if the firm has a policy which is ignored or routinely breached.

From 10 January 2024 the way in which domestic PEPs should be treated has changed. Domestic PEPs are now defined as those PEPs entrusted with prominent public functions by the UK, and are subject to a different level of risk assessment and enhanced due diligence (EDD). The difference is as follows:

- The starting point for the assessment is that the customer or potential customer presents a lower level of risk than a non-domestic PEP.
- If no enhanced risk factors are present, the extent of EDD measures to be applied in relation to that customer or potential customer is less than the extent to be applied in the case of a non-domestic PEP.

While domestic PEPs may now be subjected to a lower level of EDD than other PEPs, it remains EDD. It must be at a higher level than the CDD you usually apply, and include the measures specified at Regulation 33(5).

It is also important to note that PEPs may instruct a variety of firms, not just those that are large and high-profile. In our proactive work, we noted that PEPs are equally likely to instruct small firms and sole practitioners.

External support

Many firms engage external advice to meet their compliance requirements. In most cases, this is a helpful resource. Some firms, however, rely too heavily on external consultants or systems.

This can include:

- Unsuitable use of templates for risk assessments, failing to take the firm's individual circumstances into account.
- Using electronic identification and verification systems without understanding the underlying processes or their limitations.
- Assuming that because an e-verification check has cleared a client, no further checks or due diligence are needed.
- Using external consultants to draft their compliance documents who do not have an in depth understanding of the work of the firm.
- Using external consultants who have limited knowledge of the legal profession.

While seeking external help with your compliance can be of benefit, the firm itself is in the best position to understand its own risks and design and implement effective mitigation.

You should consider whether the person who is carrying out the audit is sufficiently independent and removed from authorship of the firm's risk assessments and policies, controls and procedures.

It is also important to note that the obligations under the MLR 2017 apply to the firm and cannot be outsourced. The same can be said for the individual responsibilities held by a firm's MLCO, MLRO and beneficial owners, operators and managers under the Regulations.

Firms should also exercise caution when relying on accreditation schemes to fulfil AML obligations such as independent audit (where applicable due to firm size and nature) under regulation 21. In particular, firms should check whether the scheme is intended to provide this kind of assurance. We have, for example, noted that the remit of some schemes only runs to checking that an AML policy exists rather than checking that it is compliant. Likewise, the

training modules of some schemes are geared towards a particular part of the firm or its work, neglecting other key roles.

Firms should remember that audit functions under regulation 21 must:

i. examine and evaluate the adequacy and effectiveness of the firm's AML policies, controls and procedures
ii. make recommendations in relation to those policies, controls, and procedures
iii. monitor the firm's compliance with those recommendations.

'Effectiveness' in particular implies that some form of file review is needed to assess whether the policies are being followed and are serving the intended purpose.

Risk in the legal sector

The 2025 National Risk Assessment [https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2025] says at 5.193-5.196:

The money laundering risk for the sector is assessed to have remained high with no significant change in vulnerabilities since 2020. Criminals are often drawn to legal service providers due to the veneer of legitimacy legal professionals can offer due to perceptions of the sector's integrity. The nature of the services offered, and the volumes of money that can be moved through them also contribute to the sector vulnerabilities, although the speed of transfer can often be slower than in some other regulated sectors. Non-compliance levels remain relatively low across the sector, but the vulnerabilities the sector is exposed to and the scale of money laundering involving the legal sector have also remained high since 2020.

Vulnerabilities

The 2020 NRA judged that the services most at risk of abuse for money laundering purposes were conveyancing, trust or company services and misuse and exploitation client accounts. These continue to be assessed as the highest risk services and more details on these areas are below.

Legal Service Providers that offer a combination of legal services, such as solicitors, are at the greatest risk in the legal sector. […]

Criminals may use a combination of legal services to frustrate due diligence efforts and complicate transactions. Whilst criminals typically seek to use a single lawyer or firm, ultra-high-net worth criminals wishing to avoid scrutiny may employ the services of several firms. This can make it more difficult for a single LSP to identify illicit activity, particularly where inadequate source of funds checks are performed.

The NRA goes on to highlight how a lack of focus on compliance, taking a tick-box approach or a lack of understanding of risk in firms, leads to a higher risk of being exploited by criminals.

The NRA rated the legal sector as being low risk of being used for terrorist financing.

The NRA contains more detailed sections on Property, Companies & Trusts, and Professional Enablers. Firms should familiarise themselves with those sections when preparing their FWRA.

Supply chain risk

Where you are working alongside other professionals, or on one aspect of a wider legal matter, you should also consider supply chain risk.

A supply chain refers to the end-to-end activities/actions involved in the provision of a service/product to the end customer or beneficiary.

A simple supply chain could involve only a few individuals / companies while a more complex supply chain could involve multiple service providers.

Understanding the purpose of the service you are providing and who is ultimately benefiting from it is important in being able to identify and manage any supply chain risks. This could involve making preliminary enquiries of your client to help you understand the purpose of the whole instruction and how your instructions fit into the overall supply chain. If necessary, you

should also look beyond your own instruction to understand the totality of the transaction and identify any risks. This may include taking steps to understand the role of other professionals in the supply chain, eg accountants or company formation agents, and ensuring that these services fit with your understanding.

Proliferation financing

Amendments to the Regulations in 2022 mean that all firms must now carry out an assessment of their exposure to the risk of proliferation financing.

Simply put, this means the risk of the firm being involved with the global proliferation of nuclear, chemical, biological or radiological weapons by groups and countries which are not permitted to have them under international treaty. This includes both materials for weapons, and also 'dual-use goods'. These are goods which are not manufactured as weapons but could be used in weapons or to produce them, for example fertiliser.

We consider the overall risk posed by proliferation financing to the legal profession to be low. In most cases, firms will be able to cover their proliferation financing risk as part of their AML FWRA, given that many of the risk indicators are the same.

There are, however, some sectors which have heightened exposure to proliferation financing, and where we would expect a more thorough risk assessment, either as part of the AML FWRA or as a standalone document. These include:

- trade finance
- commercial contracts
- manufacturing - particularly in relation to dual-use goods
- commodities – particularly mined metals and chemicals
- shipping/maritime
- military/defence
- aviation.

Firms may be of a greater risk where they have exposure to countries which:

- are subject to UN sanctions (for example, Iran or North Korea)
- are suspected of using or seeking to acquire nuclear, chemical, biological or radiological weapons (for example, Syria)
- share a porous border with such countries.

This risk of diversion across borders, where criminals and terrorists may export goods to a border region and then smuggle them to a country subject to sanctions, is one to which firms should be particularly aware.

The Legal Sector Affinity Group guidance [https://upgrade.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf] includes advice on assessing the risk of proliferation finance.

Risk factors

Risk is the likelihood of money laundering or terrorist financing taking place through your firm. Risk in this document refers here to the inherent level of risk before any mitigation – it does not refer to the residual risk that remains after you have put mitigation in place. Risk can exist in isolation, or through a combination of factors that increase or decrease the risk posed by the client or transaction.

The different types of risk factors that we consider to be significant for firms we regulate are set out below. Your firm's risk assessment will need to address all of these.

You should not confuse low frequency with low risk. A firm that conducts three conveyances a year, for example, is likely to be less familiar with the process and have less of an appreciation of current risks than a firm that carries out several every day.

We expect firms to have both:

- a realistic awareness of the risk posed to the profession and to their own business and clients
- systems to manage risk appropriately.

It is important to note, though, that none of these risk factors are prohibitive in and of themselves, nor are they a reason to withdraw from offering these services.

Products and services

We have noticed that firms will often attempt to address risk by highlighting what they do not do. Firms should consider the services they provide and the risk each of them presents.

This may require you to divide services and products into subcategories, in order to draw out high risk elements from lower risk ones. A large amount of solicitors' money laundering risk depends on the services, or combination of services they offer.

Based on our supervisory work and analysis, we have found that the following services pose the highest risk.

Service	Risk
Conveyancing	Property is an attractive asset for criminals because of the large amounts of money that can be laundered through a single transaction, and the fact that property will tend to appreciate, can be used to generate rental income or can be lived in. Solicitors are in a position of trust, and their client account can be viewed as a way of making criminal funds appear to have a legitimate source. Criminals target client accounts as a way of moving money from one individual to another through a trusted third party under the guise of a legal transaction without attracting the attention of law enforcement.
Client Accounts	You must never allow your client account to be used as a banking facility, or to pass funds through it without a legitimate underlying transaction. Firms should be aware of any attempt to pay funds into a client account without a genuine reason, or to get a refund of funds from a client account (particularly to a different account from which the original funds were paid). It is best practice to provide details of your account only when required and not to make them visible (for example by including them in engagement letters). If you hold client money in a third-party managed account [https://upgrade.sra.org.uk/solicitors/guidance/third-party-managed-accounts/] , you should be aware that there are still risks in play.
Third-party managed accounts	You will be less able to monitor the movement of client monies, but under the MLRs the responsibility for any breach would still rest with you. You should also carry out due diligence on the account provider to make sure that they are properly defended against risks such as ransomware and cyber attacks.
Creating or managing trusts and companies	Trusts or corporate structures which can facilitate anonymity can help disguise the source or destination of money or assets. Law enforcement have flagged that many investigations of money laundering lead to opaque corporate structures, used to hide the beneficial ownership of assets. We would regard the following red flags to demonstrate particularly high risk: • any involvement of bearer shares • quick repayment of loans by entities under the client's control • the involvement of an entity type or jurisdiction which may facilitate anonymity • involvement of one or more jurisdictions seemingly unrelated to the matter • use of nominee trustees or shareholders • using pre-existing entities (as opposed to newly formed ones) in an attempt to make a transaction seem more legitimate • using non-business relationships to mask control of an entity, for example, family members.

	Increased knowledge of terrorist methods has raised the terrorism risk of trust or company services from low to medium in the 2025 National Risk Assessment. Legal services overall continue to be assessed as a low terrorism risk. Firms should continue to be vigilant for potential risk in this area.
Tax Advice	Firms need to be aware that while offering certain types of advice and services, there is a higher risk that they may come into contact with the proceeds of crime. One such example would be in offering advice (which includes assistance and material aid as defined at Regulation 11(d)) to a client who is attempting to evade or avoid tax.
Family Offices	Family offices will generally offer a mix of legal (such as tax advice, conveyancing etc), wealth and property management, accountancy and concierge services, often for ultra-high net worth individuals and their families and associates. These may be stand-alone companies, or a service offered alongside others by a company catering to high net-worth individuals, for example an investment bank. Use of these services adds one or more extra layers between the firm and the client and may obscure the origin of funds or assets. Firms must also bear in mind their obligations under regulation 28(10) when dealing with intermediaries such as family offices. In these circumstances firms must: • verify that the intermediary has the authority to act • identify the intermediary • verify the intermediary's identity.

Client risk

Each client is different, and each will have their own particular risk-profile. There are a number of different factors that increase the risk of money laundering presented by clients. Warning signs include clients:

- with an excessive or unreasonable desire for anonymity or privacy
- acting outside their usual pattern of transactions
- whose identity is difficult to verify
- being evasive about providing ID documents
- pressuring you into a certain course of action.

The risk posed by your client also extends to the risk posed by the beneficial owner, if applicable. You need to be confident you know who your client is and why they are asking for your services, and any risk that you do not should be duly considered.

You should also not assume that existing clients are necessarily lower risk. Clients may seek to be onboarded with you for low risk work, and then transition to higher risk work in order to bypass more stringent checks at the point of onboarding.

Existing clients can also present a risk where they have been onboarded in a way that may deviate from your firm's standard practices. Common scenarios include:

- clients onboarded in another firm which has since merged with your own
- clients ported from a foreign branch office, or a company in the same group
- clients onboarded by a consultant or individual who may not be applying the firm's approach consistently.

Effective ongoing monitoring of all clients is the best control against these risks.

Client	Risk
Politically exposed persons (PEPs)	PEPs may be from the UK or abroad. Generally speaking, PEPs may have access to public funds or significant public influence and the Regulations require PEPs and their close family members and associates to be identified and require extra checks to mitigate the risks of corruption.

	The Regulations require firms to be able to identify PEPs and their associates and family members and to undertake enhanced due diligence on them. Onboarded clients may become PEPs over time due to a change in their circumstances which makes effective ongoing monitoring very important. PEPs also retain their status for at least twelve months after leaving the relevant office.
Physical cash intensive sectors or businesses	The nature of the client's business might increase risk if it is cash-intensive (eg take-aways, car washes, nail salons and lessors of residential or commercial property) and therefore presents a greater risk of disguising illegal funds within legitimate payments. The client's sector or area of work is also a significant risk factor, in particular if they are associated with a higher risk of corruption or being used for money laundering, for example those from the arms trade, casinos, or trade in high value items (eg art or precious metals). You should also be vigilant for types of business which are at particular risk of being involved in modern slavery and human trafficking. The NCA has identified [https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file#page=13] businesses such as car washes, nail bars and takeaways as examples of this, as well as live-in factories, care homes and the garment trade. A recent alert [https://www.nationalcrimeagency.gov.uk/who-we-are/publications/655-modern-slavery-in-construction-industry-information/file] also highlights risk in the construction sector.
Familiar clients	Dealing with individuals with whom you, or your staff, may be familiar (such as friends or family) can lead to complacency in assessing and addressing risk and broader compliance with the Regulations. You should seek to account for and appropriately challenge assumptions of the low risk nature of clients with whom you have a non-professional relationship. You should also ensure you are appropriately verifying information you may know (or think you know) about the client and ensure you have done all the checks required. Employees may also pose unique risks as they may be in a position to avoid controls and otherwise use their influence and knowledge to manipulate the firm improperly. This also extends to referrals via trusted third parties. Being referred by someone known to you does not automatically mean a client is legitimate or trustworthy. You should take the same care and apply the same measures as you would for any other client.
Anonymity/cannot prove ID	You should be aware that clients who are seeking anonymity on behalf of themselves, a third party or beneficial owner may be seeking to launder money. You should also be alert to risk regarding clients who are evasive about proving their identity, who produce non-standard documentation or who wish to have undue control over how a service is provided. In some circumstances there may be valid reasons why clients cannot easily provide ID evidence (for example those in care homes), but it is up to you to have processes in place to check that validity in such scenarios.
Intermediaries or agents	It is generally legitimate for a client to expect confidentiality in dealing with their legal representative. Excessive or unreasonable desire for privacy or anonymity, however, should be treated as a warning sign and trigger further scrutiny. While there may be perfectly good reasons for a client to seek to engage with a law firm through an agent or third party, it may make it more difficult to understand who the underlying customer is. Similarly, it creates the risk that the third party or agent does not have the appropriate permission to act on behalf of the customer.

This can also include entities such as family offices, as outlined above.

Regulation 28(10) requires you to identify and verify both the intermediary and the underlying client, as well as obtaining evidence of the intermediary's authority to instruct you.

Transaction risk

There are a number of factors that might make an individual transaction higher risk. Much of the work in identifying risk involves being alert for unusual activity or requests that do not make commercial sense. The use of cash, either as part of a transaction or for payment of fees is inherently higher risk, and firms should have a policy on what amount of cash they will accept, and in what circumstances. You should consider what is normal for your particular firm.

Understanding the source of funds and the source of wealth will help you to manage the risk from a transaction. For the avoidance of doubt, for a source of funds check you should be checking where the customer got the funds from, not just ensuring the funds came from a bank account at a regulated UK financial institution. You should consider the following factors:

What	Why
Size and value of the transaction	Money launderers incur a risk with each transaction, and so 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 presents a higher risk.
Vendor fraud	We continue to see cases of this type, where a fraudster impersonates the vendor of an asset. The conveyancing process is attractive to fraudsters because it provides both the method of committing the fraud and the means of laundering. Once the purchaser has transferred the money into their solicitor's account, and on completion to the supposed seller, the funds have passed through two solicitors firms' client bank accounts making the funds appear to come from a genuine property transaction. However, these funds represent criminal property and are therefore proceeds of crime. Failures in identification and verification make it easier for such frauds to take place.
Cryptocurrency and crypto assets (crypto), including digital assets such as non-fungible tokens	Cryptocurrencies and assets present various risks: • They may facilitate anonymity and obscure the origin of funds. • They are volatile and often subject to sudden and unpredictable changes in value. • Clients may use the opaque nature and volatility of crypto as an explanation for having unusually large amounts of money. This should be clearly evidenced. • The crypto may have been purchased on an unregulated exchange. • The crypto may have been purchased on an exchange operating legally in a jurisdiction with a less stringent AML regime.
Physical cash	Physical cash can facilitate anonymity and enable money laundering. There may be legitimate reasons that a client wants to pay in cash. It is also important to note that being paid into a bank account, even a UK bank account, does not render a sum of physical cash legitimate. Sums deriving from physical cash should undergo the same checks that the original sum would.
Cash purchases of real property	Large sums of ready cash, as opposed to monies raised by a loan or mortgage, should prompt questions about the client's source of funds and potentially of wealth.

	Legitimate sources of funds for these transactions could, for example, be an inheritance, a gift, a lottery win, etc. They should be reasonably simple to prove, and unwillingness to disclose the source of this cash should be considered a warning sign.
	Firms will know where their expertise is and what services they normally provide. In addition, initial client due diligence should include gathering some information on the expected ongoing client relationship and related activities.
Transactions that do not fit the norms of your firm or the client's activity	If a new or existing client is requesting transactions or services that you wouldn't normally expect your firm to offer, you might consider this suspicious if there is no obvious reason for the request.
	Similarly, if a client is requesting services which are not in line with your customer due diligence or are out of their normal pattern of transactions, without a good reason, you should consider whether this constitutes suspicious behaviour.
	Accurate and up-to-date information on beneficial owners is a key factor in preventing financial crime and tracing criminals who try to hide their identity behind corporate structures.
Transactions or products that facilitate anonymity	Firms should be alert to customers seeking products or transactions that could facilitate anonymity and allow beneficial owners to remain hidden without a reasonable explanation.
	This may also apply to transactions which do not involve money or personal property, such as artworks, vessels or aircraft.
New products, delivery mechanisms or technologies	The changing nature of money laundering means that criminals are always seeking new ways to launder funds as old ways become too risky and loopholes are closed. Moving into a new business area or providing a new delivery channel for services means your firm may come across new or previously unidentified risks. In moving into a new area, you will not necessarily have a previous pattern of transactions with which to compare new behaviour that might be suspicious. You should risk assess any such new products, delivery mechanisms or technologies before using them.
Pooled funds and funding platforms	This refers to transactions where a large number of participants, often strangers to each other, contribute to fund the purchase of a property or asset. For example: • Cash gifts given at a wedding. • Crowdfunding to purchase a property. These can be challenging for firms as it may prove difficult to establish the source of funds, particularly where there are numerous separate sums. Without knowing this it is impossible to assess the level of risk involved, or to determine whether any of the money involved has been laundered or is subject to sanctions.
Complex transactions	Criminals can use complexity as a way of obscuring the source of funds or their ownership. Firms should make sure that they fully understand the purpose and nature of a transaction they are being asked to undertake. If your client cannot tell you why the proposed transaction is so complex, for example saying 'tax reasons' without explaining further, this should be treated as a high risk. You should make further enquiries or seek expert help if unsure.

Delivery channel risk

The way in which you deliver your services can increase or reduce risk to the firm.

If you do not meet clients in person, it is inherently more difficult to identify and verify their identity. These risks can be mitigated by the use of effective electronic identification and verification tools.

These tools represent an evolution in the identification and verification capabilities of firms and may be seen as an improvement when compared to some previous common practices such as relying on certified copies of documents.

While they can be valuable in aiding firms to fulfil their AML duties, they may however present risks where they are not fully understood: For example:

- Being used in a way that was not intended. For example, just because a system has stated that a client has 'passed' does not mean no further enquiries are necessary, nor does it obviate the requirement to identify and verify them.
- Assuming that such a system fulfils the requirement to carry out a client/matter risk assessment. These systems may be very helpful in informing the client/matter risk assessment, but cannot do so automatically.
- Those using them are not properly trained in the systems leading to user error.
- Viewing the checks as a one-time exercise and failing to regularly update the checks as part of their ongoing monitoring obligations.

The Financial Action Task Force (FATF) has produced guidance on using these services [https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html] .

Ultimately the firm is responsible for its own compliance, and this responsibility can never be outsourced.

What	Why
Remote clients	Not meeting a client face-to-face can increase the risk of identity fraud and without suitable mitigation such as robust identity verification may help facilitate anonymity. Not meeting face-to-face may make sense in the context of a given transaction or wider context. But where clients appear unnecessarily reluctant or evasive about meeting in person, you should consider whether this is a cause for concern. You should also be aware of the risk posed by AI tools – known as 'Deepfakes' – which can impersonate a real person's appearance convincingly. This increases the risk of relying on video calls to identify and verify your client. If you only meet clients remotely, you should understand whether your electronic due diligence protects you against this, or to explore software solutions to assist in detecting deepfakes.
Combining services	Some services might not be inherently high risk, but when combined with other services or transactions become risky. For example, there might be legitimate reasons for setting up a company, but if that company is used to purchase property and its structure disguises the beneficial owner, this could increase the risk of money laundering. Clients may take steps to hide the combination of services they are using. For example, if a client is enquiring about, or taking advantage of information barriers within firms (for example between branches or practice areas) or allowing a significant amount of time to pass between instructions so they appear unlinked, these should be seen as indicators of risk.
Payments to or from third parties	Launderers can seek to disguise the source of funds by having payments made by or to associates or third parties. This is a way of disguising assets and you should make sure you identify the source of funds and source of wealth to mitigate this risk. A payment to or from a third party is particularly suspicious if it is unexpected, occurs at short notice, or is claimed to have been made in error with a request for the money to be refunded. There may be some legitimate reasons for third party payments, for example parents gifting a house deposit to their child. You should ensure you do appropriate due diligence including checking source of funds before accepting such payments.
Irregular methods of	If a client insists on depositing a sum of money with your firm in portions or tranches, or asks you to transfer sums to them or third parties in a similar way,

transfer	you should investigate further. It may be that the client is transferring these sums in this way to evade AML controls imposed by banks. If the reason given is deposit or withdrawal limits, this should be simple for the client to evidence.

Geographic risk

When assessing geographic risk, you should consider the jurisdiction in which services will be delivered, the location of the client, and that of any beneficial owners or counterparties as well as the source and destination of funds.

In some jurisdictions the sources of money laundering are more common, for example locations where the production of drugs, drugs trafficking, terrorism, corruption, people trafficking or illegal arms dealing more commonly occur.

While countries with anti-money laundering and counter-terrorist financing regimes which are equivalent to the UK may be considered lower risk, you must guard against complacency. There have been major examples of local AML failures with international impacts, in what had been seen previously as low risk jurisdictions.

Below are the key issues to consider regarding geographic risk.

What	Why
Countries that do not have equivalent AML standards to the UK	The Regulations set out that those countries which appear on FATF's lists of countries subject to a call for action [https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2023.html] or increased monitoring [https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html] are high risk third countries, and specific EDD measures must be applied. These lists are not an exhaustive list of all high risk countries (notably omitting Russia, for example), and other higher risk jurisdictions are listed by sources such as the Basel Institute of Governance AML Index [https://www.baselgovernance.org/basel-aml-index] . You should take a cautious approach to deciding whether a country is high risk for the purposes of applying enhanced due diligence. If in doubt about a country, you should consider treating it as higher risk.
Information to which your firm has access	While externally drawn up lists of high-risk countries may be useful, your firm may have access to wider intelligence that may cause you to upgrade the risk posed by a particular client, firm or geographic location. For example, there may be sector specific information you may be more aware of due to your firm's main areas of business. While overall the jurisdiction might be seen as generally low risk, it could still be high risk for your firm. For example, an otherwise low risk EU country, may be worth considering as high risk if there is well-known local criminality in a sector that you may have exposure to.
Local characteristics	A multi-branch firm may have day-to-day exposure to different risks across their various offices or locations. This could mean that what is unusual or a potential risk indicator in one branch is not necessarily the same in others. For example, an office in the City of London may have a greater number of corporate and PEP clients, while a branch in a smaller regional town may have greater exposure to high cash-use businesses, such as restaurants and independent retailers.
Countries with significant levels of corruption	The Regulations require firms to put in place enhanced due diligence measures in dealing with countries with significant levels of corruption or other criminal activity, such as terrorism. Transparency International also produces a corruption perceptions index [http://www.transparency.org] .
Stringent currency controls	China is an example of a country that has significant constraints on its citizens and residents investing or moving capital abroad. This has led to some people

using alternative networks to move wealth out of the country.

Evasion of local currency controls is not an offence under UK law and does not automatically mean that funds are the proceeds of crime.

The informal value transfer systems used, however, often present risks of their own. Legitimately obtained money may be transferred by illegitimate means. Firms must ensure that methods of delivery, as well as the funds themselves, are legitimate.

We have noticed an increase in payments from various third parties being used to fund property purchases, apparently to circumvent these controls. Where this happens, firms should take care to establish the legitimacy of the source of funds from each donor.

LSAG has produced guidance on this subject. [https://upgrade.sra.org.uk/globalassets/documents/sra/research/chinese-funds-ml-lsag-guidance-5-pages-62kb-pdf.pdf?version=493794]

Sanctions risk

The sanctions regime has expanded over the past few years, mainly due to the Russian invasion of Ukraine in 2022. The long-standing involvement of Russian interests and beneficial owners in British business, and vice versa, has meant that many firms have been exposed to the sanctions regime for the first time.

It is important to remember, however, that there are a large number of thematic and geographic sanctions regimes beyond Russia and Belarus. Firms cannot assume that sanctions are not relevant to them. There are a significant number of British nationals subject to sanctions.

In particular the Office for Financial Sanctions Implementation (OFSI) have recently applied sanctions to a domestic neo-Nazi group, Blood & Honour, including under its aliases 28 Radio and Combat 18. The group's assets are now subject to an asset freeze. This further illustrates that sanctions are not only applicable to firms with overseas clients.

The sanctions regime is separate to the proceeds of crime and money laundering regimes, but overlaps with them in many ways:

- It involves many of the same risk factors as money laundering, such as suspect jurisdictions, politically exposed persons (PEPs) and complex corporate structures.
- Sanctions create a motive for wanting to obscure the origin or recipient of funds or assets.
- The ownership and control requirements of the sanctions regime also mean that it is necessary to identify a corporate entity's ultimate beneficial owners and those who control it – who may be different people. This makes it even more important to carry out effective client due diligence (CDD).

We expect the sanctions regime to continue to expand, so all firms should be familiar with the requirements. Sanctioned individuals and businesses are likely to seek to instruct firms with weaker controls.

The sanctions regime is also strict liability and applies to all firms – indeed, to all natural and legal persons in the UK. The sanctions regime therefore poses a risk to all firms, whatever their size, nature or area of work.

Firms involved in aviation, international trade, or shipping should also note the establishment of the Office for Trade Sanctions Implementation (OTSI). This operates in a similar manner to OFSI, but with a different focus.

We have also produced comprehensive guidance on the sanctions regime, [https://upgrade.sra.org.uk/solicitors/guidance/financial-sanctions-regime/] as have OFSI [https://www.gov.uk/government/publications/financial-sanctions-faqs] and OTSI [https://www.gov.uk/government/organisations/office-of-trade-sanctions-implementation] .

The Regulations require firms working in scope to put in place enhanced due diligence measures in dealing with countries subject to sanctions, embargos or similar measures (regulation 33(6)(c)(iii)). In the UK, the Office of Financial Sanctions Implementation maintains a searchable database of designated persons and entities [https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/] . You can

also subscribe to email alerts [https://www.gov.uk/email-signup?link=/government/organisations/office-of-financial-sanctions-implementation] of any changes.

We have been conducting an ongoing programme of sanctions monitoring work since 2022 and have noted some themes. We have not noticed widespread intentional breaches of the sanctions regime. It is far more common for firms to breach the regime by exceeding the boundaries of a general or specific licence, for example by:

- failing to renew the licence in time when work is ongoing
- exceeding the limits of the licence in terms of fees
- failing to meet reporting requirements.

These are generally in line with HM Treasury's Legal Sector Threat Assessment [https://assets.publishing.service.gov.uk/media/67ee635698b3bac1ec299c3e/OFSI_Legal_Services_Threat_Assessment.pdf], which also noted the frequent use of intermediary jurisdictions.

It is also important to note that breaches of the regime can, and do, attract severe penalties. The subsidiary of a large London firm was fined £465,000 in March 2025 [https://ofsi.blog.gov.uk/2025/04/04/hsf-moscow-penalty-key-lessons-for-industry/] due to sanctions breaches in the closure of its Moscow office. The fine was assessed at £930,000, but reduced by 50% due to the firm having made a self-report.

What	Why
Client risk	You should remain vigilant to the possibility of your firm being instructed by a sanctioned entity or individual (a designated person) or an entity owned or controlled by them. A robust and reliable check using the OFSI Consolidated List or a programme derived from it is the best way to tell whether or not the client is a designated person. Ownership and control, however, is a broader concept and is different to ultimate beneficial ownership in the MLRs. If the control of the company is unclear or obscured, or appears to operate contrary to expectations, there is a risk you will unknowingly act for a designated person. Some designated persons are also PEPs, but you should be aware that the two concepts are not interchangeable.
Geographic risk	You should be vigilant for any clients who are established in, or have links with, jurisdictions which have a country regime in place. [https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases] Similarly, you should exercise caution when dealing with entities whose chain of ownership originates from or passes through these jurisdictions. Designated persons also seek to use neighbouring countries to hide their ownership and control of entities and assets. Jurisdictions with a sanctions regime in place are generally widely known, so designated persons may use intermediaries, agents or other third parties to try to circumvent this.
Products & services risk	You should check to see whether there is a ban in place on the products and services you are offering. For example, it is currently prohibited to provide trust services to Russians or persons connected with Russia, unless a licence is in place. We consider that the following areas of work are more exposed to sanctions risk: • trade (imports/exports outside of the UK) • shipping • aviation • immigration. However, it is important to remember that all areas of work may be of interest to designated persons, including those (eg litigation) out of scope of the MLRs.

	The same principles as for AML apply here, and the most risky activities are likely to involve transactions which: • are large • are complex • involve obscure or uncertain sources of funds • involve risky jurisdictions or those with links to them • involve transfers to and from unrelated third parties.
Transaction risk	The NCA has issued alerts on non-monetary assets being used to evade sanctions, including: • a red alert on the use of gold bullion to circumvent sanctions [https://www.nationalcrimeagency.gov.uk/who-we-are/publications/679-necc-red-alert-gold-sanctions-circumvention/file] . Russian gold is being passed through non-sanctioned jurisdictions, melted down, and reconstituted to disguise its origin. • an amber alert on the use of art storage facilities [https://nationalcrimeagency.gov.uk/who-we-are/publications/692-0735-necc-amber-alert-sanctions-evasion-money-laundering-in-the-art-sec/file] . This includes the sale, transfer and storage of art, including at UK freeports. Designated persons may attempt to hide their own true identity, or to obscure their true role.
Delivery channel risk	As with AML, you should make sure that you identify and verify those with whom you deal. Designated persons may use intermediaries, family offices or agents to obscure their involvement in transactions and other matters. You should ensure that the appropriate level of due diligence is carried out on both the principal and intermediary, and that you establish ownership and control of legal persons.

Summary of changes

This sectoral risk assessment was published on 31 July 2025. The major changes from our previous Sectoral Risk Assessment (dated 5 March 2024) are as follows:

- Updated references to, and summary of, the National Risk Assessment.
- Added new emerging risks:
  - capital flight from high-risk countries
  - client account issues
  - poor CDD scrutiny
  - changing firm business models
- Moved the following risks from emerging to new locations, reflecting that they are now part of the risk landscape:
  - vendor fraud
  - proliferation financing
  - supply chain risk.
- Added further updates and context to the Sanctions section, including new designations and penalties imposed.