Risk assessment

Sectoral Risk Assessment - Anti-money laundering and terrorist financing

28 January 2021

Background

Money laundering is the means by which criminals make the proceeds of crime appear legitimate. The National Crime Agency (NCA) believes that serious and organised crime costs the UK £37 billion a year [https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file] . By preventing money laundering, we can take away criminals' incentive to commit acquisitive crimes, for example trading drugs or human trafficking, so many of which particularly impact on the vulnerable. This helps reduce wider crime to create 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 owe a duty to society at large, and to protect the integrity of the legal sector through tackling intentional and inadvertent enablers of money laundering.

Open all [#]

What is the purpose of this document?

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.

The UK Government periodically undertakes a National Risk Assessment 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 in order to help firms to better estimate the risks they are exposed to. Our sectoral risk assessment must be considered as a part of each firm's firm-wide risk assessment.

We ask to see firms' written risk assessments and policies, procedures and controls as part of our proactive supervision programme, or in response to specific information we have received. Your firm's risk assessment 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 and terrorist 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 and 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 the all the requirements of regulations. 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 Regulation 18 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

Covid-19

As a result of the Covid-19 pandemic, the UK economy has entered a period of significant economic disruption. This has potentially left some firms in a vulnerable position, where they might be more likely to become involved in business areas and relationships they would otherwise have avoided. Criminals know this is happening and will be looking to exploit those firms where tolerance to risk has increased. While a culture of AML compliance is now more mature in the legal sector than in the past, any firm without robust policies, controls and procedures (including the accurate assessment of risks at every level) is at risk of exploitation.

Covid-19 has accelerated the trend for firms not meeting clients face to face, which can make it inherently more difficult to identify and verify the identity of these clients. These risks are mitigatable by the use of effective electronic identification and verification tools.

These tools represent an evolution in the identification and verification capabilities of firms and might 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 might however present risks where:

- they are not fully understood,
- they are being used in a way that they are not intended for and
- those using them are not properly trained in the systems leading to user error.

The Financial Action Task Force (FATF) has produced guidance on using these services [http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html] .
Ultimately the firm is responsible for their own compliance, and this responsibility can never be outsourced.

Technology

There are similar risks in the use of new types of financial technology, eg 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.

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 client's sensitive data and the firm's systems, allowing them to be used for laundering money.

Wider economic pressures

A separate issue which is of growing importance is the issue of sufficient resourcing of AML work. Economic conditions have deteriorated and there is much uncertainty for firms. Firms are likely to be under pressure to reduce costs, and elements of businesses that do not directly generate revenue might see their budgets reduced.

Whatever decisions are made about resourcing, firms need to understand that economic conditions do not change the requirement to comply with the regulations. 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.

Legal status of cannabis

With the partial or total decriminalisation of cannabis in some countries overseas, and its increased use in therapeutic settings, how firms handle funds generated through the sale of cannabis has become a greater issue in recent years. This has made it more challenging to draw the boundary between legal and illegal revenue in the UK.

This issue extends to revenue from foreign cannabis businesses (for example in Canada) that while locally legitimate, might technically be the proceeds of crime in the UK according to the definitions in the Proceeds of Crime Act, 2002. Any firms involved in the legitimate cannabis industry need to be fully aware of the legal risks prevalent in this area and the specific restrictions that might be present in the matters they act on.

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 firm risk assessments, policies, controls and procedures and client files. We have published a detailed account of findings [/globalassets/documents/sra/research/anti-money-laundering-aml-visits-2019-2020.pdf?version=4ada2c] from a recent set of visits.

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 [/solicitors/guidance/money-laundering-terrorist-financing/]
  - suspicious activity reports [/solicitors/guidance/money-laundering-terrorist-financing-suspicious-activity-reports/]
  - firm risk assessments [/solicitors/guidance/compliance-money-laundering-regulations-firm-risk-assessment/]
- an AML topic guide [/sra/corporate-strategy/sub-strategies/enforcement-practice/anti-money-laundering/] which informs our approach to enforcement and
- guidance on firm risk assessments [/solicitors/guidance/firm-risk-assessments/] .

Weak controls

While there is a widespread desire to comply with the regulations, often innocent 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, open up firms to the risk of infiltration 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
- matter risk assessments

We have also seen that while larger firms might 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 might:

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

Politically-Exposed Persons (PEPS) and higher risk jurisdictions

We have found that, smaller firms in particular, 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. Simply stating that your firm does not deal with clients like this is not a sufficient protection against the risks they present. It is also important to note that PEPs might also be from the UK, and indeed there are many thousands of PEPs in the UK, who may seek legal services for entirely legitimate reasons.

External support

Finally, we have also seen that firms will often over-rely on external help in order to meet their compliance requirements. This can include:

- unsuitable use of templates for risk assessments
- using electronic identification and verification systems without understanding the underlying processes or their limitations
- using external consultants to draft their compliance documents without an in depth understanding of the work of the firm.

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

Risk in the legal sector

The 2020 national risk assessment said: The risk of abuse of legal services for money laundering purposes remains high overall. Legal service providers (LSPs) offer a wide range of services and 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 national risk assessment 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 national risk assessment rated the legal sector as being low risk of being used for terrorist financing.

The risk assessment identifies several potential emerging issues including:

- sham litigation (ie fake lawsuits between collaborating parties to launder money as payment of damages through the courts)
- use of crypto assets for payments, which while not always automatically suspicious inherently make it harder to identify the beneficial owner and as a result should be treated as high risk
- use of crowdfunding which can make the source of funds extremely difficult to establish

Risk factors

Risk is the likelihood of money laundering or terrorist financing taking place through your firm. Risk refers 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 headings.

None of these risk factors are forbidden in and of themselves, nor are they a reason to withdraw from offering these services. We expect firms to be aware of the risk present, manage it properly and keep themselves and the public safe. Done correctly these are all services that can help meet the legitimate needs of society.

Products and services

We have noticed that firms will often attempt to address risk by highlighting what they do not do. This approach leads to a tick-box mentality to risk and should be avoided. Instead, you should focus on what your firm does do, and from there honestly identify and evaluate all risks present.This might 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.
Client accounts	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. 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

Service	Risk
	account (particularly to a different account from which the original funds were paid). It is a good idea not to make the details of your client account visible (for example by including them in engagement letters) and to provide them only when required.
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 denote scenarios of 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 using pre-existing entities (as opposed to newly formed one) in an attempt to make a transaction seem more legitimate using non-business relationships to mask control of an entity, for example, family members
Tax Advice	Firms need to be aware that while offering certain types 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 per the definition in the regulations) to a client who is attempting to evade or avoid tax. The national risk assessment addresses tax advice directly: ‘The provision of tax advice and acting as an agent with HMRC on behalf of clients provides several means to launder money and poses a high risk.’
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. Firms that act as family offices, either exclusively for one family or for more than one group of clients may be unduly open to influence, due to the more exclusive nature of the relationship.

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:

- appearing to want anonymity
- 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 might seek to engage 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 might 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
- 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 money laundering regulations require PEPs and their close family members and associates to be identified and require extra checks to mitigate the risks of corruption. The money laundering regulations require firms to be able to identify PEPs and their associates and family members and to undertake enhanced due diligence on them. It is also worth highlighting that there have been changes to the regulations regarding who is a PEP and it now includes UK residents. This may mean that onboarded clients previously not considered PEPs, may now be regarded as such. Also onboarded clients may become PEPs over time due to a change in their circumstances which makes effective ongoing monitoring very important.
Cash intensive/risky sectors or businesses	The nature of the client's business might increase risk if it is cash-intensive (eg take-aways and nail salons) 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

Client	Risk
	metals).
Familiar clients	Dealing with individuals with whom you, or your staff, might 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.
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 the elderly or refugees), but it is up to you to have processes in place to check that validity in such scenarios.
Intermediaries or agents	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 will inherently 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.

Transaction risk

There are a number of factors that might make an individual transaction higher risk. Much of identifying risk is being alert for unusual activity or requests that don't 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.

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 might seek large or high-value transactions to launder as much money as possible in one go.

What	Why
	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.
Payment type	Physical cash and cryptocurrencies can facilitate anonymity and enable money laundering. There may be legitimate reasons that a client wants to pay in cash, however this must be considered higher risk because it has not passed through the banking system and is often untraceable. Any use of cryptocurrencies should also be regarded as being of higher risk because they may facilitate anonymity, and the origin of funding is likely to be obscured.
Transactions that don't fit the norms of your firm or the client's activity	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. 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.
Transactions or products that facilitate anonymity	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. 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.
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.
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. 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.

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.

What	Why
	Not meeting face-to-face may make sense in the context of a given transaction or wider context, for example circumstances linked to the Covid-19 pandemic. But where clients appear unnecessarily reluctant or evasive about meeting in person, you should consider whether this is a cause for concern.
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.

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	In 2020, it became a regulatory requirement for clients or counterparties

equivalent AML standards to the UK	What based in the countries on the European Commission's list of high-risk third countries, to be subject to a specified form of enhanced due diligence. The EU Commission list is to be replaced by UK recognition of the FATF grey [https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html] ' and black [http://www.fatf-gafi.org/countries/#high-risk] ' lists for this purpose after the February 2021 FATF Plenary in order to pick up any changes made. These lists are not an exhaustive list of all high-risk countries, and other higher risk jurisdictions are listed by sources such as the Basel Institute of Governance [https://www.baselgovernance.org/basel-aml-index] . There are also information aggregators, like Know Your Country [https://www.knowyourcountry.com/] which combine insights from these resources. You should take an inclusive approach to deciding whether a country is high risk or not, for the purposes of applying enhanced due diligence. If doubt about a country, you should consider treating it as higher risk.
Information your firm has access to	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, you may have 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 might be worth considering as high risk if there is well-known local criminality in a sector that you might have exposure to.
Local characteristics	A multi-branch firm might 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 Politically-Exposed Person 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 money laundering 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 index [http://www.transparency.org/country]
Sanctions	The money laundering regulations require firms to put in place enhanced due diligence measures in dealing with countries subject to sanctions, embargos or similar measures. In the UK, the Office of Financial Sanctions Implementation maintains a list of all those subject to financial sanctions [http://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases] . You can also subscribe to an email alerting you to any changes.
Stringent local capital offshoring controls	China is an example of a country that has significant constraints on its citizens investing or moving capital abroad. This has led to some people using alternative shadow banking networks to move wealth out of the country. These networks usually have a dual purpose of cleaning illicit funds for criminals (while facilitating people to sidestep local capital controls),

What Why	meaning that funds that pass through these networks will generally be the proceeds of crime, even if the client is not themselves a criminal. You may consider such networks as illegal money transfer businesses. Source of funds checks are very important where there is a risk that money has passed through one of these networks. See here a link to the NCA's explanation of how this works [https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file] in China.

We have published more information [/home/hot-topics/cybercrime/] on preventing money laundering and terrorist financing