Solicitors Regulation Authority

Guidance

Guidance

Firm-wide risk assessments

Firm-wide risk assessments

Updated 21 September 2023 (Date first published: 29 October 2019)

Print this page [#] Save as PDF [https://upgrade.sra.org.uk/pdfcentre/?type=Id&data=4014064231]

Status

This guidance is to help you understand your legal and regulatory obligations and how to comply with them. We will have regard to it when exercising our regulatory functions.

Who is this guidance for?

All firms that are subject to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the money laundering regulations).

Purpose of this guidance

This guidance is aimed to help firms subject to the money laundering regulations comply with the requirement to have a firm wide risk assessment under regulation 18.

This guidance is a living document and we will update it from time to time.

Introduction

Firms that are within scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('the money laundering regulations') must have a written firm-wide risk assessment in place.

The requirement to produce a firm risk assessment is set out at regulation 18 of the money laundering regulations. The risk assessment must be appropriate to the size and nature of your business and take into account:

- any take into account information we publish in particular our sectoral risk assessment
- the risk factors set out in the money laundering regulations, namely:
    - your firm's customers
    - the countries or geographic areas in which you operate
    - the products or services which your firm provides
    - your firm's transactions
    - how your firm's products and services are delivered

Regulation 18A of the money laundering regulations also requires you to identify the risk of proliferation financing to your business. This can either be considered separately or within your firm-wide risk assessment. Further guidance on how to carry out a proliferation financing risk assessment can be found in the Legal Sector Affinity Group guidance.

Why is it important to have a firm wide risk assessment?

The purpose of a firm wide risk assessment is to help you identify the money laundering risks your firm is, or could be, exposed to, and consider how any risks could be mitigated. Essentially, it will help your firm to take a risk-based approach to preventing money laundering.

Having a firm wide risk assessment in place will also help you to develop appropriate policies, controls and procedures. Fee earners may also need to refer to your firm wide risk assessment when assessing risk at client and matter level.

It is an important document which should be regularly reviewed, kept up to date and approved by senior management.

What we have seen

As part of our supervisory activities, we review firm wide risk assessments during our inspections to firms and desk-based reviews.

We have found that most firms now have a firm wide risk assessment in place. Over the last few years, we have also seen an improvement in the quality of firm wide risk assessments which reflects the thought, effort and time that many firms put into these documents.

However, we continue to find a significant proportion of firm wide risk assessments which fall short of our expectations.

Most worrying are those firms who only put in place a firm wide risk assessment after we request to see it. The requirement to have a firm wide risk assessment has now been in force since 2017. The purpose of a firm wide risk assessment is help identify the risks a firm is or could be exposed to, and the measures which should then be put in place to help mitigate the firms' exposure to financial crime. It is a crucial step in being able to prevent money laundering. We will continue to take robust action against any firms who do not have a firm wide risk assessment in place.

We also continue to see a minority of firm wide risk assessments which we deem to be non-compliant or partially compliant.

This could be because the firm has failed to consider the information we publish, or consider one or more of the risk factors set out in the money laundering regulations. For example, of the 73 firm wide risk assessments we reviewed during our desk based reviews in 2021/2022:

- Almost 20% did not refer to areas identified by our sectoral risk assessment.
- We provided feedback to half of firms on what they had included about client and / or the firm's transactions in their firm wide risk assessment. It is important that firms do this as it will then help inform the client and matter risk assessments.
- 10% of firms did not properly consider the potential money laundering risks associated with how their services are delivered. We consider this to be a growing risk area for firms especially as more services are now being delivered by email or through online meetings.
- Almost a third of firms used templates or templated text which had not been tailored to the firm. While there is nothing inherently wrong in using a template, you must make sure you adapt and tailor it to your firm and avoid copying and pasting specimen text.

Next steps and further information

Money laundering presents a financial, reputational and regulatory risk to firms, and you should take action to prevent your firm from being exploited by criminals.

As mentioned above, some firms still need to familiarise themselves with the requirements of regulation 18 of the money laundering regulations.

We expect firms to be compliant in this area and have provided a variety of resources to help firms draft an effective firm risk assessment:

- a sectoral risk assessment [https://upgrade.sra.org.uk/sra/how-we-work/archive/reports/aml-risk-assessment/] , setting out common risks
- the Legal Sector Affinity Group Anti Money Laundering Guidance for the Legal Sector 2023 (PDF 220 pages) [https://upgrade.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf?version=49d62e]
- a checklist to help firms prepare for a firm risk assessment (DOC 8 pages, 44KB) [https://upgrade.sra.org.uk/globalassets/documents/solicitors/anti-money-laundering-aml-firm-risk-assessment-checklist.docx]
- a template (DOC 5 pages, 42KB) [https://upgrade.sra.org.uk/globalassets/documents/solicitors/firm-wide-risk-assessment-template.docx] which we have developed using learning from our review and which firms can use to frame their risk assessment – unlike the other templates we have seen, this does not include specimen text.

Tips for completing your risk assessment

Below, we set out some of the good and poor practice we saw, as well as four common questions we are asked.

1. Should I use a template risk assessment?

This is entirely up to you. Some firms find template risk assessments useful in helping get to grips with the AML requirements.

If you use a template, however, you must ensure that it is tailored to your practice. In many cases we found that the risk assessment did not match a firm's profile and did not reflect the risks from its services and client demographic. The money laundering regulations are clear: you must carry out a risk assessment which must be relevant to the size and nature of your business. In this sense, you are the expert.

Remember, you cannot pass the regulatory risk of non-compliance on to a third party. If a consultancy gives you the wrong advice, the responsibility remains with you.

2. What is the difference between matter and firm risk assessments?

Firms often confused a matter or client risk assessment with a firm-wide risk assessment. These are different documents which do different jobs, but both are a requirement of the money laundering regulations.

A firm-wide risk assessment should evaluate the money laundering risk that your whole business is exposed to and set out how you have arrived at that conclusion. It should then set out the steps which will be taken to

help mitigate any risks.

A matter or client risk assessment is linked to a specific client file, and should assess the money laundering risk associated with that particular client or matter. It should also then inform the level of customer due diligence and ongoing monitoring required.

The two documents should correspond with each other, and client or matter risk assessments should be informed by the themes identified in the firm-wide risk assessment.

3. Do I need to include proliferation financing in my firm wide risk assessment?

You are required to carry out a risk assessment which assesses the inherent proliferation financing risks your firm faces given your clients, services, geographic and delivery channels. You may include this as part of your firm wide risk assessment or you may create a stand alone document.

For the majority of firms, we expect the risk of proliferation financing to be low. The risk may be higher for firms providing services in the following sectors:

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

4. How should I deal with politically exposed persons (PEPs)?

You can find further information in the LSAG guidance [https://upgrade.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf] .

Some firms stated that they would never act for PEPs. This suggests that are not aware that the definition of a PEP is very wide, or they believe that they cannot, or should not act on behalf of PEPS.

You should be aware of the type of person likely to be a PEP. As well as political figures, the definition includes state-run enterprises and international organisations. For example, the following are PEPs:

- the business partner of a member of the board of Network Rail, Channel 4 or the BBC
- the children of certain Church of England bishops.

Further information can be found in the FCA guidance note FG17/6 at paragraph 2.16 [https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf] .

It is for firms to decide their own risk appetite, but your policies should be realistic. If a firm has an overly-restrictive PEP policy, it is at risk of:

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

The table below sets out the different areas you should consider under regulation 18 along with examples of good practice and bad practice we have seen.

Regulation 18 risk	Questions to ask	Good practice	Bad practice
Clients: • **Risk profile** • **Know your client** • **What brought them here?**	• What kind of clients instruct my firm? • What is their usual pattern of business? • Do my fee earners know what is usual for our clients? • Is there anything about our client profile which makes them higher risk, for example, high-net worth individuals or PEPs?	• Knowing what a PEP is and how to recognise one • Demonstrating a good working knowledge of your client base's variance in wealth and typical funding sources • Referring to due diligence you have stored on your clients • Considering the steps you take to authenticate a client's claim of identity • Consider the ownership and control structures you typically encounter, describing any extraordinary exceptions • Ensuring that robust measures are in place to establish ultimate beneficial ownership • Consider how clients are referred to your firm • Making sure that fee earners are aware of how to spot changes in a client's usual activity • Effective use of a client risk assessment which alerts fee earners to unusual transactions.	• Stating that you never act for PEPs or assuming they would not instruct you • A narrow definition of PEPS that does not include UK individuals, those working for state-run enterprises or international organisations • Not involving fee earners in spotting unusual clients

	• How good are fee earners at collecting information source of funds and wealth? • Are fee earners equipped to recognise risks and report them? • In what countries do my clients have connections, such as business relationships? • Do any of my clients have links to high-risk jurisdictions? • Do any of our clients come from jurisdictions with sanctions against them? • Do we have repeat clients, walk-in clients, referral agreements or similar?		or transactions.
Geographical area: • **Jurisdictions** • **Connections** • **Local knowledge**	• Where does the firm operate? • Does the firm operate in jurisdictions with AML regulations and controls not equivalent to the UK? • Is the firm referred work from persons/entities based in jurisdictions outside of the UK? • Do you provide services to clients outside of the UK? • How do we check for geographic risk?	• Considering where you have offices and where you offer services • Including consideration of where your clients, client entities or the transactions you are working on are based and where they are linked to • Using reputable sources of information, such as Transparency International [https://www.transparency.org], Basel [https://www.baselgovernance.org/sites/default/files/2019-08/Basel%20AML%20Index%202019.pdf], FATF [http://www.fatf-gafi.org/countries/], or a combination, to determine country risk • Using your own knowledge of countries to inform your assessment • Having a system for identifying high-risk countries which does not need constant updating.	• Being vague, for example, dividing countries into 'UK' and 'worldwide', which misses any sense of the different risk posed by different countries • Making unrealistic statements, for example, stating that 'the firm would never act for an overseas client' • Being complacent, such as one firm which mandated simplified due diligence for all clients within 'the local area', which itself was not defined • Misinterpreting the regulation to exclude

			anyone from a high-risk jurisdiction from being a client. Most people in high risk jurisdictions are not criminals, and it is perfectly acceptable to act for them if a proper process is followed.
Products & services: • **Legal sectors** • **Activities** • **Client account**	• What sort of work does my firm carry out? • How risky are the firm's activities? • Do our fee earners ever go outside our main practice areas, for example, as a favour to a client or a one-off?	• Considering the SRA sectoral risk assessment [https://upgrade.sra.org.uk/sra/how-we-work/archive/reports/aml-risk-assessment/] and other reputable sources in determining your firm's level of risk and other reputable sources in determining your firm's level of risk • Describing your specific service offering within each area of law • Assessing the risks that those represent in collaboration with the relevant subject matter experts (such as departmental heads) • Listing specific department risks and steps of mitigation (as appropriate) • Describing any exceptional cases relevant to your practice • Ensuring any one-offs or favours are acknowledged, and that the inherent risk of these is considered. • Considering the interplay between regulated and unregulated work under the money laundering regulations.	• Not describing the services you offer or activities you undertake.
Delivery channels: • **Remote clients** • **Combining Services** • **Third Party Payments**	• By what means does my firm deliver its services to our clients? • What safeguards do we employ internally to catch repeat clients? • In what circumstances do we accept payments from third parties? • In what circumstances do we send payments to third parties? • Who instructs us remotely and why?	• Describing the means by which you deal with your clients (face to face meetings, telephone calls, emails, Skype calls, etc) and assessing the risks, in practice, that these represent • Describing an effective process that ensures repeat clients instructing new departments are newly risk assessed in proportion to the risks relevant to the new service area • Addressing the circumstances in which you deal with third party payments and how you mitigate the associated risks • Assessing the risks of remote instructions and describing the circumstances and basis on which this is usually permitted.	• Omitting any consideration of the other day to day means by which you deliver services to your clients (excepting face-to-face). • Mentioning bu not assessing remote delivery of services. Mentioning transacting with third parties, but not the basis on which this happens • Failure to consider the risk of 'passporting' - where a client instructs a firm on a low risk matter to avoid scrutiny on later, high risk instructions

Transactions: • **Buying and selling** • **Transferring funds** • **Non-monetary transactions eg shares.**	• Are there adequate safeguards around our client account? • Do we ever receive unsolicited payments? • Do we deal with transactions that are unusually large? • Do we deal with complex transactions? • Do we deal with alternative payment methods? • Do we deal with transactions that facilitate anonymity?	• Describing the size and frequency of transactions that your firm deals with • Evaluating the circumstances in which you will deal with transactions that are unusually large, remarking on any notable cases • Describing the service areas which might remove identifying detail from a payor or payee, and why this risk is tolerated • Considering whether any payments other than GBP are typically used in the matters you deal with (including crypto assets, high value products, alternative fiat currencies), and evaluate the risks these present • Considering the risks of cross-border transactions involving other jurisdictions • Acknowledging training undergone by accounts employees.	• Providing no description of the monetary transactions you are engaged in • Stating a generic list of transactional risk factors • Failure to consider how the firm will monitor transactions, for example unexplained payments into the client account.