Guidance

Firm risk assessments

Updated 25 November 2019 (Date first published: 29 October 2019)

Status

This guidance is to help you understand your legal and regulatory obligations and how to comply with them. We may 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.

General

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. This has been a legal requirement since 26 June 2017.

The requirement to produce a firm risk assessment is set out at Regulation 18 of the money laundering regulations. The risk assessment must:

- take into account information we publish
- address 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

- take into account, and be appropriate to, the size and nature of your business.

What we have seen

In spring 2019, we called in 400 firms' anti-money laundering risk assessments. We found high levels of non-compliance with the money laundering regulations, with 21% not compliant. Of the 400 firms we contacted:

- 83 risk assessments were not compliant:
  - 40 firms did not send us a firm risk assessment, instead sending us something else
  - 43 firms did not address one or more of the Regulation 18 criteria.

We found that 135 of the risk assessments we received (38%) were dated after our request went out. A proportion of these may have been updates of earlier risk assessments, however others may have been a newly created document, suggesting that some firms within our sample did not have an existing risk assessment at the time our request was received.

When we reviewed our records and the firms' own websites, we found that many risk assessments were not appropriate to:

- the size of the firm´s business
- the services the firm offered
- the geographical area in which the firm operated.

We also found that the use of templates had an impact, with risk assessments based on a template being generally lower quality. Those risk assessments which were not based on a template tended to be better. If you are choosing to use a template, you must make sure to 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.

A considerable minority of 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, setting out common risks
- the Legal Sector Affinity Group Anti-Money Laundering Guidance for the Legal Sector 2021 (PDF 212 pages, 2.2MB)
- a checklist to help firms prepare for a firm risk assessment (DOC 8 pages, 44KB)
- a template (DOC 5 pages, 42KB) 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 three 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.

More than half of the risk assessments we received (64%), used a template. While there is nothing inherently wrong in using a template we noted that many we saw were almost or completely identical.

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. We were encouraged that small practices and sole practitioners tended to produce very good and detailed risk assessments, often from scratch using their expert knowledge of their clients and work.

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. Of the 40 firms which sent us the wrong document, 22 were matter risk assessments. 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
- A matter or client risk assessment is linked to a specific client file, and should assess the money laundering risk of that client or client matter.

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

A number of 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
- senior office holders of international bodies such as the Red Cross or Amnesty International.

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.

Regulation 18 risk	Questions to ask	Good practice	Bad practice
Clients: • Risk profile • Know your client	• What kind of clients instruct my firm? • What is their usual pattern of business?	• 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	• Stating that you never act for PEPs • A narrow definition of PEPS that doesn't include UK individuals, those working for state-run enterprises or international organisations

Regulation 18 risk	Questions to ask	Good practice	Bad practice
brought them here?	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? • 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?	• 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.	
Geographical area: • Jurisdictions	• Where does the firm operate? • Does the firm operate in	• Considering where you have offices and where you offer services • Including consideration of where	• Being vague, for example, dividing countries into 'UK' and 'worldwide', which misses any sense of the different risk posed by different countries

Regulation 18 risk	Questions to ask	Good practice	Bad practice
• Local knowledge	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?	are based and where they are linked to • Using reputable sources of information, such as Transparency International, Basel, FATF, 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.	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 regulations 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 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:	• By what means does my firm	• Describing the means by which you deal with your clients (face to	• Omitting any consideration of the other day to day means by which you

Regulation 18 risk	Questions to ask	Good practice	Bad practice
• Combining Services • Third Party Payments	• 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 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.	• Mentioning but 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' I 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.


CYBER
ESSENTIALS
CERTIFIED
PLUS