Firm-wide risk assessment methodology

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17) require firms to take the appropriate steps to identify and assess the risk that they could be used for money laundering, including terrorist financing.

Firms providing accountancy, trust or company services need to assess the services they provide and the types of clients they have, to understand how criminals could use them to conceal the proceeds of a crime or use their services to create an arrangement that could facilitate money laundering.

If you are providing these services, you will need to step back and think about the risks affecting your firm as a whole.

Your risk assessment will identify the areas of your business that are most at risk and this will enable you to focus your resources on the areas of greatest risk.

You must document your firm-wide risk assessment.

It is the responsibility of your firm's senior management to approve the policies, controls and procedures that address and mitigate the risks and you must document all these aspects.

MLR17 defines senior management as an officer or employee of your firm with sufficient knowledge of the money laundering and terrorist financing risks that your firm is exposed to; and sufficient authority to take decisions affecting your firm's risk exposure.

PERFORMING YOUR FIRM-WIDE RISK ASSESSMENT

You can design your own firm-wide risk assessment and MLR17 acknowledges that you can take into account the size and nature of the business. The risk assessment for a small practice, providing a limited range of services to a small number of clients, may be quite succinct. But most importantly, you must properly identify and assess the risk of money laundering or terrorist financing and you must document your assessment.
There are three key steps to performing and effective risk assessment as follows:

Step 1: identify the money laundering risks faced by the different areas of your business, and the clients and markets you serve.

Step 2: assess each identified risk by considering the likelihood of it occurring and the resulting impact if it occurs.

Step 3: review the mitigating checks, systems and controls you have in place, or mitigating actions you could take, to bring the level of net risk to an acceptable level. Once you have concluded what your existing or planned mitigating actions are, you should make sure your firm's policies, controls and procedures are designed appropriately and properly understood and implemented by your staff, so that they remain effective in addressing the level of risk you have identified.

The following sections of this paper explain these steps in greater detail.

HOW TO IDENTIFY MONEY LAUNDERING RISKS

You must assess the risk that criminals could use your firm to conceal the proceeds of a crime or use your services to create an arrangement that could facilitate money laundering. In particular, you must consider:

- How your firm could be used to launder money. Could you receive criminal proceeds into a client money account or could you create a corporate structure (through company or trust formation) that disguises the beneficial ownership of criminal proceeds?

- How your firm could conceal the proceeds of a crime. Could you legitimise the proceeds of a crime by recording the cash/income as revenue in the financial statements that you are preparing when the cash/income has nothing to do with the principal activity of the client?

MLR17 requires you to consider risk factors including:

- your clients;
- the products and services you provide;
- the countries that your clients operate in;
- the transactions you are involved in; and
- the delivery channels.

In determining your risks in relation to each of the above categories you should have reference to the following:

- The latest National Risk Assessment
- ICAEW risk guidance
- The Accountancy AML Supervisors' Group Risk Outlook

You must also take into account the size and nature of your practice. For example, the risk assessment of an accountancy firm with 20 offices covering the whole of the UK and an overseas network with audit, accounting, tax, and insolvency service lines would consider very different risksto a sole practitioner providing book-keeping and accounts preparation services to businesses operating in the local town.

Risk factor 1: Your clients

You should identify the type of clients that your business serves and assess whether these are known to be frequently used by money launderers.

You can separate your client base by industry, size, or type (eg, individual, trust, LLP or limited company).

To identify all the types of client that your firm serves, you could:

- consider whether any of your principals have industry specialisms;
- review your website or promotional material for references to client industry or nature;
- use data from your practice management system; or
- consider whether there are certain types of client that already require senior management approval at take-on.

You should then assess the risk of money laundering associated with each of those client types. When assessing client risk, you could consider whether there are any characteristics that are known to be used by money-launders.

When you have assessed the level of risk associated with each client type, you should identify any mitigating actions that you take to address this risk. This could include enhanced due diligence, senior management approval at take-on, or updating your client due diligence on a very frequent basis. We have set out further guidance on how to address the risks below.

Risk factor 2: Products and services you provide.

You should identify all the services that you offer and assess whether these could be used by criminals to launder money.

To identify all the services you identify you could:

- use the categories of firm turnover that you disclose on your annual return;
- list the services you explain on your webpage or promotional material;
- consider the categories of service you list on your client take-on forms; or
- think about the organisational structure of your firm, and how you manage your staff.

You should then assess the risk of money laundering associated with each of those services. When assessing client risk, you could consider whether there are any services that can be easily used to launder money or to conceal or layer money laundering.

We have set out those services that could pose a higher-risk in our risk guidance.

When you have assessed the level of risk associated with each service type, you should identify any mitigating actions that you already take, or plan to take, to address the risk. You could decide to stop offering services that are very high risk or you could decide to enforce a second-partner review for certain service types. You should make sure that you include any high-risk services in your compliance reviews to confirm that your staff are implementing your policies and procedures. We have set out further guidance on how to address the risks below.

Risk factor 3: The countries that your clients operate in

You should identify the countries that your clients operate in. You could consider:

- the countries your clients are based in or operate from;
- where your clients obtain their funding from;
- where your clients sell most of their goods and services;
- where your clients buy most of their raw materials; or

- how your clients are linked to countries through networks, agencies, or outsourcing suppliers.

You should then assess the risk of money laundering associated with each of those countries. When assessing geographic risk, you could consider factors such as whether there is a perception of corruption in that country, whether there is known to be criminal activity or if the country is on the sanctions list. Mitigating factors could include where countries are known to have effective AML regimes.

Firms with considerable experience of operating in 'high-risk' jurisdictions could have a different risk assessment, and mitigating action, to those firms with limited experience. We have set out further guidance on how to address the risks below.

We have set out those countries that could pose a higher-risk in our risk guidance.

Risk factor 4: The transactions you are involved in.

You should identify any transactions that your firm could facilitate and assess the risk that these transactions could relate to the proceeds of a crime or terrorist financing.

This is most likely to be relevant if you operate a clients' money account or any client's own accounts. You should identify the types of transactions that pass through your clients' money account and assess the risk associated with each of these types of transaction.

Payroll and Insolvency services provided by the firm could also be used to support criminal activity or effect illegal transactions.

However, you could also facilitate transactions of 'assets' and you should identify these types of transactions and assess the risks associated with them.

We have set out those transactions that could pose a higher-risk in our risk guidance.

You should then document your risk assessment of the transactions that your firm is involved in. You should identify how you mitigate, or plan to mitigate, those risks. This could include the consideration of the regulatory framework within which those transactions are facilitated – for example, the ICAEW Clients' Money Regulations. We have set out further guidance on how to address the risks below.

Risk factor 5: Delivery channels

You should identify all the methods of interaction you have with your clients and how close you are to them. Some delivery channels can increase risk because they can make it more difficult to determine the identity of a client.

Factors to consider are:

- whether you meet your clients face-to-face;
- if you have some clients that you only correspond with online;
- whether your clients are introduced through an intermediary and whether you only correspond with that intermediary;
- the extent to which you rely on the CDD of the referrer or intermediary (and the procedures you employ to justify reliance) or the quality of evidence obtained from them to support your own CDD.

We have set out those delivery channels that could pose a higher-risk in our risk guidance.

You should identify how you mitigate, or plan to mitigate, these risks. You could decide that you will only take on clients that you have met face-to-face, or you could specify the client due diligence, and frequency with which they are updated, for those clients that you haven't met. We have set out further guidance on how to address the risks below.

HOW TO ASSESS MONEY LAUNDERING RISKS

To assess the money laundering risk, you must consider the likelihood of the risk occurring, and the impact if the risk did occur.

Most risk management tools will identify a range of likelihood and impact that you can apply to your identified risks. You can determine your own ranges, or use risk management tools that are widely available over the internet.

One possible range for likelihood is:

- Almost certain – the event will occur in all but exceptional circumstances.
- Probable – the event is expected to occur in most circumstances.
- Possible – the event should occur at some time.
- Unlikely – the event may occur at some time.
- Rare – the event may occur at some time, but it would be exceptional.

For example:

- it is 'almost certain' that a criminal would want to use a chartered accountant to legitimise the proceeds of a crime; or
- it is 'rare' that a locally based client you meet face-to-face will lie to you about their identity because they want to conceal their background and source of funds or wealth.

A sensible range for impact is:

- Critical – significant sums of money could be laundered with potential criminal prosecution against principals in the firm.
- Major – large sums of money could be laundered with significant reputational damage to the firm.
- Significant – moderate sums of money could be laundered with some reputational damage to the firm.
- Minor – limited sums of money could be laundered with negligible reputational impact.

For example:

- there is a 'critical' impact of a criminal using the firm to legitimise the proceeds of a crime as this may result in significant sums of money being laundered by the firm with potential criminal prosecution against principals in the firm.

TAKING STEPS TO MITIGATE MONEY LAUNDERING RISKS.

Once you have identified and assessed the risks of the various ways your firm could be used for money laundering, including terrorist financing, you must take steps to mitigate those risks by implementing appropriate policies, controls and procedures. We've set out the options that you might consider below:

- Your first and most important defence against the risk of money laundering is to design effective client due diligence (CDD) procedures that, while being proportionate to the level of risk you have identified, should aim to prevent your firm taking on clients that could be connected to criminal activity or laundering the proceeds of crime.

- You can tailor your CDD procedures to the risks in your firm. You could identify areas of your business or client types where simplified due diligence is appropriate, just as there could be higher-risk services or clients that merit enhanced due diligence (with more frequent reviews accordingly).

- You should regularly screen staff involved in higher risk areas (and involved in the internal AML and client take-on procedures) to ensure they are fit and proper and have no criminal history.

- You should consider whether staff working in high-risk business areas require more frequent or more specialised training.

- You should encourage your MLRO/MLCP to maintain contact with other professionals or groups providing similar services or operating in similar sectors or countries, in order to maintain a good understanding of new and emerging risks that could affect the firm. They should ensure that they are receiving AML bulletins and risk alerts that may be issued by their AML professional body supervisor.

- You should establish checks within your firm to assess and frequently review higher risk engagements, which should be performed by personnel independent of the principal responsible for the engagement. For example, these checks could involve the approval of theMLRO, the MLCP, the firm's management team, its board (or equivalent) or a combination ofthese.

- You may decide, in extreme cases, that the only way to mitigate the risk to an acceptable level is to terminate the relationship with a client or to stop offering a very high-risk service.

Your assessment of how you design your procedures can take into account your firm's experience and knowledge of different environments. For example:

- if your firm has no experience of clients operating in a particular country, you could conclude that the risk is normal or high risk even if other firms may conclude it to be low risk; or

- if your firm has considerable experience of dealing with clients from a high-risk country or industry sector, you could conclude that the client risk is normal, but you may want to perform additional due diligence to address the perceived risks associated with that country/industry sector.

THE PURPOSE OF CDD

The purpose of CDD is to know and understand a client's identity and business activities, as well as the source of funds. Criminals often seek to mask their true identify by using complex and opaque business structures and so it is important that you verify the identity of a client and, on a risk-based approach, its ultimate beneficial owner. Once you have verified the identity of a client, you can enhance your understanding of your client and mitigate risks with other information gathering procedures, for example open-source (google) checks or PEPs and sanctions screening. (ICAEW client screening service). These can confirm that what the client has told you is true and serve to identify any risks that may not be apparent during an initial meeting, for example prior criminal activity.

CDD also helps you to understand your client's 'normal' business activities, which will better equip you to identify any abnormal events or transactions that could point to money laundering and terrorist financing.

EVALUATING THE EFFECTIVENESS OF YOUR POLICIES, PROCEDURES, AND CONTROLS

You should regularly examine and evaluate the adequacy and effectiveness of the policies, controls and procedures and monitor the firm's compliance with them.

ICAEW is developing a compliance review checklist that explains how you can examine and evaluate your policies, controls, and procedures. When it is finished, we will make it available onthe webpages.

REVIEWING YOUR FIRM-WIDE RISK ASSESSMENT

You must regularly review your firm-wide risk assessment to ensure that it remains relevant and fit-for-purpose. For most firms this might require an annual programme of review by senior management.

In particular, you must regularly consider whether you have identified all the money laundering and terrorist financing risks present in your firm.

To enhance your approach and ensure you have identified all relevant risks, you could consider any reports from your staff on suspicious activity (as well as those lodged with the NCA) and review a sample of completed client due diligence documents to re-confirm that you know the clients sufficiently well and that the risks associated with the services being performed, the geographic location of the client and transaction involved in their businesses have been fairly and carefully assessed.

EXAMPLE OF FIRM-WIDE RISK ASSESSMENTS

Profile of firm

- Sole practitioner with 10 staff. Total firm income £500k.
- Services – accounts preparation for small businesses, limited companies, tax returns and payroll.
- Clients – individuals, small businesses, and limited companies. Two high net worth individuals (not high profile).
- Geographic reach – locally based clients. No overseas.
- Special work - practitioner is a trustee for one trust.
- Client money – few accounts, mainly used for tax refunds.

Risk factor	Summary of firm	Assessment of risk	Mitigating actions
Clients	• Individuals (including two high net worth) • Small businesses and limited companies • Mainly manufacturing and tradespeopleoperating within the UK • Some farming clients	Risk is normal, although some elevated risks with farming/agricultural clients in this county. The two high net worth clients are longstanding clients. We understand and can verify sources of wealth, one through inheritance, the other through sale of successful businesses. We don't have anyclients who are PEPs. No clients with complex business structures that appear designed to obfuscate control. We do have farming clients and there is a risk of labour being sourced illegally (Modern slavery and human trafficking MSHT).	Perform standard CDD to verify clientidentity, and business activities. Check and verify sources of wealth and funds where appropriate. Provide staff with training on where riskof ML arises and relevant case studies. Consider gross and net profit margins on farming clients, consider whether staff costs are reasonable and ensure our staff are alert to payroll anomalies that might be indicative of MSHT. I am the MLRO and I approve all new clients and would be aware of any PEPs. However, where there are

			any risk factors, including overseas links, we sanction check and PEP screen using ICAEW client screening services.
Services	• accounts prep (£120k) • tax returns (£100k) • payroll (£30k) • trustee (£1k) • company formation and registered office service (£1k)	Risk is normal for most services although we are aware that criminals may use our services to provide credibility to their business. We have reviewed ICAEW risk guidance: • We don't provide tax planning services. • We are aware of the risks associated withincomplete records. • We only form companies and act as registered office for clients for whom we also offer other accountancy services.	Perform CDD to confirm client identityand business activities. Provide staff with training on where the riskof ML arises and relevant case studies. Design procedures for incomplete records to establish supporting evidence/records. Do not offer company formation and/or registered office services as a single service offering.

		• We make payments from our clients' own accounts,and we receive monies to pay to client staff. • We are aware of the risks associated with trusteeservices. This is not a routine service offering but a one-offengagement for a long-standing client. We do notintend to offer it to any other clients	Design procedures for payroll clients toensure that staff exist. Specific training for payroll staff on risks and red flags. Include all areas of business in compliance review to confirm policiesand procedures are implemented. When we are notified of changes to bank account details for payroll clients, we call the client to ensure legitimate email.
Geography	All clients are based locally.	Risk is low. All clients are based locally, and none have anyconnections to other countries. Most clients are referred by other clients and we rarely get 'walk-in' trade. This is a rural office, and we tend to know most clients personally as well as professionally.	Perform CDD to confirm client identityand business activities. Client take-onchecklist has flag for jurisdictions considered to be high-risk. Staff must notify MLRO if they come across connections to countries on thehigh-risk list. Additional checks if a new client is completely unknown to our staff/our clients.

Transactions	Client money account	Risk is normal. Account is used for tax refunds 15-20 transactions per year from HMRC. We don't operate any other accounts and don't operate any clients' accounts. Risk associated with payroll monies above.	Perform CDD to confirm client identityand business activities. Provide accounts staff with training on where ML risk arises and relevant casestudies. Most funds received from HMRC and therefore can be verified. We only provide our client bank account details to a limited number of our payroll clients. Subject to ICAEW's Client's Money Regulations.
Transactions	Firm's office account	Risk is normal. Our income is from locally based clients and bills are settled from UK bank accounts.	Provide accounts staff with training onwhere risk of ML arises and relevant case studies. Our clients receive our bank accountdetails on our invoices. We are alert to push payment fraud and where suppliers notify changes in bank account details, we verify this directly with them.

Delivery channels	Face to face	Risk is low. We deal with all our clients face to face. We do operate though online delivery methods (eg, online accounting software) but we regularly meet with ourclients as well.	Perform CDD to confirm client identityand business activities. We only accept clients that we have met. If we aren't planning to meet witha client, staff must notify the MLRO.
Other	None identified.		

Actions	Delivery date	Owner
Schedule update training for summer 20xx	31 July 20xx	A Practitioner
Perform annual compliance review	31 July 20xx	A Practitioner

Signed: A Practitioner
Dated: 31 December 20xx

Next review due: 31 December 20xx