March 2026

AML Declaration 2026
Guidance

Introduction to Guidance for AML Declaration 2026

Importance of the AML Declaration

Whilst the UK Government announced on 6 November 2025 that the Financial Conduct Authority will take over the AML supervision of the accountancy and legal sectors, the timescale for this transfer of responsibility is still to be finalised. In the meantime, ICAS continues to be an AML supervisor, with statutory responsibility over ICAS supervised Firms.

The Money Laundering Regulations 2017 require that ICAS conducts a risk assessment of each Firm ICAS AML supervises. Our regulator, OPBAS also expects ICAS to focus its monitoring effort on a risk-basis.

To achieve this, we require every Firm to submit an annual AML declaration to ICAS each year. The information submitted highlights the money laundering, terrorist financing and proliferation risks faced by the Firm. The return includes questions on the nature of the Firm's clients, the services provided, various AML compliance questions, and other risk factors. The declaration is updated annually to ensure that it reflects current risks.

Many of the questions derive directly from risks highlighted in the National Risk Assessment ('NRA') and from the risk intelligence we receive from regulatory and supervisory sources and law enforcement. The NRA was updated in July 2025 and this guidance reflects updated intelligence provided in that assessment. Similarly, guidance has been published by the Accountancy AML Supervisor's Group ('AASG') in September 2025, called the **AASG Risk Outlook**, which has also been referenced in updating this publication.

The responses provided by Firms are collated, with risk scores and weightings allocated, giving every Firm an overall AML risk score and then a risk category.

This risk category has determined:

- How often a Firm is reviewed.
- How the Firm is reviewed.
- How the Authorisation Committee will deal with serious non-compliance.

Your AML Declaration is. Therefore. very important to the overall effective operation of the ICAS AML supervision regime.

Firms are reminded of the results of our **ICAS Firm-Wide Risk Assessment Thematic Review** which concluded that a number of smaller Firms had incorrectly omitted risks from their declaration and were therefore showing as low risk when, in fact, had the declaration been completed correctly, the Firm would have been assessed as medium (or in fewer cases high) risk.

In accordance with the **Regulatory Actions Guidance**, which was updated and effective from 6 April 2025, a Firm risks regulatory action, including regulatory penalties, where a monitoring visit identifies significant differences between the information provided by the Firm to ICAS in its AML Declaration and information identified during the monitoring visit. Already a small number of Firms have received financial penalties for significant under-declaration of risks in their AML declaration.

It is, therefore, important that you give sufficient time and effort to identifying and assessing your AML risks as part of your Firm-Wide Risk Assessment (also called 'Whole Firm Risk Assessment 'WFRA') and to ensuring that both the WFRA and the AML declaration reflect all the risk factors being faced in your Firm.

If you are in doubt, please don't hesitate to contact **regulatoryauthorisation@icas.com** .

We would always say if in doubt it is better to overstate a risk than understate it.

Thank you in advance for your cooperation with this important process.

For more information on our supervision regime and for key findings from monitoring visits, please refer to our annual report **here.**

Purpose of the Guidance

This document serves as a practical guide to assist you in accurately completing the AML Declaration 2026.

It provides clear explanations of key terms, concepts, and requirements. The purpose is to ensure consistency, clarity, and a comprehensive understanding of the declaration's questions.

By referring to this guide, you will be better equipped to identify and disclose relevant information, assess risks, and provide complete and compliant responses.

This guidance should also help you in completing your Firm-Wide Risk Assessment, given that it provides your with comprehensive intelligence on the key risks currently being faced by the UK, as extracted from the 2025 National Risk Assessment ('NRA') and the AASG Risk Outlook.

Section1: Standing Data

The first sections of the return are pre-populated with data we hold about your Firm from information your Firm has previously supplied. If you identify that there are changes to your Firm details, you should contact **regulatoryauthorisation@icas.com** to ensure that these are corrected.

Firm Details

Please review the data held about your Firm and ensure that this is up to date. You should ensure that the information about your Firm's name, address and telephone number is correct.

Please ensure that the name of the Firm's MLRO is correct. This is the person who is the 'nominated officer' under S 21(3) of the Money Laundering Regulations 2017 and who is responsible for receiving internal reports and making Suspicious Activity Reports.

Money Laundering Compliance Principal

Please ensure that we have the correct details of the name of the Money Laundering Compliance Principal (MLCP). This is the person designated under S 21(1) of the Money Laundering Regulations 2017, who is a member of the board or senior management, who is the officer with overall responsibility for the Firm's overall AML compliance. In smaller Firms, the MLCP and MLRO may be the same person. If that is the case, you should still check that the MLCP details are correct.

Important: Beneficial Owner, Officer and Managers (BOOMs)

You should ensure that all Beneficial Owners, Officers and Managers in your Firm have been approved by ICAS as BOOMs and that they are disclosed on this declaration. Failure to obtain ICAS approval of each person who holds the role of a BOOM in your Firm is a criminal offence.

Please refer to the **BOOM Thematic Review** that was published in October 2025, which highlights the key areas that are commonly missed by Firms.

If the list of BOOMs is incorrect or incomplete, in any way, you must notify ICAS. Failure to do so, could risk the Firm receiving a regulatory penalty, as previously communicated to all AML Supervised Firms and as explained **here.**

The definition of BOOMs is included at icas.com **here**.

Common mistakes:
Firms are reminded of the common mistakes found on monitoring visits:

- The company secretary of the Firm (if applicable) is sometimes missed - they should be a BOOM;
- In some Firms we have found that spouses who are BOOMs are omitted. Any spouse/partner of a principal in the Firm who has been designated a beneficial owner (e.g. shareholder), director or company secretary must be a BOOM even if they are not actively involved in the Firm.
- We have found that AML personnel are sometimes omitted. Any member of staff involved in ensuring compliance with the Firm's AML policies and procedures (e.g. an AML manager, ML compliance officer, MLRO) must be a BOOM.

Section 2: AML risk questions

Under Regulation 17 of the **Money Laundering Regulations 2017** we must identify and assess the risks that our supervised Firms face, particularly in relation to:

- The Firm's clients;
- Any geographic risks;
- The nature of the Firm's services;
- The transactions the Firm enters into; and
- The delivery methods the Firm uses to provide services to clients.

The questions below collect information on your Firm, and your clients, that will help us to perform this assessment.

For the avoidance of doubt, each question in relation to client type asks whether you have any clients in each category below, not whether there are any risky clients in that category.

In answering the questions below please answer 'Yes' to having any clients in the following categories, regardless of how you have assessed their risk.

This is because the extent of risk in relation to each client is more nuanced and is more appropriate for discussion during an AML monitoring visit. We have given you pointers in the guidance below as to more risky situations in order to help your own Firm-Wide (Whole Firm) Risk Assessment and CDD

If you are in doubt as to whether to include 'Yes' to any category, you are better to over-declare risks than under-declare.

1. High Net Worth Individuals (HNWIs)

A person with a substantial amount of assets of £2million or more (excluding their primary residence) or annual income of £200,000 or more.

The definition of an HNWI can vary but it's generally based on their net worth and the value of of their assets.

His Majesty's Revenue and Customs (HMRC) generally regards an individual as 'wealthy' if they have income of £200,000 or more, or assets equal to or above £2 million in any of the last 3 years.

(The Financial Conduct Authority defines a HNWI as an individual with an annual net income of £170,000 or more, or net assets of £430,000 or more. We have not used this guidance).

For the purposes of this return we have used the figures published by HMRC, which is consistent with other accountancy supervisors.

You are being asked if you have ANY HNWI clients, regardless of your risk assessment – if you do please answer 'Yes'

Why we ask the question:
Not all HNWI individuals are high risk but some may be and therefore we require to ask you if you have any such clients – we will discuss these clients in more detail during a monitoring visit. Some HNWI clients may be considered high risk for money laundering for a number of reasons including risk factors such as: their sources of wealth may be numerous, complex or could be difficult to verify; they may have multiple sources of income and multiple investments and they may have holdings in various assets (e.g. high value property; cryptoassets; cash; gold; precious metals and stones; art work; luxury goods etc); they may have international exposure; and may well have complex tax situations involving a number of jurisdictions; there

could be elements of offshoring etc. All of these factors, and more, should be considered in conducting your client due diligence, and where considered necessary, enhanced due diligence may be required.

When dealing with HNWI clients it is important to consider all possible risks and ensure that sufficient KYC information is obtained to support your risk assessment, including a full consideration of source of wealth, source of income, nature of investments etc.

2. Uncooperative clients

A client who is difficult to work with and may be resistant to providing all the information required to ensure that the engagement service is AML compliant.

If you have ANY such uncooperative clients, please answer 'Yes'.

Why we ask the question:
There will of course always be some clients who are less helpful than others, but you should declare only those clients who refuse to cooperate with your AML processes or who are particularly difficult to deal with and therefore you may have concerns that not all information pertinent to AML is forthcoming.

For example, they may not be forthcoming or may be slow in responding when you are trying to understand control & ownership structure, or not provide all the identity verification information or background KYC information required.

When dealing with such clients, you should consider whether any delays, or lack of information, prevent you from meeting the AML requirements and you are also reminded of the need to consider the Code of Ethics requirements in relation to considering the client's integrity and whether you should continue to act.

A Firm should not act for a client which would result in the Firm not being able to meet its legal and ethical obligations.

3. Clients with connections to high risk, corrupt or sanctioned countries

Jurisdictions identified as having weak regulatory frameworks, poor enforcement of AML laws, high levels of corruption, or known links to terrorism financing or proliferation, or are on a current sanctions list.

If you have ANY clients connected to high-risk, corrupt or sanctioned countries, please answer 'Yes'.

'Connected to' has the widest meaning in the context of this question (e.g. it includes whether the client resident in; from; has family members or close associates connected; has a residence or offices there; trades with those countries etc).

Why we ask the question:
These countries present a greater risk of money laundering, terrorism financing, proliferation and other financial crimes.

High risk countries
Money Laundering Regulation 33(1) (b) and 33(3)(A) requires Firms to apply enhanced due diligence (EDD) automatically for any country that is named on either of the following lists:

1. High-Risk Jurisdictions subject to a Call for Action (the 'black list');

2. Jurisdictions under Increased Monitoring (the 'grey list').

The FATF (Financial Action Task Force) regularly publishes these lists which are available **here**. We would expect the Firm to answer 'Yes' if there are clients connected to these countries.

By way of illustration only, the following countries were included on the two FATF lists at the time of publication (all grey except for the three noted as black): Algeria; Angola; Bolivia; British Virgin Islands (BVI); Bulgaria; Cameroon; Côte d'Ivoire; Democratic People's Republic of Korea (black); Democratic Republic of the Congo; Haiti; Iran (black); Kenya; Lao PDR; Lebanon; Monaco; Myanmar (black); Namibia; Nepal; South Sudan; Syria; Venezuela; Vietnam; and Yemen

Please note that this list is updated regularly and cannot be relied upon as a complete list - Firms must stay up to date with emerging risks.

Sanctioned countries

Sanctioned countries are those where there are economic or political measures taken due to geo-political issues, conflicts, human rights issues etc. Sanctions are restrictions limiting the freedom of a state, such as financial restrictions such as freezing assets, or trade restrictions on specific goods or travel restrictions. In some cases, sanctions are wide-reaching prohibitions and in some cases the sanctions may relate to specific industries or geographic areas. An example of a sanctioned country, currently, is Russia.

Money Laundering Regulation 33(6)(c)(ii) requires that in considering whether a client is in a high-risk jurisdiction and requires enhanced due diligence, the Firm should consider geographic risk factors including:
'countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations'

The **UK's sanctions list** is published by the Foreign & Commonwealth Office. The list contains all individuals, entities and ships specified/designated under Sanctions and Anti-Money Laundering Act (SAMLA) 2018. The list includes all those designated under the types of sanctions including financial, immigration, trade and transport.

(The Office of Financial Sanctions Implementation (OFSI), used to produce the consolidated list of asset freeze targets, but this is no longer being updated is replaced by the UK Sanctions List).

Countries linked to significant levels of corruption

Money Laundering Regulation 33(6)(c)(ii) requires that in considering whether a client is in a high-risk jurisdiction and requires enhanced due diligence, the Firm should consider geographic risk factors including:
'countries identified by credible sources as having significant levels of corruption or other criminal activity such as terrorism'

One such credible source in relation to corruption is the **annual corruption perceptions index** published by Transparency International - those countries with the highest scores (or the lowest rankings) have a perception of being corrupt regimes. Many of the countries listed at the bottom of the table with the highest rankings, are the same as those on the FATF lists but not all of them – for example a number (e.g. Somalia; Libya; Eritrea; Sudan; Nicaragua; Equitorial Guinea; Afghanistan to name a few) are not on the FATF list.

4. Individual Clients and entities on any Sanctions List:

Sanctions or restrictive measures placed over named persons such as a legal entity or a natural person (including asset freezes, trade embargoes and travel bans).

If you have ANY such clients, please answer 'Yes'.

Why we ask the question:
Acting for a person or entity on a sanctions list may be prohibited, or if not illegal, could indicate a high risk from a money laundering, terrorist financing or proliferation perspective.

The UK's sanctions list is published by the Foreign & Commonwealth Office. The list contains all individuals, entities and ships specified/designated under Sanctions and Anti-Money Laundering Act (SAMLA) 2018. The list includes all those designated under the types of sanctions including financial, immigration, trade and transport.

Firms are reminded to check the names of beneficial owners and not just the names of the client entity.

This list can include:

- Individuals or entities subject to asset freezes.
- Entities under trade embargoes.
- Travel bans and restrictions on financial services

5. Clients which are largely based outside of the United Kingdom

Any client entities largely based, or with operations largely based, outside the UK. Any individual/personal clients where the person is largely based outside the UK.

If you have ANY clients based overseas in this category, regardless of their risk level, please answer 'Yes'.

Why we ask the question:
For the purposes of this return, we are interested in whether there are any clients meeting these criteria as a starting point to risk assess our Firms.

Not all clients based largely overseas will pose a higher AML risk. You are asked to provide details of any overseas connections to allow the monitoring team to have more detailed discussions with you on those connections at a monitoring visit. It should also be a starting point for you to consider whether there are any risk factors in conducting your customer due diligence.

The extent of money laundering, terrorist financing, and proliferation risks will vary depending on the country in question, the nature of the client, and of the services provided. Some clients based overseas will have no additional risks, while others will have increased complexity and risk (e.g. taxation can be more complex; it may be more difficult to obtain reliable KYC information from that country, there could be connections with countries which have less stringent AML rules etc.). In considering whether these clients might have higher risk factors please refer to the additional guidance in the next Section 6 below which highlights risks with particular types of countries, for example.

Examples that would result in answering 'Yes' to this question:

- your Firm has a personal tax client who is resident in Portugal, but you manage their UK tax affairs as they hold a UK property.
- your Firm has a corporate client that is headquartered and registered in Turkey.
- your Firm has a client whose largest branch is based in France.

6. Overseas connections

This covers any other situation not included already i.e. clients with any other overseas connections whatsoever.

Please answer 'Yes' if you have ANY clients with any overseas connections, not already covered in previous questions, and regardless of their risk category.

Why we ask the question:
This is a 'catch-all' question to cover any other situations where there are international considerations which are not already captured in earlier questions.

Not all overseas connections will pose a higher AML risk. The extent of money laundering, terrorist financing and proliferation risks will vary depending on the country in question and the nature of the client and services provided. Some clients with an international connection will have no additional risk and others can have increased complexity (e.g. taxation can be more complex; it may be more difficult to obtain reliable KYC information from that country, there could be connections with countries which have less stringent AML rules etc.).

However, for the purposes of this return, we are interested in whether there are any clients meeting these criteria as a starting point to risk assess our Firms.

This could, for example include:

- a client with an overseas nationality;
- a client with some residency overseas (although not largely based abroad) or with family connections overseas;
- clients with, for example:
    - some (but not the majority of) operations overseas;
    - some branches or subsidiaries overseas;
    - connected entities overseas;
    - connected trusts/trustees overseas;
    - parent companies overseas;
    - beneficial owners based overseas;
    - directors or trustees based overseas;
    - overseas customers or suppliers.

This list is not exhaustive.

Whilst this is a catch-all question to identify **any and all overseas connections**, when you are considering which of your clients pose a higher risk in conducting your own customer due diligence, you should consider both the list of higher risk countries (see Section 3 above) but also additional intelligence, such as data provided in the 2025 NRA, for example (the list below is illustrative only):

- ‘Offshore’ destinations for tax purposes are popular for money laundering and a number of offshore destinations were mentioned in the NRA including the Crown Dependencies (Jersey; Guernsey, Isle of Man), Luxembourg , Lichtenstein, the Caribbean (such as British Virgin Islands, Cayman Islands, Bermuda) for example.
- Other countries which are popular for high-net worth individuals, and kleptocrats, particularly those looking to avoid sanctions, include the United Arab Emirates (‘UAE’), Monaco, Cyprus (due to shipping connections/corporate restructuring), Singapore for example.
- Other countries which were mentioned in relation to Organised Crime Groups include the Balkans (Albania, Bulgaria, Bosnia, Romania etc), drug cartels in Latin America, China etc.

7. Clients operating cash-based businesses and cash-intensive business:

Any clients that can accept cash for goods and services - even if the % of cash received is small.

How we define a cash-based business is any business which has the ability to transact in cash, whether they hold high levels of cash or not.

If you have ANY cash-based clients, regardless of their risk, please answer ‘Yes’.

Why we ask the question:
Cash based businesses can be targets for money launderers because:

- they can be used to integrate from illicit activity (such as from drugs, prostitution etc.) into the financial system; and
- there is a risk of under-declaration of income to reduce tax (i.e. tax evasion).

This definition will include cash-intensive businesses, but is not limited to them. Many businesses now only have a small proportion of cash, following the use of electronic payment systems, but are still considered risky because they could still be at risk of facilitating illegal transactions given their ability to make payments and accept receipts in cash.

A cash-based business is not automatically higher risk. The Know Your Client work that your Firm conducts is very important in understanding the extent of the risk of each cash-based business, which will include important factors like: the nature of the goods and services; the nature of the client’s customers; the cash-controls in place etc. Most Firms who achieve good standards of AML compliance conduct sufficient analytical review work over their cash-based clients’ cash and income levels in order to obtain comfort that the client is not involved in any illicit activities.

Prominent examples of cash-based businesses which are commonly used in the UK to launder money include retail stores including convenience stores, vape shops, petrol stations, newsagents, nail salons, hairdressers, barbers, taxi firms, hotels, bars, money exchanges, cafes, ice-cream parlours, cash-based gambling (amusement arcades for example), scrap-merchants and restaurants.

Where cash-based businesses are used for money laundering, cash is often pooled into larger sums before being integrated into the financial system via bank deposits, money-service businesses, the Post Office (which according to the 2025 NRA is commonly targeted), gambling and purchasing high value goods.

When cash is laundered it is often moved out of the UK via neighbouring countries (France, Belgium, Netherlands), as well as common destinations such as Romania, Turkey, Middle East (e.g. Dubai), and the Far East (e.g. China, Hong Kong). Large volumes of UK cash

generated in the UK are integrated into the Western Balkans, most notably Albania. The UK is often a thoroughfare for cash from illicit activity in the Republic of Ireland.

8. Clients involved with crypto assets

Any clients that trade in, accept or make payment in, or otherwise hold crypto assets.

If you have ANY clients involved with crypto assets, whatsoever, regardless of their assessed risk, please answer 'Yes'.

Why we ask the question:
The 2025 NRA highlights the growth of crypto assets to facilitate money laundering, terrorist financing and proliferation finance. This category was previously included in higher risk industries question but has now been given its own prominence given the fast growth in this area.

A crypto asset is a digital representation of value/contractual rights. The most common types are cryptocurrencies (such as Bitcoin), stablecoins and non-fungible tokens (NFTs)

Crypto assets by their nature, offer anonymity that complicates the tracking of illicit transactions. The pace of crypto technology development challenges regulatory efforts and there is a general lack of effective oversight in crypto, compared to the traditional finance sector.

Bitcoin is used significantly for illicit finance as is stablecoins such as Tether. This is due to the relative price stability, fast transaction speed and wide adoption.

Crypto assets have grown in popularity since 2024 with an estimated 12% of UK adults owning crypto assets. Intelligence reports indicate that they have been increasingly used in the following offences:

- fraud;
- cyber-crime and ransomware attacks where payment is extorted in crypto currency;
- online sexual exploitation and abuse;
- to launder the proceeds from drugs where drug-dealers launder the cash from drug sales into crypto assets, giving the crypto asset providers a means of liquidating significant amounts of crypto assets into cash;
- to evade taxation;
- to evade sanctions.

The NCA assesses that it is likely that hundreds of millions of pounds per year are being laundered through over-the-counter crypto asset brokers in the UK. Over the countertrades are being cashed out in higher-risk countries such as Albania, Colombia, Russia, Singapore, UAE and Vietnam.

There has also an increase in cryptocurrency theft where cryptocurrency assets are stolen directly from the victim's accounts.

Supervised sectors with the highest risk of exposure are crypto asset businesses; retail banking; wholesale banking; wealth management and casinos. Whilst it is currently less commonly seen in the accountancy sector, Firms should still be vigilant to the risks.

Holding crypto assets does not necessarily signify that you act for a higher risk client – whether there are heightened risks will be dependent on many factors including the source of the funds/wealth and the destination of the funds. Firms should be considering all the risk factors in conducting their customer due diligence in order to make an informed risk assessment.

9. Clients involved with informal value transfer systems or money service businesses

Any client which is acting as an IVTS or a money service business

If you have ANY clients which operate as IVTS or money service providers or utilise the services of IVTS or money service providers such as forex-bureaux, regardless of the risk, please answer 'Yes'.

Why we ask the question:
As explained below, the nature of both IVTS and Money Service Providers means that they can be used to launder illicit funds or transfer funds for terrorist financing/proliferation.

Informal Value Transfer Systems

Any clients which are informal value transfer systems (IVTS), money service businesses or), or utilise IVTS or money service businesses in the UK or abroad.

'Informal value transfer systems' (IVTS) is a general term that refers to a wide range of networks used to transfer value from one location to a third party in another. IVTS rely on a network of operators and intermediaries who act as facilitators in transferring money/goods. To make an IVTS payment an individual will approach an operator, often a trusted member of their community, to give them cash or goods and a payment instruction. That operator will contact an operator in a second location who will issue the payment/goods to the recipient, with one or both charging commission and so on until the payment/goods reach their ultimate destination. These providers serve as an alternative for communities where traditional banking systems are less popular, and there are various communities in the UK where they provide a means to send remittances to family/community links in another country. They can be targeted as a means of money laundering, terrorist financing and proliferation financing.

All UK-based IVTS providers are required to register with HMRC as money service businesses and to adhere to the requirements of the Money Laundering Regulations. It is legal to make such transfers in the UK as long as the business is HMRC registered. However, in other countries these providers are often not regulated.

The 2025 NRA provides examples of countries which commonly use IVTS: China; Middle East; Afghanistan; Pakistan; India; Burma; Myanmar; Philippines; Vietnam; and Thailand. It is a common method for laundering monies from drugs, organised immigration crime (human trafficking); tax evasion and fraud.

As part of customer due diligence, each Firms will need to consider whether there are any risk factors for any clients acting as IVTS/money service providers or clients utilise IVTS indicating that they could be higher risk.

Other money service providers

Other non-bank providers which facilitate money transmission including currency exchange (bureaux), check cashing, and pre-paid card services. For the purposes of this question we are ignoring international payment service providers, such as Paypal and Applepay, given this would account for very large numbers of clients, and our focus is on the more unusual situations.

10. Clients operating in sectors vulnerable to organised immigration crime, human trafficking, modern slavery, or sexual exploitation

A client operating in a sector which could be at risk of organised immigration crime, human trafficking, modern slavery, or sexual exploitation.

If you have ANY clients in any sector which has such vulnerabilities (such as those involved in casual labour markets) regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
In accordance with the 2025 NRA and government statistics human trafficking has been on a significant trajectory due to large scale migration caused by political instability in a number of geographic regions, such as the Middle-East for example, those living in poorer third world countries seeking economic opportunities, and those seeking to exploit vulnerable people, and particularly women and children for commercial purposes. Modern slavery includes the offences of human trafficking, servitude, forced or compulsory labour.

Many organisations are vulnerable, and particularly those using more casual labour arrangements or more manual labour. There are vulnerabilities in sectors such as: construction, agriculture, transportation, beauty industries, employment agencies, domestic work, catering industry, garment and textile industries, entertainment, including adult entertainment, and car washes.

However, this list is not exhaustive. Firms should be particularly alert to multiple risk factors which could indicate the existence of Organised Crime Groups – such a client that runs an employment agency and is involved in the property rental sector or agricultural sector for example, or a client which runs both adult entertainment and beauty businesses, or property letting and adult entertainment.

11. High value dealers (HVDs)

A dealer that accepts cash payments of €10,000 or more (or the equivalent in any currency) for goods, whether in a single transaction or a series of linked transactions.

If you have ANY clients in this category, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
As explained in the 2025 NRA, high value goods and traders is one of the oldest money laundering vehicles used by criminals, as goods are purchased and then exchanged back into currency at a later date. Payments can include any form of cash, including notes, coins, or travellers' cheques.

Again, not all High-Value Dealers are high risk, but it is important that the risk factors are appropriately assessed as part of the Firm's CDD procedures.

Examples of High-Value Dealers that could accept cash payments of these amounts include:

- Jewellery and Precious Metal & Precious Stone Dealers.
- Art market participants.
- Antique Dealers.
- Luxury Goods Retailers: Businesses that sell luxury items such as designer clothing, cars, watches, yachts, or other high-ticket items.
- Motor Vehicle Dealers: Dealerships that accept large cash payments for vehicles.
- Real-estate.
- Auction Houses.

- Businesses selling alcohol and tobacco.
- Wholesale cash and carry business.
- Businesses selling supply tools and equipment to tradespeople

HVD businesses must comply with Money Laundering Regulations and should be registered with HMRC for AML supervision if they accept or make high value payments in cash for the following:

- single high value cash payments for a large quantity of low value goods
- high value wholesale or retail transactions
- a single high value transaction made in instalments or on account

HVD businesses must not accept or make a high value cash payment until they have registered as a high value dealer.

More information can be found **here.**

12. Clients with high-risk activities, assets or are in high-risk industries

Activities, asset-holdings or industries which are high risk in that they could be more susceptible to money laundering, trade-based money laundering, terrorist financing, proliferation or proliferation financing (PF).

If you have ANY clients in higher-risk sectors, with higher-risk asset holding, or high-risk activities, please answer 'Yes'. If you have clients operating in any other sectors you consider risky from a money laundering or terrorist financing/proliferation perspective, please answer 'Yes'.

Why we ask the question:
This is a 'catch all' question aimed at identifying high-risk activities, assets, industries not already identified in other parts of this declaration.

A number of activities, assets, or industries are more susceptible to the above risks due to their nature – for example they may have high value portable products or products/services promoting anonymity; they may have significant cross-border transactions; make or sell dual-use goods etc.

Examples of clients with high-risk activities, asset-holdings or high-risk industries include (but is not limited to):

- **Transport, warehousing or shipping:** transport, warehousing and shipping could be used for human trafficking, but could also be used for trade-based money laundering or for the transport, and stockpiling, of weapons or drugs;
- **Other industries susceptible to trade-based money laundering:** import/export businesses, manufacturers which export significantly etc, clients who change their goods services into
- **Defence/arms:** could be used for terrorism or proliferation, for example, or for illegal sales to high-risk or sanctioned countries;
- **Pharmaceuticals:** they can be high value, portable commodities which often traverse multiple countries and intermediaries making them susceptible to money laundering, there is also a significant black-market in counterfeit drugs.

- **Luxury goods market:** can be used as part of money laundering process to convert cash into high value portable goods, or for sanctions avoidance.
- **Dual-use goods:** Sectors with the ability to have dual-use are those which can be used for both civilian and military applications: For example, fertiliser can be used for agricultural purposes but can also be used for explosive-making, and therefore could be involved in proliferation.
- **Waste-management:** the NRA has highlighted that environmental crime is a significant risk in the UK including waste crime, illegal dumping, profits laundered through 'front' companies.
- **Property:** estate agents (are themselves AML supervised) are classed as medium risk in the NRA. Clients holding property through complex structures would be considered higher risk as would clients who are based or overseas buyers using property to potentially obscure illicit funds. Clients holding very high value properties could also be a sign of Organised Crime Group activity.
- **Casinos:** both casino venues and remote casinos can be used to launder significant amounts of cash and are considered by the NRA to be medium risk. They are AML supervised by the Gambling Commission
- **Financial services:** the NRA highlights sectors such as wealth management, insurance and banking as being high risk sectors susceptible to money laundering. In most cases, these entities are AML supervised by the FCA. However, there are some wealth management companies which avail of exemptions (high-net-worth or sophisticated investor exemptions) and may not be subject to the same degree of supervision.
- **Legal services:** whilst also heavily supervised by the relevant professional body this sector is considered high risk, in that legal advisors can wittingly or otherwise act as professional enablers, are involved in the transfer of client funds, property transactions etc.
- **Charities/non-profits/schools/colleges/universities:** these are currently considered low risk in the NRA but this sector has been vulnerable in the past to being used as fundraising for terrorist or proliferation activities. One of the key vulnerabilities highlighted in the 2025 NRA is the abuse of the education sector by criminals, due to the acceptance of tuition fees, grants and donations in cash. Examples include: the admission of a child of an International PEP as a student to a school or college; funding from Russian oligarchs thereby breaching sanctions; Chinese students in the UK being used by organised crime gangs as money mules etc. Organised crime groups are also known to invest in local charity and sports facilities to win 'hearts and minds' in order to reduce the risk of being reported.
- **Football Clubs and football agents:** according to the 2025 NRA these are an attractive target for criminals, including kleptocrats, to launder criminal funds or generate further illicit gains. There are a significant number of financially distressed clubs that make an attractive target for money laundering. Other connected crimes including illegal betting, match fixing, fraud and bribery. In relation to tax evasion there has been a significant rise in spurious Research & Development tax claims which are now the subject of HMC investigations.

Trade-based money laundering (TBML) risk explained:
This is the movement of money or value which is disguised as trade in legitimate goods or services. The National Crime Agency estimates that as much as £10billion is laundered through UK TBML schemes each year.

The complexity, scale, and relative anonymity of the global trade system make it attractive to criminals who seek to hide the movement of criminal funds within the high volume and value of trade transactions.

There are a variety of means by which criminals integrate illicit funds into trade:

- Over and under-invoicing by misrepresenting of the price of goods or services; or
- Mis-stating the quality or type of good to justify value differences;
- Mis-representing the quantity of goods/services (e.g. fictitious transport of goods/service where none are actually transferred, also known as ghost or phantom shipping)
- Issuing multiple invoices for the same transaction to justify multiple payments for the same shipment of goods or delivery of services;

The accountancy sector plays an important role in detecting such fictitious trading, with risk factors including clients diversifying into goods/services not previously traded, clients involving previously unknown third parties in their trade etc. Such crimes involve a significant amount of collusion.

Trade financing and debt factoring are also used to launder proceed of crime.

Proliferation risk explained:
Proliferation is defined as the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, including both technologies and dual-use goods used for non-legitimate purposes. Proliferation Financing is the means to finance those activities.

The list of industries above is not exhaustive and you may have other clients in sectors that you consider to be risky from a money laundering, terrorist financing or proliferation perspective.

13. UK PEPs:

An individual who is entrusted with a prominent public function in the UK, other than as a middle-ranking or more junior official.

If you have ANY clients who are UK PEPs, or known family members or close associates of a UK PEP, in accordance with FCA guidance, this question should be answered 'Yes'.

Why we ask the question:
PEPs (as well as their families and persons known to be close associates) are required to be subject to enhanced scrutiny by Firms subject to the Money Laundering Regulations 2017. This is because international standards issued by the Financial Action Taskforce (FATF) recognise that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

As FATF says '*these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatising PEPs as such being involved in criminal activity*'.

It is because of their function that a person becomes a PEP and is required to be subject to enhanced scrutiny by Firms. Likewise, a PEP's family or close associates may also benefit from, or be used to facilitate, abuse of public funds by the PEP. It is as a result of this connection that family and known close associates are required to be subject to greater scrutiny. Family and close associates are not themselves PEPs solely as a result of their connection to a PEP.

A list of prominent functions is given in regulation 35 (14). The FCA issued revised Guidance on 15 July 2025 - linked **here** – provides detailed guidance on what public roles within the UK are classified UK PEPs and how UK PEPs are treated.

Examples of prominent functions are given below (this is not an exhaustive list):

- Heads of state or government, ministers, deputy and assistant ministers
- Members of parliament or similar legislative bodies
- Members of governing bodies of political parties
- Members of supreme courts
- Members of courts of auditors or of the boards of central banks
- Ambassadors, charge d'affaires and high-ranking officers in the armed forces
- Members of administrative, management or supervisory bodies of state-owned enterprises.

14. International PEP clients

An individual who is entrusted with a prominent public function in a foreign country, other than as a middle-ranking or more junior official.

If you have ANY clients who are International PEPs, or known family members or close associates of a PEP, in accordance with this FCA guidance, this question should be answered 'Yes'.

Why we ask the question:
Similar to the position with UK PEPs, the risk with International PEPs is that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

Corruption is assessed to cost the global economy billions, if not trillions of pounds every year. It also undermines trust in governments and institutions. A considerable threat to the UK arises from overseas PEPs laundering illicit gains through the UK.

The Money Laundering Regulations defines International PEPs as individuals who hold or have held similar prominent positions in a foreign country.

Examples of prominent functions are given below

- Heads of state or government, ministers, deputy and assistant ministers
- Members of parliament or similar legislative bodies
- Members of governing bodies of political parties
- Members of supreme courts
- Members of courts of auditors or of the boards of central banks
- Ambassadors, charge d'affaires and high-ranking officers in the armed forces
- Members of administrative, management or supervisory bodies of state-owned enterprises.
- Directors, deputy directors and members of the board of equivalent of an international organisation (e.g., United Nations, Nato).

Family members (spouses, civil partners, children, parents, siblings) and close associates of International PEPs may also be considered PEPs due to their potential influence or access to funds.

As before, please see the **FCA Guidance** for further information .

15. Non face-to-face clients

A client where there are no 'in-person' interactions.

If you have ANY remote clients, regardless of the risk assessment, you should answer 'Yes'.

Why we ask the question:
In this digital age it is becoming more common for Firms to engage with, and provide services to, clients remotely and on-line. The absence of in-person interactions can increase the difficulty of verifying client identities (i.e. to ensure such clients 'are who they say they are'), detecting suspicious behaviours or truly understanding the business or conducting sufficient 'Know Your Client' work.

The NRA has indicated that Artificial Intelligence (AI) is being used to use stolen, hijacked or synthetic (fraudulent accounts set up by cyber criminals) accounts to facilitate money laundering. Generative AI could potentially help criminals to pass Firms' onboarding checks by creating synthetic identities or generating images to match stolen documents.

Given these risks, Firms should have appropriate policies and procedures in place to identify such clients and ensure that these increase risks are mitigated. The Firm could, for example, also use an electronic CDD platform which includes facial recognition for additional security. Where a client cannot be met face-to-face, the Firm may wish to meet the client over an online platform such as Teams or Zoom, which would reduce the AI impersonation risk.

16. Clients with a criminal record or has criminal ties

A person who has a criminal record that is a relevant offence or is connected to such a person.

If you have ANY such clients with relevant offences, regardless of the risk assessment, you should answer 'Yes'.

Why we ask the question:
Clients with a history or connection with criminal activity, that could be relevant to a money laundering, terrorism or proliferation offence, are likely to pose a very high risk of money laundering to your Firm. Each Firm should consider a client's criminal record, or potential ties with criminals, before taking on a client and in regularly assessing the client's money laundering risk.

Relevant offences include those associated with economic crimes like fraud, bribery, dishonesty, tax offences and breaches of money laundering regulations, drugs offences, organised crime groups, human trafficking etc.

Not all offences increase the money laundering risk. For example, a motoring offence need not be included.

17. Scottish Limited Partnerships

A form of limited partnership registered under Scots law.

Please answer 'Yes' if you have ANY SLP clients, regardless of the risk assessment, and to provide the number of SLPs.

Why we ask the question:
Unlike other UK limited partnerships, SLPs have legal personality, which allows them to hold assets and enter into contracts in their own right. Prior to 2017, the ownership of an SLP did not require to be disclosed in SLP filings. This made SLPs attractive to those wanting to hold assets, such as property, anonymously and became popular as a money laundering vehicle, to hold property from criminal proceeds.

From 26 June 2017 onwards, SLPs are now required to disclose persons with significant control to Companies House, which has led to a large drop in their use as a money laundering vehicle.

18. Clients where the structure, or nature of business/transactions is unusual or complex

This question potentially covers a wide range of potential scenarios which may be complex or unusual including (but not limited to) clients in the following scenarios:

- **where there are layers of ownership and control (that may or may not involve overseas entities) that make it more complex to determine the ultimate owners**;
- **arrangements which would promote anonymity, such as nominee shareholders, bearer shares or nominee directors;**
- **where dormant or shell companies are being utilised (i.e. are nor dormant/shell);**
- **where a succession of failed legal entities are being utilised (called 'phoenixing');**
- **where the source of funds in the business are unusual or unknown;**
- **where the client has raised funds through crowdfunding;**
- **where there are changes to trade/goods and services/ trading patterns, with no obvious commercial reason;**
- **where the client has multiple bank accounts or foreign accounts with no good reason;**
- **unusual, complex transactions or business arrangements;**
- **arrangements/ activities where there is no apparent economic or legal purpose;**
- **the client's lifestyle and/or transactions are inconsistent with known business and personal information;**
- **where there are contractors or agency workers paid by an umbrella company (which might be used to allow agency workers to keep more of their earnings and avoid paying tax);**
- **where government support schemes or grants are claimed over which there is no apparent valid justification or are not being used for valid business purposes.**

If you have ANY clients in any of these scenarios, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
All of the above risk factors could indicate illicit activities. Where, following your customer due diligence it is clear that the arrangement makes business sense or has a clear commercial reason, the risk is obviously reduced.

19. Unknown beneficial ownership

Where the identity of the person or people who ultimately own or control a legal entity or asset is unknown.

If you have ANY such clients, please answer 'Yes'.

Why we ask the question:
A beneficial owner is a person who has the right to control or own an asset such as a company or property.

Identifying beneficial ownership is a key component of AML compliance and is a legal requirement. By requiring the disclosure of beneficial ownership, authorities can enhance transparency, prevent illicit activities, and ensure the integrity of financial markets.

Without knowing who the beneficial owner it is impossible to ensure that, for example:

- the Firm is not engaging with a criminal, terrorist or a sanctioned person;
- the Firm is not engaging with a sanctioned or high-risk country;
- the source of wealth of a client does not come from illegal activities;

to name a few risks.

Guidance on identification of beneficial owners for different types of entities is included in the **CCAB AML Guidance**.

20. Clients outside of your normal client base

A client which is outside your normal client base for reasons such as (but not limited to):

- **a client based in a location significantly different from your normal client base;**
- **a client involved in sectors significantly different from your normal client base;**
- **a client introduced to your Firm through intermediaries or third parties who are not well-known by you;**
- **a client where the Firm is only engaged to conduct a one-off transaction, and this is unusual for your Firm given your usual client base or services provided;**
- **a client which has changed professional advisors several times in a short space of time;**
- **the client engages with several professional advisors for different accountancy services;**
- **another professional advisor refused to provide the service to the client;**
- **the customer is prepared to pay substantially higher fees than usual, or requests the engagement be completed in tight deadlines;**
- **the client's previous professional advisor was not a comparably sized Firm;**
- **supply chain risk: professional services are being provided to the client across multiple jurisdictions which might result in the identity of the ultimate beneficial owner to be obscured or the purpose of the entity involved in the transaction (or the purpose of the transaction itself) being obscured from the Firm.**
- **the client engages with the Firm only to deal with a tax investigation.**

If you have ANY clients meeting any of the criteria, regardless of the risk assessment, please answer 'Yes'

Why we ask the question:
Accountancy Firms can be engaged, unwittingly, as professional enablers to facilitate economic crime. This question highlights a number of potential risk flags which might indicate that the Firm is being targeted.

The CDD procedures should be directed towards investigating the risk flag and removing any doubts over the reason why the Firm is being asked to act for the client.

Clients are reminded of both their legal and ethical obligations in relation to client acceptance and continuance and that Firms should remain vigilant.

21. Does the Firm hold clients' money/use a Clients Money account

A bank account in the name of the Firm which holds money on behalf of clients. This also includes estate bank accounts held by Insolvency Practitioners.

You are asked in this question whether you hold ANY client money or estate accounts - if you do, please answer 'Yes'.

Why we ask the question:
A client money bank account should only be used for receiving or making payments which relate to accountancy-related services which the Firm is performing, has performed or has been engaged to perform, for the client.

Similarly, an estate account should only be used in compliance with the Statement of Insolvency Practice.

Holding a client money account or estate bank account puts the Firm at higher risk in relation to money laundering as they could be used to launder proceeds from crime.

It should not be used as banking facility for clients and Firms must remain vigilant and take steps to obtain and hold sufficient information to ensure that the client bank account or estate account is being used for a lawful and legitimate purpose and for bona fide transactions.

Firms are reminded that sufficient CDD procedures must be conducted when receiving or paying out monies from a client money or estate account to ensure that the Firm does not inadvertently become involved in the transfer of illicit funds.

22. Does the Firm trade from premises outside the UK or outsource services to service providers outside the UK

Where the Firm operates from premises outside the UK (including a second home or office abroad), or outsources services to service providers outside the UK.

If your Firm has, or outsources, operations abroad, please answer 'Yes'.

Why we ask the question:
This may increase your money laundering risk because you may be providing engagement services to UK clients in a jurisdiction that has less robust AML requirements than the UK.

For example, say your Firm outsources bookkeeping and payroll services for UK clients to subcontractors based in South Africa, there is a risk that these persons are not sufficiently trained or knowledgeable on the UK money laundering regulations or are not sufficiently knowledgeable about the Firm's AML policies or procedures or the risks associated with those UK clients. It is therefore important that the Firm, in this example, ensures that the overseas subcontractors are appropriately trained on the UK AML requirements; that they comply with the Firm's UK AML policies and procedures; that the Firm has shared the Firm's Firm-Wide Risk Assessment to the subcontractor so that they understand the risks in the Firm; that the subcontractors are trained on, understand and comply with the Firm's internal reporting procedures; that the subcontractors understand the UK client's risk assessment etc. This list is not exhaustive.

Another example would be where you live abroad or have an office abroad and act for both local clients abroad as well as UK clients. There is a risk that you apply local requirements, rather than UK requirements, to the UK clients.

23. Accounts preparation

The process of preparing financial statements for a business or organisation.

If you provide ANY accounts preparation services, regardless of risk, please answer 'Yes'.

Why we ask the question:
The 2025 NRA views accounts preparation as being at high risk of money laundering as there is the risk that the Firm could be used as a professional enabler i.e. provide legitimacy and respectability by producing accounts for a person involved in money laundering.

For example, a Firm is involved in preparing the accounts for a cash-based business which, unknown to the Firm, has had illegal funds flow through the business. By producing the accounts, and not identifying the potential risks posed by the client, the Firm has acted inadvertently as a professional enabler by producing the accounts which lends an air of legitimacy and reputation as it has been prepared by a Firm of Chartered Accountants.

24. Tax compliance

Adhering to tax laws and regulations by correctly reporting income, expenses and other financial details to the relevant tax authorities. This includes the filing of tax returns, advising on tax liabilities/due dates, standard remuneration planning and timing of fixed asset purchases for capital allowance purposes.

If you provide ANY tax services, regardless of risk, please answer Yes'.

Why we ask the question:
Similar to accounts preparation, the 2025 NRA views tax compliance work as being at high risk of money laundering as there is the risk that the Firm could be used as a professional enabler i.e. provide legitimacy and respectability by producing tax returns for a person involved in money laundering, terrorist financing or proliferation.

For example, a Firm is involved in preparing the tax return for a cash-based business which, unknown to the Firm, has under-declared income. By producing the tax return and not having

conducted sufficient analytical work to identify under-declared income, the Firm has acted inadvertently as a professional enabler by producing the tax return which lends an air of legitimacy and reputation as it has been prepared by an ICAS supervised Firm.

The 2025 NRA highlights, in particular, the prevalence of 'phoenixing' in relation to tax evasion, whereby criminals may carry on a similar business successively through a serious of companies where each becomes insolvent in turn.

Another risk highlighted in the AASG Accountancy Sector Risk Outlook is clients who work as contractors or agency workers paid by umbrella companies. An umbrella company might use contrived arrangements that claim to allow agency workers and contractors to keep more of their earnings. These arrangements are tax avoidance schemes and most likely not compliant with tax rules.

Firms are also reminded of their ethical obligations under the '**Professional Conduct in Relation to Taxation**' ('PCRT'). This includes detailed guidance on how to deal with under-declared tax or tax errors.

25. Tax planning

This includes evaluating the overall financial situation and developing strategies to ensure the minimum legal amount of tax is paid.

Examples of tax planning would include succession planning, advising in connection with the sale or purchase of a business, IHT planning, R&D advisory work and capital allowance reports.

This would generally not include routine tax advice in connection with year-on-year remuneration planning and timing of fixed asset purchases.

If you provide ANY tax planning services (other than routine tax advice), regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
This can, at times, be considered high risk as it could involve facilitating planning for those whose assets and businesses are involved in illegal activities.

For less 'tested' or more aggressive tax efficient schemes, the Firm could risk bordering into tax evasion. For example, there have been recent HMRC investigations into R&D tax claims, some of which are found to be erroneous or fraudulent.

The 2025 NRA highlights, in particular, the prevalence of 'phoenixing' in relation to tax evasion whereby criminals may carry on a similar business successively and evade the payment of tax through a serious of companies where each becomes insolvent in turn.

Firms are also reminded of their ethical obligations under the '**Professional Conduct in Relation to Taxation**' ('PCRT'). This includes detailed guidance on how to deal with under-declared tax or tax errors.

26. Payroll

The provision of payroll services to a client including calculating the wages and salaries and the associated payroll taxes.

If you provide ANY payroll services, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
The AASG Risk Outlook identifies payroll services as being one of the mainstream accountancy services which is at most risk of exploitation and is considered high risk. One such risk is the use of ghost employees i.e. fake persons being set up on the payroll in order that payments out of the business appear to be legitimate payments.

27. Bookkeeping/VAT

The keeping of the financial books and records, and recording client's transactions.

If you provide ANY payroll/VAT services, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
It is considered a high-risk activity in accordance with the AASG Risk Outlook as bookkeepers can enable money laundering by transferring money or creating paperwork to legitimise the flow of funds, both unwittingly and knowingly. This can include under-declaration of income for tax evasion, or over-declaration of income for money laundering. This can include trade-based money laundering, where invoices are created in the absence of a sale, or invoices inflate the value of goods sold. Records can also be created to hide the existence of taxable assets. This can legitimise large amounts of illicit funds.

Similarly keeping the VAT records and making VAT returns is also high risk and can risk sales being under-declared in order to avoid VAT, clients failing to register for VAT, VAT reclaim fraud being perpetrated.

28. Insolvency

The services conducted by a licensed Insolvency Practitioner (IP).

If you provide ANY insolvency services, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
They are considered to be of high risk of money laundering by the 2025 NRA and the AASG Risk Outlook which states '*There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company'*.

Insolvency by its nature exposes the IP to many money laundering risks given the nature and types of debtors that the IP may have to, on occasions, act for. A few risks are listed here: cash-based businesses; clients with a criminal background; clients with directors' misconduct; Bounce Back Loan fraud; employee fraud; criminals setting up and winding up businesses regularly; debtors unwilling to provide books and records or not cooperating; directors misappropriation of assets; illegal directors' loans; books and records failures; underdeclared income etc.

29. Corporate finance

Where the Firm is involved in advising on, negotiating relating to the capital structuring, financing and investment decisions of a client.

If you provide this service, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
Corporate finance includes services in relation to raising finance (loans and equity); mergers; acquisitions; buy-ins and buy-outs; selling and purchases other businesses; business structuring; raising capital; raising start-up funds; conducting due diligence; raising finance via high-net-worth investors etc.

Many corporate finance activities will be lower risk. However, corporate finance can become higher risk given that corporate entities are commonly used to conceal the ownership of criminal assets and facilitate the movement of money.

The CDD procedures will require to establish the risks associated with the nature of the business and the nature of the transactions the Firm has been asked to advise on.

Examples where corporate finance could be used include, for example: the Firm inadvertently becoming involved in arranging the sale of a business to an Organised Crime Group; or the Firm becomes involving in arranging deals for a high-net-worth business 'angel' whose source of wealth is from illegitimate sources.

30. Probate, estate management or executry

Dealing with the assets, debts and taxation of person's estates before or after death.

If you conduct ANY probate or estate administration service, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
While the risk will generally be considered lower there is always the risk of the Firm acting for a client where the source of wealth is from illegal means.

31. UK regulated agent/Overseas entity agent work

Assisting overseas entities (e.g. foreign companies, trusts, or partnerships) in complying with legal requirements to register and disclose their beneficial ownership.

If you conduct this service, regardless of the risk assessment, please answer 'Yes'.

Why we ask the question:
Under the UK's Register of Overseas Entities (introduced by the Economic Crime (Transparency and Enforcement) Act 2022), overseas entities that own or intend to acquire land or property in the UK must:

- Identify and verify their beneficial owners (or managing officers if no beneficial owners meet the required thresholds).
- Submit the required information to Companies House.
- Keep the information updated annually or when changes occur.

More information can be found **here.**

This work is considered high risk given the Firm is essentially certifying that the beneficial owner information is correct, which is a higher bar than the customer due diligence work required under the money laundering regulations. An ICAS 'AML in focus' video explains the risks and can be accessed **here.**

32. Is your Firm an Authorised Corporate Service Provider (ACSP) providing ID Verification (IDV) services for clients on Companies House

Where the Firm has been authorised by Companies House as an Authorised Corporate Service Provider (ACSP) and is providing identity verification services for clients on the Companies House website.

If you are authorised to conduct this service, please answer 'Yes'.

Why we ask the question:

The Economic Crime and Corporate Transparency Act 2023 introduced requirements for all directors and PSCs to verify their identity at Companies House. Third parties, such as accountants, who want to verify on behalf of their clients require to be registered as an Authorised Corporate Service Provider (ACSP).

This work is high-risk for similar reasons to the UK Register of Overseas Entities work:

- there is a risk that those clients who do not want to reveal their identities may take steps to obscure it;
- the complex nature of the verification work required means that the accountant may not perform sufficient work to meet the requirements for the work. The verification work required for the IDV standard for ACSPs is not the same as the risk-based approach to client due diligence under MLR17, as like the ROE work the Firm is effectively certifying that the identity of the directors and PSCs, which is a far higher bar.

ICAS has an article **here.**

33. TCSP services

These include: legal entity formation (companies, trusts, partnerships etc); providing a registered office; arranging for a person to act or acting as a director, company secretary or trustee; and submitting confirmation statements.

If you provide ANY such service, please answer 'Yes'.

Firms conducting TCSP services are required by law to be registered with their AML supervisor to do so. If you conduct TCSP services, you must disclose this to ICAS.

The TCSP section is one of the most important sections in the return as all Firms conducting such services must appear on the TCSP register and failure to disclose any of these services is a criminal offence.

Please note that it does not matter how infrequently you might do TCSP work, or whether it might be provided as ancillary to some other service. Compliance with the regulations is still required in all cases.

Why we ask the question:
The 2025 NRA assesses legal entity formation (e.g. company or trust formation) and associated services as one of the highest risk services as Firms can become involved, albeit inadvertently, in establishing and administering legal entities that are being used to conceal the ownership of criminal assets and facilitate the movement of money.

Please note that if you act as a director, company secretary or a trustee and you bill for this service through your Firm, this is a TCSP service.

34. Company formation

The formation of company and other legal entities.

If your Firm forms companies or other legal entities (such as SLPs or LLPs) please answer 'Yes'.

Why we ask the question:
As explained previously the formation of legal entities is considered high risk in the National Risk Assessment.

The 2025 NRA highlights, in particular, the prevalence of 'phoenixing' whereby criminals may carry on a similar business successively through a serious of companies where each becomes insolvent in turn.

The NRA also highlights the use of apparent 'dormant' or shell companies to launder criminal funds.

35. Trust formation

The formation of trusts or similar vehicles.

If you Firm forms trusts, please answer 'Yes'.

Why we ask the question:
As explained previously the formation of legal entities is considered high risk. The 2025 NRA highlights that the misuse of trusts for money laundering remains a global problem. They are rarely used in isolation, but as part of complex structures layered with corporate structures.

Trusts are often used as the last step in the money laundering process after other laundering methods have been used to disguise the origin of funds. Trusts can provide the appearance of distance between the settlor and the assets, when in reality the settlor may maintain a level of control over the assets.

Trust arrangements are often more complicated than corporate structures and likely require professionals to establish. While trusts have been identified in significantly fewer cases than corporate structures, they tend to be of higher value, frequently in the tens of millions of pounds and often linked to international corruption, sanctions evasion and serious fraud.

36. Providing registered office

Where your Firm provides the main 'official' address for a legal entity.

If your Firm provides this service, please answer 'Yes'.

Why we ask the question:
Providing such services when associated with other TCSP services could be considered high risk. It will depend on the nature of the client and the nature of all services provided.

37. Arranging / acting as director / secretary

Arranging for someone to act, or acting as: a director, or company secretary of a company; partner of a partnership or other similar position in another legal entity.

If your Firm provides this service, please answer 'Yes'.

Why we ask the question:
This is where a person in your Firm acts as:

- a director or company secretary to a company.
- a partner of a partnerships; or
- in a similar capacity in relation to other legal entities.

The Firm need only include director or company secretary services where the Firm is billing the client through the Firm. Where the position is held in a personal capacity and not billed through the Firm these are excluded.

It also includes where your Firm arranges for another person to be the director or company secretary. For example, the main Firm may arrange for a subsidiary of the Firm to take on all the Company Sectary roles for clients with the main Firm conducting the billing. In that case as the fees are billed through the main Firm the main Firm is arranging for someone else to be the company secretary and needs to be a TCSP.

Please note that nominee director/shareholder services are included here (which is defined in 18 above). If such services are provided these can be considered higher risk given that these services could be used, if appropriate controls are not in place, to facilitate concealment.

Further advice is provided on the government website **here**.

38. Arranging/ acting as a trustee

This is where your Firm, or a person in your Firm, acts as a trustee of a trust or arranges for another person to be the trustee.

If your Firm, or someone in your Firm, provides this service, please answer 'Yes'.

Why we ask the question:
If such services are provided these can be considered higher risk depending on the nature of the trust, its geography, the assets held etc. as they could be used for concealment.

39. Submitting a confirmation statement

If you complete and file a confirmation statement on behalf of a client, please answer 'Yes'. If you are only filing what the client has completed, then please answer 'No'.

Why we ask the question:
The confirmation statement is the responsibility of the client's directors. If the Firm submits a confirmation statement on behalf of a client it may be considered higher risk given the Firm is taking on a responsibility that belongs to the directors, and because the Firm is essentially certifying that the information is correct. The Firm is therefore at risk if they provide information which is not accurate or conduct the service for a company which has been used for concealment. The risk will depend on the nature of the client and the controls in place.

40. For how many clients do you provide TCSP service for?

Please add up the number of clients for which you conduct all of the above services i.e. company and trust formation; registered office; director, company secretary and trustee services; and confirmation statements.

41. How many legal entities has your Firm formed in the last 12 months?

Please sum the total number of company, partnership, trust and other legal entity formations in the year.

42. Of those, how many have beneficial owners are resident overseas?

Please indicate in how many entity formations (whether it be company, trust, partnership, or other legal entity) there were beneficial owners resident overseas.

43. How many companies does your Firm act as a registered office for?

Please sum the total number of legal entities for which the Firm provides the registered office.

44. How many companies does your Firm conduct director services for?

Please sum the total number of legal entities for which the Firm/a person in the Firm provides director services. This includes any shadow director services where there is no director appointment, but the Firm/person is acting in this capacity.

45. How many companies does your Firm conduct nominee director or nominee shareholder services for?

Please sum the total number of appointments where your Firm, or a person in your Firm acts as a nominee shareholder or director.

Why we ask the question:
A nominee service is where a business owner has appointed the Firm to act on their behalf. Nominee situations are often considered high risk because it can be used to facilitate anonymity i.e. can allow the true director/shareholder that controls the business to hide behind the nominee director/shareholder.

46. How many trusteeships do you conduct for overseas trusts?

Please sum the total number of trusteeships held by the Firm or someone within the Firm that relate to trusts registered overseas or which have overseas beneficiaries.

Why we ask the question:
As explained previously, trusts are often used as the last step in the money laundering process after other laundering methods have been used to disguise the origin of funds. Trusts can provide the appearance of distance between the settlor and the assets, when in reality the settlor may maintain a level of control over the assets. Overseas trusts in particular may be established in jurisdictions with less scrutiny, less stringent AML supervision, with more attractrive tax-offshoring opportunities and to facilitate the disguising of the beneficiaries.

47. How many SARs were submitted in relation to TCSP services?

Please total the number of Suspicious Activity Reports made in relation to TCSP services i.e. company, trust, partnership etc formation; director, company secretary and trustee services; registered office services; or confirmation statements.

Why we ask the question:
Given the higher risk nature of TCSP services and the potential for corporate entities to be targeted in the laundering of illicit funds, there would expected to be a higher awareness of ML/CTF/proliferation risks and therefore the potential for SARs to be made.

48. Regulatory Compliance

Most of the sections in this section should be self-explanatory to Firms as they should be embedded in your Firm's AML policies and procedures. Only the less frequent questions have been explained below.

IMPORTANT NOTICE:
A number of Firms have received regulatory penalties for stating that they have the required AML policies & procedures in place, which are then not evident during a monitoring visit. Firms MUST only confirm that they have the policies & procedures in place if that is the case.

Where the Firm has identified it cannot confirm that all such policies & procedures are in place you must take immediate effective action to rectify the position.

- **Have all BOOMs obtained basic disclosure checks?**

  As explained in Section 1 you should ensure that all Beneficial Owners, Officers and Managers in your Firm have been approved by ICAS as BOOMs and that they are disclosed on this declaration**.** Before an individual is approved by ICAS as a BOOM Section 26(7) of the Money Laundering Regulations 2017 requires the firm to obtain evidence, via a disclosure check, that the individual has not committed a 'relevant offence'.

  The firm will be asked to confirm that this has been conducted during the application process. There is no need to update disclosure checks annually. However, where the firm becomes aware that a 'relevant offence' has been committed by a BOOM the Firm must notify ICAS immediately. Section 26(10) requires notification within 30 days of becoming aware of the conviction (the individual themselves has an obligation to notify the firm within 30 days of receiving a conviction).

  This question therefore asks you to confirm that disclosure checks have been obtained for all BOOMs in your Firm.

- **Have you made any Defence Against Money Laundering (DAML) SARs in the last calendar Year?**

  Why we ask the question:
  A Defence Against Money Laundering (DAML) requires to be requested from the NCA where the Firm has made SAR to the NCA and has a suspicion that property they intend to provide services in relation to is in some way criminal, and that by dealing with it they risk committing one of the principal money laundering offences under the Proceeds of Crime Act 2002 (POCA). It is also needed before the Firm is about to accept fees from a client where it suspects that the fees will come from/tainted with criminal property.
  We require to know whether any DAML requests were made in the last year.

- **If yes, how many DAMLs have been submitted to the NCA during the period of the return?**

  Why we ask the question:
  For the reasons set out in the last question.
  Please sum the number of DAML requests made in the last 12 months.

Thank you for your cooperation and completion of the AML declaration