AASG
Accountancy AML Supervisors' Group

AASG risk outlook: Money laundering, terrorist financing and proliferation financing risk in the accountancy sector

22 September 2025

Contents

WHAT IS THE PURPOSE OF THIS DOCUMENT?

The impact of money laundering is devastating – it enables serious organised crime such as modern slavery, drugs trafficking, fraud, corruption and terrorism.

A comprehensive risk assessment is key to understanding the money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks that a business is exposed to. By knowing and understanding the risks to which the accountancy sector is exposed, HM Government, law enforcement, and the professional body supervisors, as well as the accountancy firms themselves, can work together to ensure that criminals find it difficult to exploit accountancy services.

In this document, we have set out the key risks, and red-flag indicators, the AASG consider are relevant to the accountancy sector. We will update it on a regular basis, reflecting the UK's National Risk Assessment and other emerging threats and trends.

We recommend that firms read the NRA, alongside the AASG Risk Outlook, as together these documents provide detailed information on the threats and vulnerabilities in the UK and detail on the red flags and indicators for the key risk areas.

WHO DOES IT APPLY TO?

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 and proliferation financing.

This guidance is for auditors, insolvency practitioners, external accountants and tax advisers, as well as firms providing trust or company services. Firms 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 and/or terrorist financing and/or proliferation financing.

The firm's written risk assessment will identify the areas of the business that are most at risk and this will enable the firm to focus resources on the areas of greatest risk. It is the responsibility of the firm's senior management to approve, document and implement the policies, controls and procedures that address and mitigate the risks. The firm must also provide training to staff on the risks and how the firm mitigates those risks (eg, through client due diligence procedures).

OVERARCHING UK MONEY LAUNDERING RISKS AND THREATS

The UK remains highly exposed to money laundering risks, driven by its position as one of the world's largest and most open economies. The UK's prominence in financial and professional services and its openness to trade, investment, and ease of doing business creates vulnerabilities that criminals exploit.

Geopolitical changes have led to increased connections between money laundering, kleptocracy, and sanctions evasion. Individuals and entities under sanctions are making greater use of established laundering networks—including international controllers, professionals, and complex organizational structures—to conceal the sources of their funds. These methods, previously mainly associated with the movement of criminal proceeds, are now also being applied for the purpose of circumventing sanctions.

Technological advancements have further reshaped the risk landscape. The UK's status as a fintech hub has led to widespread integration of Electronic Money Institutions (EMIs) and Payment Service Providers (PSPs) into the financial system. While most transactions are legitimate, the widespread adoption of these platforms allows criminals to operate undetected. Cryptoassets have also surged in popularity amongst the general population but this has been mirrored with cryptoassets being increasingly featured in money laundering intelligence, often facilitated by overseas crypto service providers. Their use is linked to rising fraud and ransomware attacks, where payments are demanded in cryptocurrencies. Artificial Intelligence (AI) presents a dual-edged sword. While it offers potential for enhanced detection and prevention of money laundering, it also empowers criminals to bypass AML controls and commit predicate offences like fraud more efficiently. AI can accelerate the movement of illicit funds across broader networks, complicating enforcement efforts.

Despite these evolving threats, several persistent risks remain:

- Cash-based money laundering continues to be prevalent, even as regulated cash use declines. Traditional methods—such as cash smuggling, use of cash-intensive businesses, money mules, and exploitation of legitimate channels like Post Offices—are still widely employed by criminals.

- Financial and professional service firms remain vulnerable to exploitation by organized crime groups seeking to integrate illicit funds into the legitimate economy.

- UK companies are frequently used in laundering schemes, both by regional organized crime groups employing front companies and cash-intensive businesses, and by high-end cross-border criminals using complex corporate structures to move illicit funds.

Money laundering affects all regions of the UK. Cities, particularly London, attract cross-border and complex laundering due to their concentration of financial and professional services. Rural areas are susceptible to local and regional organized crime groups, who often rely on cash and exploit smaller, locally based professional services firms to launder proceeds.

Money laundering threats

The NRA 2025 summarises the most common predicate offences that generate criminal funds. The nature of accountancy services means that it is possible for any firm to come across these predicate offences however, some predicate offences are more obviously linked to specific services such as tax advice and tax evasion, or payroll and modern slavery/human trafficking.

Fraud	• Continues to be the most prevalent predicate offence for money laundering in the UK, accounting for a significant proportion of Suspicious Activity Reports (SARs). • Includes a wide range of schemes such as investment fraud, authorised push payment fraud, and COVID-related scams. • Increasing use of digital platforms and social engineering tactics has made detection and disruption more complex.
Sanctions evasion	• Criminals and hostile state actors exploit weaknesses in compliance systems to circumvent UK and international sanctions. • Use of complex corporate structures, offshore jurisdictions, and professional enablers to obscure beneficial ownership and transaction flows.
Acquisitive crime	• Includes burglary, theft, and robbery, often linked to organised crime groups. • Stolen goods are either sold to generate cash, which is laundered through traditional techniques, or used as a store of value.
Drugs	• Mainly laundered through cash-based techniques, particularly for street-level and wholesale drug trafficking.
Cyber crime	• Rapidly growing threat with criminals using ransomware, phishing, and malware to steal funds and personal data.
Organised immigration crime	• Linked to human trafficking and exploitation, generating illicit profits that are laundered through informal value transfer systems money service businesses.
Tax evasion	• Involves deliberate underreporting of income, offshore tax havens, and misuse of trusts and shell companies. • Professional service firms are particularly exposed to the risk of being used.
Modern slavery and human trafficking	• Victims are exploited for labour or sexual services, with proceeds laundered via money mules. • Often overlaps with other criminal activities such as drugs and immigration crime.
Online child sexual exploitation and abuse	• Generates illicit income through the sale of abusive material, often paid for using cryptoassets or EMIs and PSPs.
Environmental crime	• Includes illegal waste disposal, wildlife trafficking, and logging, often linked to transnational organised crime. • Proceeds are laundered through trade-based schemes and shell companies
Bribery and corruption	• Involves misuse of public office and corporate bribery, often facilitated by opaque financial structures. • Laundered through offshore accounts, luxury goods, and real estate.

THE OVERALL RISK OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE ACCOUNTANCY SECTOR

The Economic Crime Plan 2023-2026 identifies economic crime as a rapidly growing and increasingly complex threat to UK national security and prosperity. Criminals continue to seek ways to commit, and benefit from, economic crime including fraud, money laundering, sanctions evasion and corruption, fuelling the serious organised crime that causes significant societal harm as well as threatening the interests of legitimate businesses and undermining the UK's international reputation.

The National risk assessment of money laundering and terrorist financing 2025 (NRA) highlights the significant role accountants play in the UK's financial system, which makes it a target for money laundering, and there are a range of services offered by the sector which can be used, or abused, by criminals. The risk of terrorist financing remains low.

Criminals need someone professional, capable and trustworthy to make the necessary arrangements to disguise the source of funds and the flow of those funds. To ensure this method of money laundering is effective and successful, the criminals need professional service providers to provide the skills, knowledge and expertise to unlock access to the kind of complex processes that can provide the necessary anonymity, or obfuscation, for the criminal. Consequently, many of the services provided by professional service providers in practice may potentially be exploited by criminals in this way – we have described the key services below.

Any service where the professional service provider offers a veneer of respectability is at risk of being exploited for ML. This document applies to all auditors, insolvency practitioners, external accountant and tax advisers (as set out in Regulation 11 of the MLR17) – collectively referred to as 'accountancy services' throughout this document.

The accountancy services considered most at risk of exploitation are:

- providing accountants certificates of confirmation;
- payroll services (particularly for payroll-only clients);
- tax advice services; and
- trust and company services.

The NRA describes the key vulnerability of the sector as being **poor compliance with the MLRs**, as criminals will seek to take advantage of weak or inadequate risk assessments, policies, controls and procedures. Other key vulnerabilities are fragmentation of services and supply chains, which we have explored further below.

These risks and vulnerabilities can be well-managed through effective AML policies, procedures and training, in line with the AML Guidance for the Accountancy Sector (AMLGAS). Firms should tailor their AML policies and procedures to address the risks identified in their firm-wide risk assessment and that are present in a particular service line or client.

The **terrorist financing risk** for accountancy firms remains low, with no evidence of abuse since 2020. However, accountancy firms that also provide trust and company services should be aware that the terrorist financing risk for TCSPs has increased from low to medium. This is due to the potential for UK-based company and trust arrangements to receive funds from entities that may

knowingly or unknowingly support terrorism. Firms offering such services should take note of this elevated risk and ensure they have factored this change into their firmwide risk assessments.

The National risk assessment of proliferation financing sets out that a vulnerability to proliferation financing risk in the UK is that awareness of PF risk in the designated non-financial businesses and professions (DNFBP), which includes the accountancy sector is, in general, low in most countries, and globally the PF focus continues to be on financial institutions. Given the important role UK's accountancy sector play in facilitating global finance, this could represent a particular risk to the UK, notably in relation to accountants providing trust and company services given the ease of establishing companies in the UK.

Protecting against the risk of professional enabling

When a criminal generates illicit proceeds, they sometimes need to access the skills and expertise of professional services to help them launder the funds. Criminals will frequently 'outsource' laundering to 'full time' third parties, who are rarely involved in the proceeds-generating illegal activities, but who provide expertise to disguise the nature, source, location, ownership, control, origin, movement and/or destination of funds to avoid detection.

A professional enabler is defined as "an individual or organisation that is providing professional services that enables criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations".

The accountancy sector is vulnerable to professional enabling when firms have weak compliance with the MLRs, as they are failing to meet their professional and regulatory obligations.

KEY RISKS AND RED FLAGS RELEVANT TO THE ACCOUNTANCY SECTOR

The risk of money laundering and terrorist financing is constantly evolving. Firms should regularly review the risk outlook, and any other risks published by their supervisory authority (such as AASG risk alerts) to make sure they have identified all the areas relevant to their own business – particularly as risks may evolve because of changes to the firm's client base, geography and services provided. The risks listed here are not exhaustive – you may identify other circumstances particular to your firm, where there might be a high risk of money laundering or terrorist financing.

This document is intended to help the firm understand its exposure to risk and ensure that it has designed and applied the right procedures to mitigate that exposure.

Clients

As part of the firm wide risk assessment, the firm should identify the type of clients that it serves. The firm must consider the risk posed by its clients by identifying whether they present any of the following risks and associated red-flag indicators. The presence of one or more red-flag indicators may suggest a high risk of money laundering or terrorist financing. Red flags are not exclusive to the risk areas identified below.

Firms should reinforce the importance of an 'inquiring mind' and employing professional scepticism – both in terms of the client due diligence performed and the scrutiny applied to the ongoing services provided.

Risk	Red-flag indicators	Why
Clients seeking anonymity or undue secrecy	• undue client secrecy (eg, reluctance to provide requested information) • unnecessarily complex ownership structures, including nominee shareholders or bearer shares • uncooperative clients • incorrect or misleading information on the register (Companies House) and/or reluctance to correct	Clients may try to hide who they are, or produce unusual forms of identity verification, if they are involved in criminal activity or money laundering. Clients who are seeking anonymity on behalf of themselves, a third party or beneficial owner may be seeking to launder money. Complex structures, or complex supply chains, are attractive to criminals as they may enable the integration of illicit funds into the legitimate economy.

	• clients using intermediaries to instruct the firm to perform services (eg, supply chain risk).	
Clients with a history of criminal activity	• clients with criminal convictions relating to the proceeds of crime • clients who are on the terrorist list • clients on the sanctions lists	Clients with a history of criminal activity would most likely pose a very high risk of money laundering to your firm. If you find out that a person or organisation you're dealing with is subject to financial sanctions, you must immediately: • stop dealing with them • freeze any assets you're holding for them • tell the Office of Financial Sanctions Implementation as soon as possible. The money laundering regulations require firms to put in place enhanced due diligence measures in dealing with countries subject to sanctions, embargos or similar measures. Clients may use accountancy firms to seek advice on restructuring their assets to avoid financial sanctions. **UK sanctions lists** 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. Sanctions regularly change so firms should use the most up-to-date list available online. **OFSI Consolidated of financial sanctions target** The Office of Financial Sanctions Implementation which is part of HM Treasury issues a list of all those subject to financial sanctions imposed by the UK – known as the consolidated list. Find the financial sanctions search here. Make sure you check the names of the beneficial owners, and not just the name of the client.

New clients outside of your normal client base	• new clients carrying out one-off transactions • new clients based in locations significantly different from your normal client base • new clients in sectors significantly different from your normal client base • clients introduced to you through intermediaries or third parties (eg, supply chain risk)	You should fully understand why an unusual client has approached you rather than using a firm of accountants that is closer geographically or a firm that advertises themselves as a specialist in a particular field. A client may be higher risk if there is no logical rationale.
New clients – professional advisors	• client has changed professional advisors several times in a short space of time without legitimate reasons • another professional advisor refused to provide the service to the client without legitimate reasons • the customer is prepared to pay substantially higher fees than usual without legitimate reasons • the client's previous professional advisor was not a comparably sized firm • the client engages with several professional advisors for different accountancy services	You should also be wary of why a client has changed professional advisors and seek to understand why this has happened. This may indicate a difference of opinion or a breakdown in the client-accountant relationship, which could be a red-flag indicator that the accountant had concerns about something that the client doesn't want to address. Clients concerned about the impact of sanctions or subject to sanctions may start to change their behaviours and consider changing their professional advisors. Larger professional advisors with sophisticated intelligence gathering systems may be concerned about existing clients and disengage. If a client has several different professional advisors providing different elements of accountancy and tax advice, you should consider whether this is because the client is trying to hide information from each advisor by providing each advisor with different information, or separate pieces of information.
Politically exposed persons	Regulation 35 of the amended MLR17 defines a PEP as an individual who is	MLR17 specify that PEPs, as well as certain family members and known close associates, are high risk and must undergo enhanced client due diligence. Those

	entrusted with prominent public functions, other than as a middle-ranking or more junior official.	who are entrusted with public functions often have power over public funds and the awarding of public contracts. The FCA has published guidance about the enhanced customer due diligence measures for PEPs. The starting point for the risk assessment of a UK PEP (or their family members and known close associates) is that they present a lower level of risk than a non-domestic PEP. The list of UK functions considered to be a PEP is included in Regulation 35 (14) of the amended 2017 Regulations.
Cash based businesses	• cash intensive businesses • money service businesses (MSB)	Cash is identified as one of the most common techniques of money laundering, and accountancy services are identified as being a sector with high exposure risk. We recommend all firms read the section on cash-based money laundering typologies in the NRA 2025. Certain businesses and sectors present higher risk of money laundering and terrorist financing. Cash intensive businesses are of particular risk as it is much harder to track the source of cash and its movements. It is much easier to integrate the cash proceeds of crime into legitimate income or payments. Cash made from criminal activity is reinvested within the UK to fund further both criminality and legitimate business ventures. Current examples of cash intensive businesses include barber shops, nail bars, beauty parlours, newsagents, restaurants, takeaways, car washes as well as high value dealers and cash-based gambling. Accountancy firms should also assess the risk of clients where cash may only form part of the business, or where specific types of transactions are performed via cash (eg, paying employees). You should consider whether any changes to the cash-nature of the business may result in higher risk – eg, during the COVID pandemic, businesses that were traditionally cash-based have generally moved to card payments. You should understand the reasons why a business is still transacting in cash if this is not the expected norm.

		The services offered by MSBs are attractive to criminals who want to transfer illicit cash. The NRA assesses MSBs as high risk. Criminals may use MSBs to transfer illicit cash to move money out of their hands into the financial system. The services provided by MSBs can also be attractive to those financing terrorism, who exploit the same vulnerabilities. HMRC has provided further guidance on risks within MSBs. Note that MSBs require supervision under the MLRs.
Clients that transact in cryptocurrencies or other cryptoassets	• transactions performed in crypto • client holds cryptoassets	Crypto is widely understood to be an emerging threat and pose significant ML risk. There is increasing evidence that criminals committing economic crime will use crypto as a way of transferring value and/or assets owing to the low skill required to initiate transactions, the anonymity that is provided by cryptocurrency and the increasingly complex technologies available to obscure beneficial ownership. The NRA 2025 provides further detail on how cryptoassets are used within money laundering. Privacy coins are cryptocurrencies with privacy-enhancing features designed to boost anonymity and reduce traceability. Transactions using privacy coins do not include details of the sender, receiver, or amount, and all their blockchain activity can be obfuscated, meaning payments cannot be publicly traced. Privacy coins are likely most frequently used as an intermediary currency in the laundering process, hindering law enforcement (LE) investigations by breaking the audit trail of the transactions.
Other sectors highlighted by the NRA and other sources	• arms dealers • property transactions with unclear source of funds • transport/logistics businesses • legal services • art market participants • financial services • luxury goods market	Sectors such as the arms trade are linked with corruption, money laundering or terrorism. Large property transactions, where the source of funds is unclear, have also been linked to laundering the proceeds of crime. HMRC's guidance on Understanding risks and taking action for estate agency and letting agency businesses provides further red flag indicators. Firms should also ensure that where overseas entities own UK property, the beneficial owner is properly recorded on the overseas entities register and assess the risk that a client may try to transfer ownership to avoid registering their beneficial ownership. Read more about the Register of Overseas Entities here.

	• Schools and universities • Football clubs and football agents	There has been a rise in cases reported in the press where transport and logistics businesses have been involved in modern slavery and human trafficking cases. These businesses also have the potential to be involved in in smuggling (eg, alcohol, fuel, tobacco). The NRA rates legal services, art market participants and financial services as being at higher risk of money laundering. You should employ professional scepticism when performing services or analysing the books and records of clients in these sectors. Luxury goods markets are a way to transfer value or assets from sanctioned individuals. NRA 2025 includes schools and universities and football clubs/football agents as cross-cutting risks in the UK. There is increasing evidence that schools and universities are at risk of accepting payments from criminals and kleptocrats. Football is susceptible to exploitation either through criminals assisting clubs that are in financial distress or through other crimes including illegal betting, match fixing, fraud and bribery.
Clients with a changing business, or involved in emerging sectors	• rapid rate of turnover (eg, trades for a short period of time, closes and then starts up as a new company) • client is taking on work which is outside its normal range of goods and services • clients that are involved in transactions that don't make commercial sense or involved in transactions where the source of funds is unusual or unknown • the client's lifestyle and/or transactions are inconsistent with	You should fully understand your client's business and ensure that the client can explain any changes in its business, and that you can verify that those changes are legitimate. You should take care to apply professional scepticism in such circumstances – challenging the client to provide evidence to support the change. A client may be higher risk if there is no logical rationale.

	known business and personal information • the client has multiple bank accounts or foreign accounts with no good reason • the client has raised funding through crowd funding • the client deals in, or with, crypto currency • the client's business has changed significantly during COVID eg, opening a new line of business such as selling products or services that may be linked to the pandemic	
High-net-worth individuals / wealthy individuals	• HMRC defines wealthy individuals as those earning more than £200,000 a year, or with assets over £2 million, in any of the last three years.	Not all high-net-worth individuals, or wealthy individuals, will be high risk simply because their income or assets meets the HMRC definition. However, risk will be elevated if they are a PEP or are high profile (eg, footballers or in entertainment), or if the type of services they are seeking suggests they are trying to evade paying tax, or hide the beneficial ownership of assets, or the individual is connected to / from high-risk jurisdictions. High-net-worth, or wealthy, individuals may look to use corporate structures or the services of professional advisors to structure their affairs to minimise their tax exposure. Risk will be greatest when the structures are complex and involve high secrecy jurisdictions. Family offices provide a range of services to ultra-high-net-worth individuals and their families and can coordinate the management of companies in charge of a portfolio of investments adding an extra layer of privacy to further distance the true owners. Overseas high-net-worth, or wealthy, individuals may be higher risk if they are investing in UK property.

Clients who work as contractors or agency workers paid by umbrella companies	• Unusual or complex payment arrangements such as pay appearing in bank account as two separate payments. • Client asked to sign an agreement with the umbrella company in addition to an employment contract. • Client is offered a choice between 'standard' and enhanced' arrangements with the 'enhanced' option entailing higher fees to the umbrella company. • Some or all payments a client receives are claimed to be non-taxable. • Umbrella company is based outside of the UK.	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. Umbrella companies might use disguised remuneration schemes to pay workers. They may claim that a payment is non-taxable to try to avoid paying employer National Insurance contributions (NICs). Payments to the client could be described as non-taxable loans, annuities, bonuses etc. On top of wages properly paid under PAYE (usually a national minimum wage amount), some umbrella companies may pay part of client's earnings (described as a loan or non-taxable payment) directly into the client's bank account. Other umbrella companies may route this payment through third parties or other complex arrangements.

Countries or geographies

The firm should consider whether its clients are established in countries that are known to be used by money launderers or terrorist financiers or proliferation financiers, or whether another of the parties to the transaction is established in such a country. When determining geographic risk, factors to consider may include the perceived level of corruption, criminal activity, and the effectiveness of MLTF controls within the country.

Risk	Why
Countries that do not have effective MLTF controls	MLR17 require firms to apply enhanced due diligence to clients that are established in high risk third countries – firms can find HM Treasury's guidance on High Risk Third Countries here. Firms should also consider those countries that have not implemented FATF recommendations, identified by credible sources such as FATF, the International Monetary Fund or World Bank. The Financial Action Taskforce (FATF) maintains the list of high-risk jurisdictions.

Countries with significant levels of corruption	MLR17 also identifies countries as high risk as those with significant levels of corruption or other criminal activity, such as terrorism. Transparency International produces the annual corruption index.
Countries with organisations subject to sanctions	MLR17 require firms to put in place enhanced due diligence measures in dealing with countries subject to sanctions, embargos or similar measures. **UK sanctions lists** 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. **OFSI Consolidated of financial sanctions target** The Office of Financial Sanctions Implementation which is part of HM Treasury issues a list of all those subject to financial sanctions imposed by the UK – known as the consolidated list. Make sure you check the names of the beneficial owners, and not just the name of the client.
Proliferation financing	You should consider whether the services you provide could be used in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, particularly to those countries subject to UN sanctions. Additionally, you should consider whether you have clients who make transactions to pay for goods and services that originate from a different jurisdiction to the one in which the goods and services are bound (ie, sanctions evasion).

Products or services

Criminals are attracted to the accountancy sector as a way of giving legitimacy to businesses that are a front for money laundering. Accountancy services may be used to create corporate structures or help to legitimise the movement of proceeds of funds.

The following products or services may be at high risk of being used for money laundering or terrorist financing.

Risk	Why
Trust and company services	The NRA identifies company formation and associated trust and company services as being among the highest risk services provided by the accountancy sector. The NRA also assesses there to be a high risk that UK partnerships and companies will be abused for money laundering. They can be used to enable the laundering of millions of pounds, conceal the ownership of

	criminal assets and facilitate the movement of money to secrecy jurisdictions. The risk is highest when coupled with other high-risk services or high-risk factors, such as a client in a high-risk country. The NRA 2025 sets out detailed information about this money laundering typology, alongside details on why the accountancy sector is at highest-risk. There is also a high risk when a new client approaches a firm for a one-off company formation, with no ongoing services required. The risk is also higher where a client seeking TCSP services is introduced by an intermediary or third party, particularly where those intermediaries / third parties are based in non-UK locations (eg, supply chain risk). Accountancy sector firms that offer registered office or nominee directorships are also at risk of exploitation as those services can enable the concealment of beneficial ownership. Law enforcement has indicated that many investigations into money laundering lead to complex corporate structures. By creating structures that disguise the ownership of assets, the accountant may be either wittingly or unwittingly involved in 'integration' of the illicit funds into the legitimate economy. HMRC has published guidance on Understanding risks and taking action for trust and company service providers.
Legitimising books and records	Criminals will falsify underlying books and records to hide criminal activity and engage a professional accountant to prepare the financial statements to legitimise them and benefit from the veneer of respectability provided by the professional adviser. There is also a risk associated with 'incomplete records' engagements where the accountancy firm, or bookkeeper, is asked to use bank statements to prepare the accounts and not the underlying books and records. This is another way in which the criminal can mask the true nature of the transactions. Accountants and bookkeepers should use their professional scepticism when reviewing books and records to ensure the pattern of transactions fits with what they know about the client's business. Accountants may also be relied upon to produce or verify documents that relate to a client's financial position for use in mortgage or visa applications[1]. They should take care to ensure they have sufficient information and understanding of the client's financial affairs before undertaking this task.
Payroll services	Payroll services may include the handling of clients' funds and so the accountant may provide services that legitimise the proceeds of a crime eg, modern slavery, ghost employees or individuals recorded as an employee who aren't performing

[1] The NRA 2025 refers to such engagements as accountants' certificates of confirmation.

	tasks. The accountant may also legitimise the incorrect calculation of deductions (tax evasion) by processing payments – and so they need to be careful about the accuracy and fairness of the calculations. The NCA has published indicators of modern slavery and human trafficking in the accountancy sector. This provides red flag indicators to be aware of during payroll engagements. The risk is highest where staff have not received AML training tailored to payroll services, staff are not client-facing or there is poor quality information provided by the client. Payroll services, and ghost employees, may be employed by sanctioned individuals to extract value from the businesses they control.
Insolvency services	Criminals may mask the audit trail of money laundered through a company that has gone into liquidation. By providing insolvency services that mask the funds and distance them from their source, the accountant may be involved in 'layering' of the illicit funds into the legitimate economy. In particular, member voluntary liquidations (MVL) may be used by criminals as a tool to liquidate the assets of a business, owing to the IP not having any obligation to investigate the company's affairs.
Tax advice that leads to a reduction in tax liability.	There will be many circumstances where providing tax advice to reduce a tax liability is legal. However, there is a risk that an accountant or tax adviser may provide tax advice that assists the client in masking their true income, or structuring their income and wealth to gain an illegal tax advantage.
Tax investigations where there might be a criminal element	Clients may ask firms to get involved in assisting with a tax investigation. Firms should consider whether the investigation results from underlying tax evasion, or whether the source of funds relate to criminal proceeds.
Investment business	Regulated investment business includes a limited number of areas where an accountant may provide services that could legitimise the proceeds of a crime. Some professional accountancy bodies can licence firms to conduct 'non-mainstream' investment business (DPB licence) eg, advise on private company shares. Such advice may result in the accountant being involved in the integration of the illicit funds into the legitimate economy.
Probate and estate management	The provision of probate services is not in itself a high-risk activity for accountants but the agreement of the probate papers or letters of administration may legitimise the distribution of assets, which could be proceeds of crime.

	Accountants are often involved in the administration of estates, regardless of whether they have a probate accreditation from a professional body or not. Estate administration can involve the collection of any form of asset, cash, investments, properties and the distribution of those assets to the beneficiaries.
Central and local government support schemes	There are reports in the press, and information published by HMRC, that suggests that government support schemes are at risk of fraud. You should be alert for any red flags that suggests that your client is not entitled to claim any government support. If you are making applications on behalf of a client, the firm should ensure that they have sufficient information to confirm that the application is valid.
Identity verification (IDV) for Companies House	The Economic Crime (Transparency and Enforcement) Act 2022 created the **Register of Overseas Entities** (ROE), which requires overseas entities owning UK property to reveal their beneficial owners and to register their interest on a publicly available register. The information must be verified by an approved agent. 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 will have to register as an **Authorised Corporate Service Provider**. This work is high-risk because: • there is a risk that those who don't want to reveal their identities may take steps to obscure it; • the companies on the Register of Overseas Entities and/or the property are likely to have high-risk red flags owing to the overseas ownership; and • 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 Register of Overseas Entities and for the IDV standard for ACSPs is not the same as the risk-based approach to client due diligence under MLR17.
Services subject to trade sanctions	Any UK persons anywhere and other persons in the UK are prohibited from providing the following services to a person connected with Russia: • accounting services • business and management consultancy services • auditing services. Further information can be found here.

Transactions

Most accountancy services do not involve the facilitation of transactions. However, the following area may be at high risk of being used for money laundering or terrorist financing.

Risk	Why
Clients' money bank accounts	There is a risk posed by accountants performing high value financial transactions for clients with no clear business rationale, allowing criminals to transfer funds through the client's money account. Accountants should not allow their client account to be used as a banking facility and should understand the rationale for why the client is using the firm's clients' money bank account before the transaction is initiated.

Delivery channels

The way in which the firm provides its services to its client will affect the risk to the firm.

Risk	Why
Clients that you haven't met	If the firm hasn't met its client face-to-face, it has increased the risk that the client is not who they say they are. The client may wish to hide their identity, or favour anonymity, if they are involved in criminal activity. The coronavirus pandemic has meant that not meeting clients may be the norm. Firms should consider how this change impacts the risk within their take-on procedures and how they can mitigate those risks. Although rare, there may be occasions where a client has been referred (eg via fiduciaries, solicitors etc) and, additionally, from those operating in high-secrecy jurisdictions (eg Switzerland, Lichtenstein, Luxembourg etc). Some of these referrers can be uncooperative in providing identity or due diligence information sufficient for a UK firm to fulfil its responsibilities. The COVID pandemic has also led to an increase in the delivery of services via remote methods (cloud accounting platforms). Firms should consider whether this new delivery mechanism or the use of a new technology to the firm has resulted in higher risk to their practice (Regulation 33 6 (b)).
Insider threat in relation to tax	Insider risk refers to those members of staff within organisations who may be providing or who can provide a function that enables tax evasion. This may be complicit or non-complicit.

	Complicit activity would involve instances where staff purposefully know and assist tax evasion, or obfuscate detection of client tax evasion; either by circumventing controls, taking inappropriate advantage of a lack of controls, or by deliberately failing to implement controls. Firms should assess their staff and consider whether they are appropriately trained in the firm's policies and procedures, which should be designed to provide controls to mitigate the risk of staff being complicit in tax evasion.
Combining services	Some services might not be inherently high risk, but when combined with other services or transactions become risky. For example, there might be legitimate reasons for setting up a company, but if that company is used to purchase property and disguise its beneficial owner, this increases the risk of money laundering. Services supporting complex trust or company structures involving high risk jurisdictions or tax havens, offering off-the-peg companies or shell companies, non-face to face business models, staff and customers based abroad with due diligence undertaken in high-risk jurisdictions are regarded as heightening a firm's vulnerability to MLTF risks.
Combining factors	Risk will increase where multiple risks are present in one client or engagement eg, overseas high net worth individuals may be higher risk if they are investing in UK property.
Supply chain risk	A complex supply chain spanning multiple professional services across multiple jurisdictions might result in the identity of the ultimate beneficial owner being obscured, or the purpose of the entity involved in the transaction (or the purpose of the transaction itself) being obscured from the service provider.