IPA Sector Risk Assessment under Regulation 17[1] – Insolvency Practice

September 2025

1. Introduction

The impact of money laundering can threaten the UK's prosperity, national security and financial systems, and it enables serious organised crime including tax evasion, modern slavery, drugs trafficking, fraud, corruption and terrorism.

The 2025 National Risk Assessment[2] (NRA) is the fourth comprehensive assessment of money laundering and terrorist financing risk in the UK. Published in July 2025 and spanning 163 pages, it provides an in-depth review of all high-risk sectors. It underlines the complexity of the money laundering landscape and the level of risk facing the profession. This IPA risk assessment summarises the key risks relevant to the profession; it remains the responsibility of Insolvency Practitioners (IPs) to assess the specific risks in the sectors in which their appointments operate to fully consider evolving threats and to remain up to date.

Regulation 18 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17) requires IPs to take appropriate steps to identify and assess the risks of money laundering (ML) and terrorist financing (TF) to which their business is subject. The risks of proliferation financing also need to be evidenced under Regulation 18A.

Risk assessments must take account of:

- Information made available by the IPA, including this sectoral risk assessment under regulation 17(1);
- Risk factors relating to clients, services, transactions, delivery channels, and geographic areas.

An IP must provide their risk assessment to the IPA on request, and this forms part of the wider requirements to establish and maintain policies, controls and procedures to mitigate and manage the identified risks effectively.

---

2. AML Risk in Context

Regulation 16 of MLR17 requires the UK Government to maintain a National Risk Assessment (NRA) to *identify, assess, understand and mitigate* ML/TF risks affecting the UK.

The public is ultimately most vulnerable to the risks of ML/TF. For IPs, this means both:

- The risk of being exploited for ML/TF purposes; and

---

[1] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

[2] Policy paper - National risk assessment of money laundering and terrorist financing 2025 – published 17 July 2025

- The risk of failing to identify or reasonably suspect ML/TF where it has occurred.

IPs can mitigate these risks by demonstrating that they have understood and identified the specific risk areas through their firm-wide risk assessment, and by maintaining effective policies and procedures designed to reduce risks and identify and report suspicions. This includes ensuring that training is effective and that all staff understand both the risks and the firm's procedures for managing them.

---

3. Accountancy and Insolvency Sector Risk

The NRA 2025 includes Insolvency as part of the 'Accountancy services' which can be used for money laundering purposes. The accountancy sector remains attractive to criminals seeking legitimacy for illicit funds. The services considered most at risk remain:

- Company formation and termination;
- Mainstream accounting;
- Payroll.

Although insolvency practice is not the highest-risk service, it carries unique vulnerabilities because of the statutory powers and control IPs exercise over companies and their assets.

The IPA is a member of the Accountancy AML Supervisors Group (AASG), which works with HM Government and law enforcement to make it more difficult for criminals to exploit accountancy services. The AASG's Risk Outlook (updated 22 September 2025) highlights the key risks, red-flag indicators and circumstances where there may be high risk of money laundering, terrorist financing or proliferation financing in the accountancy sector.

This document is updated regularly to reflect the latest UK NRA and other emerging threats and trends. It is intended to help auditors, insolvency practitioners, accountants, tax advisers and trust or company service providers to assess AML risk with reference to the services they provide and the types of clients they serve.

A firm's written risk assessment should identify the areas of the business most at risk and focus resources on these areas. Senior management must approve, document and implement policies, controls and procedures to address and mitigate these risks, and ensure staff are trained to recognise and respond to them effectively.

---

4. Insolvency-Specific Risks

The NRA 2020[3] noted that *"Company liquidation and insolvency services continue to present a potential vector for abuse, particularly where used to obscure audit trails, conceal the proceeds of crime, or disengage from liabilities."* While insolvency licensing requirements and regulatory oversight are important mitigants, IPs need to consider the continual evolution of the level of risk and how this varies by insolvency case type and sector. The methods used to avoid detection evolve too, with phoenixing defined in the NRA 2025 as a specific insolvency risk.

[3] Policy paper -National risk assessment of money laundering and terrorist financing 2020 – published 17 December 2020

4.1 Abuse of Corporate Structures
Intelligence suggests that there is widespread abuse of otherwise lawful corporate structures and legal arrangements (e.g. trusts) for ML purposes. Corporate structures are used to conceal the origin and destination of funds and to falsely legitimise money movements as normal business transactions. The separation of personal identity from the alleged business activity adds complexity for investigators and prosecutors.

Criminals may create and run corporate vehicles themselves or involve third-party nominees and professional service firms. The Economic Crime and Corporate Transparency Act 2023 introduces reforms aimed at making such abuse more difficult and reducing vulnerabilities, but effective due diligence by IPs remains crucial to minimise risks.

4.1.1 Predicate Offences
The most common predicate offences associated with abuse of corporate structures include:

- Fraud
- Sanctions evasion
- Tax evasion
- Drugs offences
- Corruption

4.3 Phoenixing and Nominee Directors
To avoid detection, criminals may engage in *phoenixing* – carrying on the same business through successive companies, each becoming insolvent in turn. The business (but not the debts) is transferred to a new company.
Indicators include:

- Use of nominee directors unconnected to the previous company;
- Purchase of "off the shelf" companies with existing trading history or licences.

4.4 Shelf Companies
A UK "shelf" company is incorporated but inactive, often marketed as reputable and established. Some have shareholders and directors already in place. While legal, such companies can provide an appearance of legitimacy for illicit activity, especially when linked to cash-intensive operations.

4.5 Cash-Intensive Businesses
Corporate structures, including those in insolvency, can act as a cover for paying large sums of criminal cash into bank accounts. This is frequently linked to businesses with high volumes of cash transactions, which can be used to layer illicit funds into the financial system.

4.6 Insolvency Appointment Risks – Summary by Case Type

Corporate Insolvency (Liquidations, Administrations, CVAs)

Key Risks

- Abuse of Corporate Structures – Criminals continue to exploit UK and overseas corporate vehicles (including shell companies, trusts, and Scottish Limited Partnerships) to conceal beneficial ownership and move illicit funds.

- Phoenixing – Repeated insolvencies where the business (but not the debt) is transferred to a new company, often with a different director or by using an "off-the-shelf" company to disguise continuity.
- Shelf Companies – Inactive companies sold with existing incorporation details and sometimes licences, marketed as established businesses to give false legitimacy.
- Predicate Offences – Common underlying crimes include fraud, sanctions evasion, tax evasion, drug trafficking, and corruption.
- Proceeds of Crime Purchases – Insolvent businesses purchased using illicit funds, reintroducing them into the legitimate economy.
- Cash-Intensive Businesses – Corporate entities used as a front for depositing large sums of criminal cash.

Implications for IPs

- Maintain robust CDD on directors, shareholders and connected parties.
- MVLs in particular remain the highest risk in terms of evidencing assessment and verification of the source of wealth.
- Apply scepticism where there are links to high-risk jurisdictions, rapid director changes, or unusual business acquisitions.
- Monitor Dear IP updates (e.g. Dear IP 117 – fraudulent redundancy claims).

COVID-19 Support Scheme-Related Appointments

Key Risks

- Bounce Back Loan Scheme Fraud – Significant losses, estimated at 35–60% of loans, with insolvent companies misusing funds.
- Furlough Scheme Abuse – Claims for non-existent employees or inflated wages.
- Other Grant Misuse – Diversion of support funds for personal gain or unrelated purposes.

Implications for IPs

- Investigate and document suspected fraud in directors' conduct reports.
- Submit SARs as soon as criminal property is suspected.
- Report under s.218 of the Insolvency Act as required.

Personal Insolvency (Bankruptcy, IVAs, PTDs)

Key Risks

- Money Mule Activity – Insolvent individuals recruited to move funds, purchase goods for export, or unwittingly allow account use.

- Exploitation of Vulnerability – Financial stress and coercion may make individuals more susceptible to criminal approaches.

Implications for IPs

- Train staff to identify red flags (e.g. unexplained transactions, links to known mule activity).
- Apply enhanced due diligence in high-risk personal insolvency cases.

Jurisdictional Risks

Key Risks

- Scotland and Northern Ireland have different insolvency laws, and this may be a risk to be assessed.
- Scottish Limited Partnerships (SLPs) – Historically linked to large-scale money laundering (e.g. $80bn moved from Russia in four years).
- Cross-Border Appointments – Higher complexity in verifying beneficial ownership where multiple jurisdictions are involved.

Implications for IPs

- Verify corporate ownership structures rigorously.
- Familiarise with jurisdiction-specific AML legislation and vulnerabilities.

---

5. Summary

Insolvency procedures remain a potential channel for money laundering and other economic crimes. While good regulatory oversight and licensing reduce vulnerabilities, the misuse of corporate structures, phoenixing, nominee directors, shelf companies and cash-intensive businesses continues to present significant risks.

IPs must remain vigilant from the outset of an appointment and throughout the life of the case, by recognising that risks can change as new information emerges or circumstances develop. IPs need to apply robust due diligence, scrutinising corporate histories, and challenging suspicious instructions or restructuring proposals.

Compliance with the CCAB AML Guidance for the Accountancy Sector[4] and Insolvency Appendix[5], the Insolvency Code of Ethics, and SIP 1 is essential to prevent and detect abuse. IPs must retain evidence of risk checks undertaken and decisions made by keeping clear file notes as part of due diligence.

As money laundering techniques and risks continue to evolve, IPs must ensure that training, policies, and procedures are regularly updated to reflect emerging threats. This includes the ability to spot

---

[4] CCAB Anti-Money Laundering and Counter-Terrorist Financing Guidance for the Accountancy Sector 2023 – published 17 May 2022

[5] CCAB Appendix F: Supplementary Anti Money Laundering Guidance for Insolvency Practitioners - published May 2022

imbalances in accounting records, gaps in factual information, and red flags from open-source checks, all of which should lead to timely and effective AML actions.

Version updated: September 2025