HM Treasury

National Risk Assessment of Proliferation Financing

November 2026

HM Treasury

National Risk Assessment of Proliferation Financing

November 2026



© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at: www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gov.uk

ISBN: 978-1-80994-004-9

PU: 3692

Contents

Foreword *7*

Chapter 1 ..... **9**

Aims & Methodology 9
Introduction 9
Aims of this Assessment 12
Scope of the Assessment 13
Methodology 13

Chapter 2 ..... **15**

The UK's Strategic, Regulatory, and Operational Framework: Updates to Counter Proliferation Financing *15*
The UK's approach to counter-proliferation financing 15
Domestic PF Developments since the 2021 NRA 17
International updates 26

Chapter 3 ..... **28**

Proliferation Financing Threats Facing the UK *28*
The role of state and non-state actors 28
Abuse of corporate structures 32
Export and shipping typologies 38
Typologies linked to remote IT workers in specific jurisdictions 39
Cryptoassets 40
Illicit use of artificial intelligence 43

Chapter 4 ..... **45**

UK Sectoral Vulnerabilities *45*
The UK's financial and non-financial sectors 46
Cryptoasset firms 52
UK firms employing remote IT workers 53
The maritime and shipping industries 54
Manufacturing of proliferation or dual-use goods 55
The higher education sector 55
Business-wide risk assessments 57

Chapter 5 ..... **58**

Conclusions *58*

Glossary *60*

Foreword



The proliferation of chemical, biological and nuclear weapons poses a serious and evolving threat to the United Kingdom's national security, and to the wider international community. The ability of hostile states and networks to finance and procure materials, technology and expertise remains central to the development of illicit programmes. Countering proliferation financing is therefore a critical part of the UK's broader efforts to protect our security and prevent the spread of weapons of mass destruction.

This National Risk Assessment sets out the UK's updated understanding of the threats, vulnerabilities and mitigations relating to proliferation financing. It builds on the UK's first assessment, published in 2021, and reflects developments in the threat landscape since then. The period has seen deepening political, military and economic cooperation between Russia, Iran and the Democratic People's Republic of Korea (DPRK), alongside the re-imposition of nuclear-related sanctions on Iran and the increasing use of cryptoassets and other technologies to facilitate sanctions evasion. Proliferators are becoming more sophisticated, using global networks, intermediaries, corporate structures and new technologies to move funds and avoid detection.

The UK continues to maintain a strong and comprehensive framework to counter proliferation financing. This includes robust financial sanctions, export controls, and an increasingly integrated approach within our Anti-Money Laundering and Counter-Terrorist Financing regime. Since 2021, we have strengthened this framework further through reforms to corporate transparency, enhancements to sanctions enforcement, and clearer expectations on regulated firms to identify and manage proliferation financing risk within their business activities.

The UK's openness as a global financial centre and trading hub inherently exposes us to risk. Proliferation financing activity is often indirect and embedded within otherwise legitimate transactions, making it difficult to detect and disrupt. This Assessment highlights where vulnerabilities exist, including in the use of complex supply chains, intermediary jurisdictions, and evolving financial technologies. The conflict in Ukraine has highlighted how state actors use complex procurement, shipping and financial networks, often supported by

sanctions evasion and intermediary arrangements, to sustain military capabilities. Many of these typologies are also relevant to proliferation financing risk.

This document is intended to support both public and private sector stakeholders. Regulated firms play a vital role as the first line of defence and are required to take a risk-based approach to identifying and mitigating proliferation financing risks. This assessment should therefore be used alongside published anti-money laundering, counter-terrorist financing and counter-proliferation financing guidance to inform high-quality risk assessments.

The UK remains committed to working closely with international partners to strengthen our collective response. As proliferation financing becomes increasingly intertwined with sanctions evasion, cyber-enabled crime, cryptoasset misuse and other forms of illicit finance, improving our shared understanding of risk has never been more important. By enhancing compliance, maintaining a strong enforcement framework, and maintaining vigilance against evolving threats, we will continue to detect, deter and disrupt proliferation financing activity.

Foreword by Lucy Rigby KC MP

Economic Secretary to the Treasury

Chapter 1
Aims & Methodology

Introduction

1.1 The proliferation of chemical, biological and nuclear weapons, as well as conventional, dual-use and non-controlled sanctioned technology that can be used in their development and delivery, poses a profound threat to international peace and security, and to the UK's national security.

1.2 This National Risk Assessment (NRA) of Proliferation Financing (PF) provides an updated, UK-wide assessment of the threats, vulnerabilities and mitigations relating to PF. Its first purpose is to support regulated firms subject to the Money Laundering Regulations (MLRs) in meeting their statutory obligations to identify, assess and mitigate PF risk. It is intended to act as a practical, authoritative resource for firms, helping them understand how PF risk arises in practice and how it may affect their business. By setting out key typologies, risk indicators and areas of exposure, the Assessment is intended to strengthen regulated firms' business-wide risk assessments and underpin effective, risk-based controls.

1.3 The UK last published a PF NRA in 2021.[1] Since then, both the threat landscape and the UK's response have evolved significantly. Proliferators, including state actors, networks and facilitators, have become increasingly adapted their approach, and PF typologies have become more complex and intertwined. PF risks are not limited to sanctions and sanctions evasion; it can often overlap with other forms of illicit finance with the same organised crime groups and professional enablers acting across different areas.[2]

1.4 In response, the UK has strengthened its counter-proliferation financing framework, including through enhanced regulatory requirements, expanded sanctions enforcement capabilities and reforms to corporate transparency.

What is proliferation financing?

1.5 Proliferation financing refers to the financial enablement of proliferation activity. In 2010, the Financial Action Task Force (FATF), as

---

[1] HM Treasury, National Risk Assessment of Proliferation Financing, 23 September 2021, https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing.

[2] Reference to designated persons in this document also includes reference to persons owned or controlled by designated persons, as stated in reg. 7 of the Russia (Sanctions) (EU Exit) Regulations 2019 and equivalent measures, https://www.legislation.gov.uk/uksi/2019/855.

the global standard setter for Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) stated a definition of PF activity as:

> *"the act of providing funds or financial services which are used, in whole or in part, for 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), in contravention of national laws or, where applicable, international obligations."*[3]

1.6 Consistent with the UK's 2021 PF NRA, and in the spirit of the FATF guidance, this Assessment adopts this definition of PF, with the scope covering activities which directly or indirectly finance an actor's procurement of nuclear, chemical and biological weapons.

1.7 Regulated firms should be aware that they are required to adhere to the definition of PF in the MLRs, which gives effect to FATF countermeasures in UK law, and refers only to PF "in contravention of a relevant sanctions obligation".[4] In this context, relevant sanctions obligations are those which are imposed by the UK to implement UN CPF sanctions (further detail below). The UK also imposes non-UN counter-PF sanctions through individual sanctions regimes. This Assessment as a whole takes the FATF definition as its basis, as this allows for a broader overview of the PF risks.

1.8 In 2020, the FATF imposed requirements on jurisdictions and the private sector to identify, assess, and mitigate the risks of breaches, non-implementation or evasion of targeted financial sanctions relating to PF.[5] In June 2021, FATF published updated guidance on PF assessment and mitigation.[6] The national-level PF risk assessments resulting from these additional requirements have become a critical tool for improving shared understanding and focusing mitigation where it is most needed.

1.9 The FATF working group also proposed a broader definition of "the financing of proliferation", which includes "raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery

---

[3] Financial Action Task Force, 'Combating Proliferation Financing', February 2010, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf.coredownload.inline.pdf, p.5.

[4] Reg. 16A, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, https://www.legislation.gov.uk/uksi/2017/692.

[5] Financial Action Task Force, 'Public Statement on Counter Proliferation Financing', 23 October 2020, https://www.fatf-gafi.org/en/publications/Financingofproliferation/Statement-proliferation-financing-2020.html.

[6] Financial Action Task Force, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf

or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)." However, the UK notes that this definition was not intended to replace the 2010 definition, but to make "a positive contribution to the understanding of" the risks outlined in the FATF standards.[7] For the purposes of this NRA, the UK will draw on both definitions. The 2010 FATF definition remains the basis for the assessment of PF risk against the FATF standards, while the broader 2021 definition is used to support a fuller understanding of PF risk, including activities, actors and financial flows that may contribute towards financing proliferation.

1.10 PF risk differs from, but overlaps with, money laundering and terrorist financing: PF must involve the development of nuclear, chemical or biological weapons by the end user, but the typologies used to indirectly secure funding are often consistent with other forms of illicit finance. PF often involves transactions that appear consistent with legitimate commercial activity, such as payments for industrial goods, shipping or professional services.

1.11 The UK's 2021 NRA highlighted that PF can be both direct and indirect: direct activity relates to the procurement of proliferation-sensitive or dual-use goods, while indirect activity can involve multiple layers of financial or commercial intermediaries that support procurement networks or obscure the true end user.[8] This makes PF particularly challenging to identify and requires a risk-based approach which considers typologies and systemic vulnerabilities.

1.12 For most UK firms, PF exposure is more likely to arise indirectly through customers, suppliers, intermediaries, counterparties, service providers or supply chains than through direct dealings with proliferating states or designated persons.

UN obligations

1.13 The international community has long recognised the importance of countering PF. At the time of publication, the most significant PF-relevant UN Security Council Resolutions (UNSCRs) relate to the Democratic People's Republic of Korea (DPRK) (UNSCR 1718 and its successor resolutions) and Iran (UNSCR 1737 and its successor resolutions), which remain the primary focus of international counter-proliferation financing efforts.[9] These regimes seek to constrain nuclear proliferation activities through financial restrictions, asset freezes and controls on sensitive trade. The frameworks are intended not only to prevent direct financing of proliferation programmes, but also to disrupt indirect support through trade and financial sector intermediaries.

---

[7] FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021 p.8.

[8] HMT, 'National Risk Assessment of Proliferation Financing', September 2021.

[9] UN Security Council Resolution 1718 (2006), https://docs.un.org/en/S/RES/1718%20(2006); UN Security Counsil Resolution 1737 (2006), https://docs.un.org/en/S/RES/1737%20(2006).

1.14 The UK implements its obligations under these UNSCRs through domestic legislation.

The 2021 Assessment

1.15 The UK's first PF NRA, published in 2021, established a baseline understanding of proliferation financing risk and helped embed it within the UK's wider approach to tackling illicit finance.

1.16 It concluded that whilst the UK maintains a strong regulatory framework, its financial and professional services sectors are inherently exposed to exploitation by proliferators. It identified banking and insurance as particularly exposed sectors, and highlighted the DPRK and Iran as the most significant state-level PF actors.

1.17 The Assessment also identified more limited awareness of PF risk in parts of the private sector compared to money laundering and terrorist financing, which could reduce the ability of regulated firms to identify and mitigate risk.

Aims of this Assessment

1.18 Under the MLRs, the Treasury has a statutory duty to both assess PF risk in relation to relevant financial sanctions obligations and to keep this Risk Assessment under review. This Assessment is made further to those statutory requirements.[10]

1.19 Assessments are produced in order to assist regulated firms which are required by the MLRs to take appropriate steps to identify and assess the risks of PF to which their businesses are subject.[11]

1.20 The 2026 PF NRA builds on the 2021 Assessment and has four core aims:

1.21 First, it provides **an updated overview of the UK's CPF framework**, including where the UK has strengthened its counter-PF system in response to the risks set out in the previous NRA. Since 2021, there have been developments in the implementation of PF requirements, including clearer expectations on regulated firms to identify, assess and mitigate PF risk as part of their obligations under the MLRs. This Assessment updates the picture of the UK's legal, regulatory and operational framework, including the roles of government, supervisors, law enforcement and the private sector.

1.22 Second, this Assessment focuses on **the PF typologies which constitute the most acute threat to the UK**. This includes examining how proliferators seek to raise, move and use funds, and how procurement networks operate. In line with the 2021 Assessment, the Assessment recognises that financing often involves multiple stages,

[10] Reg. 16A, Money Laundering Regulations.

[11] Ibid., reg. 18A.

and intermediaries, between the financial transaction and the ultimate end use/beneficiary.

1.23 Third, this Assessment identifies **areas of vulnerability within the UK system**. While the UK continues to have a strong framework for countering PF, vulnerabilities can arise from a range of factors, including uneven awareness and understanding of PF risk, the complexity of global trade and financial flows, and the use of increasingly sophisticated methods by proliferators to evade controls. This Assessment seeks to highlight where these vulnerabilities exist and where further strengthening of mitigations may be required.

1.24 Fourth, the PF NRA **supports a cross-government and cross-system understanding of PF risks and prioritisation**. By providing a shared assessment of key threats, vulnerabilities and mitigations, it helps inform policy development, operational activity and the prioritisation of resources across government, helping to ensure that efforts to counter proliferation financing are targeted towards the areas of greatest risk.

Scope of the Assessment

1.25 Consistent with the approach taken in 2021, this Assessment adopts a broad and practical interpretation of PF risk, consistent with the FATF definition (at 1.5 above). It recognises that an exclusive focus on actual sanctions breaches may not capture the full range of activity that contributes to proliferation. As such, the scope includes activity which supports or facilitates proliferation even where the link to nuclear, biological or chemical procurement may be more indirect.

1.26 This includes consideration of the role of enabling jurisdictions which may be used to obscure the origin, destination or purpose of funds and goods. The Assessment considers the wider networks and jurisdictions, involving a UK nexus, which may facilitate or enable proliferation activity.

1.27 The Assessment focuses on activity that has a connection to the UK (for example, the UK financial system or the economy) and/or has UK national security impacts. This includes the use of UK financial and professional services, UK-based entities, or transactions that pass through the UK or involve UK-linked actors. The objective is to identify those risks most relevant to the UK, to inform the domestic response.

Methodology

1.28 The methodology used for the 2026 PF NRA is aligned with that adopted in the 2021 Assessment, with refinements to reflect developments in approach.

1.29 While the FATF conceptual framework defines risk as a function of threats, vulnerabilities and consequences, this Assessment adopts a primarily operational focus on threats, vulnerabilities and mitigations. This reflects the approach taken in the previous PF risk assessment,

recognising that the consequences of PF are well understood, and that greater value is derived from identifying how activity occurs and where controls may be strengthened.

- **Threats** refers to the intent and capability of proliferators and associated networks, and the activities they undertake to finance and procure chemical, biological and nuclear goods and technology. This includes the typologies involved in raising, moving and using funds and services.
- **Vulnerabilities** refers to the features of the UK system that may be exploited by threat actors. These can include gaps in awareness or understanding, weaknesses in controls or their implementation, structural features of financial and trade systems, or the inherent openness of the UK economy and markets.
- **Mitigations** refers to the measures in place to reduce PF risk, including the legal and regulatory framework, supervisory activity, law enforcement capability, and the policies, controls and procedures carried out by the private sector.

1.30 While this Assessment focuses on threats, vulnerabilities and mitigations, it is also important to recognise the consequences of PF. PF activity enables the development of nuclear, chemical and biological weapons, undermining international security and the rules-based international system. PF also damages the integrity of the UK's financial system by facilitating sanctions evasion and exposing firms to legal, regulatory and reputational risk. This Assessment emphasises mitigations, supporting firms to implement effective, risk-based controls to reduce the risk of PF activity.

1.31 This Assessment draws on a wide range of evidence, including contributions from government departments, law enforcement, supervisors and private sector stakeholders. As in the 2021 NRA, this collaborative approach is essential to developing a comprehensive understanding of PF risk, given that relevant intelligence and insight is distributed across multiple sectors, organisations and government departments.

1.32 Please note that throughout this Assessment, the term "regulated firms" refers to persons subject to the Money Laundering Regulations. The term "firms" is used more broadly to refer to private-sector businesses and service providers, irrespective of whether they are subject to the MLRs. Where risks, vulnerabilities or mitigations apply more widely, including to public bodies, universities, or other organisations, the Assessment uses appropriate terms.

Chapter 2

The UK's Strategic, Regulatory, and Operational Framework: Updates to Counter Proliferation Financing

The UK's approach to counter-proliferation financing

2.1 The UK's understanding of proliferation and PF risks directly informs strategic priorities, shaping sanctions policy and broader counter-proliferation measures.

2.2 The UK National Security Strategy 2025 (NSS)[12] highlights the growing threat from nuclear weapons and the wider proliferation of disruptive technologies, noting that more states possess such capabilities and that international arms control frameworks are under increasing strain. The NSS sets the strategic direction for strengthening national resilience to hostile state activity and reinforces the role of sanctions and export controls in preventing actors from acquiring resources that could support weapons of mass destruction-related programmes.

2.3 Building on this threat picture, the UK maintains a cross-government approach to sanctions policy strategy and development. Led by the FCDO, competent authorities work together to ensure that sanctions measures are targeted towards the highest proliferation threats facing the UK. This includes through the use of autonomous sanctions powers, where appropriate, to address PF risks beyond those covered by UN measures. This is set out further from paragraph 2.10.

2.4 In addition, the UK's Counter Proliferation and Arms Control Centre (CPACC) is the UK's dedicated cross-government department responsible for coordinating policy making on international counter

[12] Cabinet Office, 'National Security Strategy 2025: Security for the British People in a Dangerous World', 24 June 2025, https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world.

proliferation and arms control issues. It brings together expertise from the Foreign, Commonwealth and Development Office (FCDO), Ministry of Defence (MOD), and the Department for Energy Security and Net Zero (DESNZ).

2.5 CPACC coordinates counter proliferation and arms control activity, including CPF, ensuring that proliferation risks are addressed coherently.

2.6 The UK has been a strong advocate for improving global understanding of PF risks and has encouraged partner countries to undertake their own PF national risk assessments, sharing lessons from the UK's 2021 PF NRA. The UK has promoted greater international action on PF in multilateral fora, including at the United Nations and in the G7 Global Partnership against the Spread of Weapons and Materials of Mass Destruction. UK advocacy has supported wider adoption of PF risk assessment approaches and more consistent implementation of FATF standards.

2.7 The UK has also funded dedicated capacity building in Southeast Asia through its partnership with the United National Interregional Crime and Justice Research Institute (UNICRI), reflecting the region's exposure to DPRK-linked proliferation financing networks and the associated risks to the UK. This regional programme has helped Cambodia, Laos and the Philippines strengthen understanding of PF typologies and compliance with international standards. Workshops under this initiative have helped authorities identify vulnerabilities linked to intermediaries, front companies and regional financial flows, which may be exploited to facilitate DPRK-related sanctions evasion and procurement activity.

Defence Review 2025

2.8 The UK Strategic Defence Review 2025[13] underscored the growing risks posed by state-led proliferation activity, highlighting renewed nuclear risks and the increasing willingness of adversaries to pursue strategic objectives through coordinated military, technological and economic means. The Review identified states including Iran and DPRK as part of a challenging global security environment in which nuclear and missile-related threats are becoming more prominent.

2.9 The Review emphasised that adversaries are increasingly operating through complex international networks, relying on illicit procurement, technology transfer and economic activity beyond the traditional battlefield. This strategic Assessment reinforces the relevance of counter-PF measures as part of the UK's national defence and deterrence posture, recognising that the ability of states such as

[13] Ministry of Defence, The Strategic Defence Review 2025 – Making Britain Safer: Secure at Home, Strong Abroad, 2 June 2025, https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad.

Iran and DPRK to sustain and advance prohibited programmes depends in part on access to finance, trade and dual-use technology.

In this context, the Defence Review supports a whole-of-government approach to countering proliferation, aligning defence policy with sanctions implementation, export controls, corporate transparency reforms and AML/CTF regulation. Together, these measures strengthen the UK's ability to identify and disrupt pathways that could otherwise be exploited to finance or enable nuclear and missile programmes.

Domestic PF Developments since the 2021 NRA

Regulatory overview

2.10 The UK has in place a comprehensive and targeted regulatory framework to counter proliferation financing, combining targeted financial and trade sanctions, and the AML/CTF regime, including requirements under the MLRs. The UK's first Proliferation Financing National Risk Assessment (2021) set out the core architecture of this framework. While its foundations remain unchanged, the government has responded to significant developments in the policy, sanctions and risk landscape since 2021.

2.11 A central component of this framework is the implementation of UK and UN financial sanctions regimes, particularly those relating to DPRK and Iran[14]. Both UN and UK autonomous sanctions are implemented under powers provided by the **Sanctions and Anti-Money Laundering Act 2018 (SAMLA)**, specifically through **the DPRK (Sanctions) (EU Exit) Regulations 2019** and **the Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019**.[15] These sanctions apply to conduct in the UK by any person and also to UK persons anywhere in the world. Amongst other things, these sanctions prohibit the making available of funds or economic resources (directly or indirectly) to (or for the benefit of) designated persons.

2.12 The UK embeds these obligations insofar as these implement UNSCRs within its wider AML/CTF framework. This framework supports the mitigation of PF risk under the MLRs.

2.13 The MLRs impose requirements for regulated firms to assess and mitigate PF risk as part of their business-wide risk assessments and

[14] "UN financial sanctions regimes" in this context means UK regulations which impose sanctions for the purpose of giving effect to the United Kingdom's obligations under relevant UNSCRs.

[15] The Sanctions and Anti-Money Laundering Act 2018, https://www.legislation.gov.uk/ukpga/2018/13/contents; The Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, https://www.legislation.gov.uk/uksi/2019/411/contents; The Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019, https://www.legislation.gov.uk/uksi/2019/461.

transaction monitoring.[16] This approach ensures effective supervision and enforcement across the UK system.

2.14 Together, these tools provide the core legal and supervisory framework for detecting, preventing and disrupting proliferation financing activity, supported by enforcement and operational measures across government.

New PF risk assessments required for businesses through the MLRs

2.15 Since the publication of the 2021 PF NRA, regulated firms and individuals are required to identify, assess and mitigate PF risk as part of their business-wide risk assessment (Regulation 18A of the MLRs) and to establish and maintain appropriate policies, controls and procedures to manage these risks (Regulation 19A). [17]

2.16 These requirements apply to all relevant persons under the MLRs. Regulated firms are therefore required to consider their exposure to PF risk having regard to their customers, products, services, delivery channels and geographic reach, including links to sanctioned jurisdictions, trade-based activity, complex corporate structures and alternative value-transfer mechanisms.

2.17 AML/CTF supervisors have supported the implementation of these requirements through their supervisory frameworks, thematic work, guidance and firm-specific interventions helping to improve regulated firms' understanding of these requirements and reinforce expectations around sanctions screening, effective customer due diligence, transaction monitoring and wider risk management controls.

2.18 Together, these measures have strengthened the UK's counter-PF framework by embedding PF risk assessment within firms' existing compliance arrangements and encouraging a more risk-based approach to identifying and mitigating proliferation financing risks.

Iran: re-imposition of nuclear-related sanctions

2.19 The UK implements two sanctions regimes that target specific activities carried out by actors in Iran: the Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019 and the Iran (Sanctions) Regulations 2023. The nuclear regulations give domestic effect to the UK's obligations under UNSCR 1737 and are aimed at restricting Iran's ability to develop nuclear weapons and related delivery systems. These measures impose targeted financial and trade restrictions on individuals and entities involved in proliferation-sensitive activities.

2.20 Due to Iran's persistent and significant non-performance of its Joint Comprehensive Plan of Action (JCPoA) commitments, in August 2025 the UK, France and Germany triggered the "snapback"

---

[16] Regs. 18A & 19A, Money Laundering Regulations.

[17] Ibid.

mechanism, bringing UN sanctions back into effect. The UK has also introduced further autonomous nuclear-related sanctions on Iran: this includes designation of key Iranian energy, financial and nuclear entities and individuals. In September 2026, the UK laid a Statutory Instrument to introduce sectoral measures on Iran which are broadly those lifted as part of the JCPOA.[18] These measures include financial prohibitions on the Government of Iran's ability to access the UK financial systems and raise funds. Trade prohibitions against Iran are expanded to additional goods, technology and services, including those key to significant industries contributing to Iranian nuclear escalation such as energy, software, metals, gold, and related activities such as shipping, insurance and banking. The export of additional goods and technology key to Iran's conventional weapons and nuclear capabilities is also prohibited.

Russia: sanctions and proliferation-related developments

2.21 UK sanctions against Russia are one of the UK's most extensive sanctions frameworks. Following Russia's full-scale invasion of Ukraine in February 2022, the UK rapidly expanded its sanctions framework against Russia. This includes asset freezes and prohibitions on making available funds and economic resources, as well as restrictions applying to certain Russian banks, capital markets, investment, correspondent banking, sterling payments, reserve and trust and asset management services.[19] One of the purposes of the Russia Regulations is encourage Russia to cease actions destabilising Ukraine or undermining Ukraine's territorial integrity, sovereignty or independence, and cover financial, trade, transport, immigration and director-disqualification measures.

2.22 Beyond financial sanctions, the regime includes a number of prohibitions relevant to this Assessment. In particular, wider trade and service controls, including restrictions on professional and business services, technology transfer, sectoral software, imports, the imposition of a maritime services ban and the implementation of the Oil Price Cap.

2.23 Russia sanctions address typologies which are also relevant to proliferation financing: opaque ownership, sanctions evasion, third-country procurement, dual-use goods, financial facilitation and the use of intermediaries to obscure end-users. Government guidance and enforcement activity now places significant emphasis on countering Russian sanctions evasion and circumvention, including through freight, shipping and high-priority goods controls.

---

[18] The Iran (Sanctions) (Amendment) Regulations 2026, https://www.legislation.gov.uk/uksi/2026/983/contents/made.

[19] Foreign, Commonwealth and Development Office, HM Treasury, Department for Transport, 'Russia sanctions: statutory guidance', updated 20 May 2026, https://www.gov.uk/government/publications/russia-sanctions-guidance/russia-sanctions-guidance.

Russia-related chemical weapons sanctions

2.24 Since the 2021 PF NRA, the UK has used its autonomous Chemical Weapons (Sanctions) (EU Exit) Regulations 2019 to designate Russian individuals and entities involved in the use and development of chemical weapons. In October 2024[20], the UK designated Russia's Radiological, Chemical and Biological Defence Troops and their commander, Igor Kirillov, for their role in the deployment of chemical weapons on the battlefield in Ukraine.

2.25 In July 2026[21], the UK designated seven individuals and two Russian scientific research institutes, involved in the development and production of chemical agents (including Novichok nerve agents and the toxin Epibatidine), under Chemical Weapons (Sanctions) (EU Exit) Regulations 2019. The sanctions were introduced in response to Russia's continued involvement in activities prohibited under the Chemical Weapons Convention and Biological and Toxins Weapon Convention, including the poisonings of Alexei Navalny and Dawn Sturgess.

2.26 While UK autonomous sanctions regimes (including the Russia and chemical weapons regimes) do not fall within the specific PF Risk Assessment requirements under the MLRs, regulated firms should ensure that sanctions screening, customer due diligence and transaction monitoring controls are capable of identifying exposure to designated persons and related sanctions evasion risks.

Strategic military and dual-use items

2.27 The UK's comprehensive sanctions regime is complemented by robust controls on the export of strategic military and proliferation sensitive dual-use items. The Export Control Act 2002 and the Export Control Order 2008 provide the legislative framework for these controls. A body of assimilated legislation and current EU legislation are also relevant. The overall framework therefore ensures the continuity of existing controls whilst also enabling the UK to update and strengthen its regime.

2.28 The vast majority of the UK's export controls come from our commitments to international export control regimes. These regimes, though their collective expertise, determine what items are added to control list for non-proliferation purposes. Since all participating states control the same items there is an effective international level playing field.

---

[20] Foreign, Commonwealth and Development Office, 'UK sanctions Russian troops deploying chemical weapons on the battlefield', 8 October 2024, https://www.gov.uk/government/news/uk-sanctions-russian-troops-deploying-chemical-weapons-on-the-battlefield.

[21] Foreign, Commonwealth and Development Office, 'UK sanctions Russians developing chemical weapons used to kill Alexei Navalny and Dawn Sturgess', 6 July 2026, https://www.gov.uk/government/news/uk-sanctions-russians-developing-chemical-weapons-used-to-kill-alexei-navalny-and-dawn-sturgess.

2.29 In addition to this, the UK's Dual-Use Items (Export Control) Regulations 2000[22] allow the Government to impose an authorisation requirement for the export of non-listed dual-use items if the exporter has been informed by the Secretary of State that the items in question are or may be intended, in their entirety or in part, for a WMD purpose, i.e. for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons.

2.30 If an exporter is aware or suspects that non listed dual-use items which he proposes to export, are intended, in their entirety or in part, for a WMD purpose he must notify the Secretary of State, who will decide whether it is expedient to make the export concerned subject to authorisation.

Sanctions end-use controls

2.31 Trade sanctions end-use controls for UK-autonomous sanctions regimes came into force in May 2026, strengthening the UK's ability to address risks of sanctions circumvention through indirect supply chains.[23]

2.32 These measures enable the government to impose licensing requirements on the export of goods where there is a risk that they may ultimately be used in connection with a sanctioned programme or destination, including where this risk arises through third-country intermediaries or complex supply chains.

2.33 These controls complement export controls and sanctions by allowing the government to act proactively where risks are identified and disrupt procurement and proliferation networks that may not involve UK financial sanctions but that still present a proliferation financing risk.[24]

Reforms to Companies House

2.34 As recognised in the 2021 PF NRA, the misuse of corporate structures can facilitate illicit activity, including proliferation financing, by obscuring ownership and control and creating a veneer of legitimacy. Criminal actors may exploit UK-registered entities to access financial and professional services, embed themselves within global

---

[22] The Dual-Use Items (Export Control) Regulations 2000, https://www.legislation.gov.uk/uksi/2000/2620/made.

[23] The Sanctions (EU Exit) (Miscellaneous Amendments) Regulations 2026, https://www.legislation.gov.uk/uksi/2026/443/made.

[24] Department of Business and Trade & Office of Trade Sanctions Implementation, 'Sanctions End-Use Controls: guidance for businesses', 22 April 2026, https://www.gov.uk/government/publications/sanctions-end-use-controls-guidance-for-businesses/sanctions-end-use-controls-guidance-for-businesses#sanctions-end-use-controls-seuc.

supply chains, and disguise the true end-user or beneficiary of transactions.

2.35 Since 2021, the UK has taken significant steps to strengthen the integrity of its corporate registration framework and reduce the risk of abuse. These reforms are designed to improve the accuracy, transparency and reliability of information held at Companies House, and to limit the ability of illicit actors to establish and operate opaque corporate structures.

2.36 The Economic Crime and Corporate Transparency Act 2023[25] (ECCTA) introduced a range of measures to strengthen Companies House as an active gatekeeper of corporate data. These include the introduction of identity verification requirements for company directors, people with significant control and those submitting filings; enhanced powers for the Registrar to query information and reject or remove inaccurate filings; and stronger powers to disrupt and strike off companies suspected of being used for unlawful purposes. These changes are intended to reduce the ability of actors, including those involved in proliferation financing, to exploit UK corporate structures to conceal their activities.

2.37 In addition, the Economic Crime (Transparency and Enforcement) Act 2022[26] established the Register of Overseas Entities, requiring overseas entities that own UK property to disclose their beneficial owners to Companies House. This enhances transparency in relation to UK property ownership and supports efforts to identify and disrupt illicit financial flows linked to complex ownership structures.

2.38 Together, these reforms represent a significant strengthening of the UK's ability to prevent the misuse of corporate structures. By improving the quality of data, increasing transparency and enhancing the powers available to Companies House, the UK is better positioned to detect and disrupt the use of companies in support of PF activity.

Companies House Strategy (2025–2030)

2.39 Building on reforms introduced through ECCTA, the Companies House Strategy 2025–2030[27] sets out a further transition towards it becoming an active gatekeeper of corporate data, with an enhanced role in disrupting economic crime, including PF.

2.40 Companies House has expanded its intelligence capability, supported by Economic Crime (AML) Levy funding of over £4m since 2023-24. It has funded a new intelligence unit of c.20 people, which has

---

[25] The Economic Crime and Corporate Transparency Act 2023, https://www.legislation.gov.uk/ukpga/2023/56/contents.

[26] Economic Crime (Transparency and Enforcement) Act 2022, https://www.legislation.gov.uk/ukpga/2022/10/contents.

[27] Companies House, Companies House Strategy 2025 to 2030, 18 November 2025, https://www.gov.uk/government/publications/companies-house-strategy-2025-to-2030/companies-house-strategy-2025-to-2030.

improved the detection of money laundering taking place through corporate entities.

2.41 The intelligence unit uses advanced data techniques to analyse company behaviours at scale and detect suspicious activities, alongside conducting risk assessments of companies and transactions to detect non-compliance and target enforcement activity.

2.42 Companies House is also expanding its collaboration with trusted partners at home and abroad, using combined data, intelligence, powers, and financial or criminal penalties to have the greatest effect. It also raises awareness of emerging threats and provides advice to individuals and businesses on measures to safeguard their information, promoting its actions to deter future criminal behaviour where appropriate.

Regulation of cryptoassets

2.43 Since the 2021 PF NRA, cryptoassets have become an increasingly significant PF risk, particularly through their use by proliferators to generate revenue, move funds and evade sanctions (see Chapter 3). In response, the UK has continued to strengthen its cryptoasset regulatory framework, including through implementation of the Cryptoasset Transfer Funds Rule ("Travel Rule") in September 2023, in line with FATF standards for virtual assets and virtual asset service providers.

2.44 The UK has also strengthened its ability to investigate and disrupt illicit cryptoasset activity through the ECCTA[28]. The Act introduced new powers for law enforcement agencies to search for, seize, detain and recover cryptoassets linked to criminal conduct, supported by a dedicated code of practice. These measures enhance the UK's ability to identify and recover cryptoassets linked to sanctions evasion, proliferation financing and other forms of illicit finance, helping to reduce opportunities for proliferators and their facilitators to exploit digital assets.

2.45 We are now going further. It is vital that the UK's cryptoasset recovery powers remain fully effective as cryptoasset technologies and business models evolve. Measures included in the Financial Services & Markets Bill 2026, which is currently before Parliament, will, if passed, introduce a targeted delegated power to allow updates to existing cryptoasset recovery powers to be updated via secondary legislation.

2.46 If the measures are passed, the government intends to publish a Statutory Instrument making technical wording changes to Cryptowallet Freezing Orders (CWFOs). This will address drafting issues

[28] Home Office, Department for Business and Trade, HM Treasury, Ministry of Justice, 'Economic Crime and Corporate Transparency Act: cryptoassets – legislation', updated 1 March 2024, https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-act-2023-factsheets/economic-crime-and-corporate-transparency-act-cryptoassets-legislation

that currently prevent them from being used in the full range of scenarios originally intended.

2.47 In the UK, certain cryptoasset activities fall within the supervisory remit of the Financial Conduct Authority (FCA) under the AML/CTF regime. Since January 2020, cryptoasset exchange providers and custodian wallet providers (CASPs), as defined in the MLRs, have needed to register with the FCA for MLRs supervision. Registered firms facilitate their customers' exchange and transfer of various types of cryptoassets, by providing services such as exchanging cryptoassets for other cryptoassets or money and vice versa. They can also provide services for the safeguarding and/or administration of cryptoassets or private cryptographic keys on behalf of customers. The FCA has maintained a robust registration gateway, with firms required to meet the UK's AML standards before registration. The number of FCA registered cryptoasset firms has increased from four at the end of 2020, to 62 as of August 2026.[29]

2.48 In February 2026, the Government legislated for a financial services regulatory regime for cryptoassets.[30] This will extend the FCA's supervisory perimeter from the current MLR framework to include certain cryptoasset activities from October 2027. Firms carrying out regulated cryptoasset activities will be required to obtain FCA authorisation and will have to follow the FCA Handbook, in addition to following obligations under the MLRs. This includes the ongoing obligation on firms to ensure they are not used for a purpose connected with financial crime. Firms will have to operate proportionate financial crime controls and report information to the FCA who can monitor, challenge and act where deficiencies or failures in those controls occur.

2.49 The application of existing or, where necessary, adapted FCA Handbook systems and controls requirements seek to strengthen the governance, prudential management, operational resilience and senior management accountabilities in cryptoasset firms.

2.50 Unregistered exchanges and/or those outside of the FCA perimeter who are instead registered in jurisdictions with more limited oversight represent the greatest threat in terms of cryptoasset money laundering. They often have less stringent identity checks and, as such, appeal to those looking to launder and move cryptoassets. Where there is limited UK nexus to this threat activity, powers for UK authorities including the FCA to directly intervene can be limited.

2.51 In June 2026, the FCA published a series of policy statements on how the FCA Handbook will apply to regulated cryptoasset activities.[31]

---

[29] The list of all FCA-registered and formerly registered firms can be found here: https://register.fca.org.uk/s/search?predefined=CA.

[30] The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, https://www.legislation.gov.uk/uksi/2026/102/contents/made.

[31] Financial Conduct Authority, 'Overview of our cryptoassets regime policy statements', 30 June 2026, https://www.fca.org.uk/publications/policy-statements/cryptoasset-regime.

The FCA intends to provide further clarity on financial crime requirements, through updates to the Financial Crime Guide.[32] These updates aim to ensure a consistent and comprehensive framework, including clear guidance and practical examples of good and poor practice. The FCA will also consult on these changes later this year.

Employment protections for sanctions-related disclosures

2.52 In 2025, secondary legislation was introduced to help workers benefit from whistleblowing protections when making sanctions-related disclosures to HM Treasury, the Department for Transport, and the Department for Business, Innovation, Science and Trade.[33] This legislation helps whistleblowers qualify for protections against being subject to detriment or dismissal following disclosure of information relating to financial, transport, and certain trade sanctions to the relevant department. This provides a clearer framework for when the relevant whistleblowing protections apply, complementing the UK's broader whistleblowing framework.

Growth of OFSI and future strategy

2.53 Since 2021, OFSI's capacity has increased, as described in its Annual Review 2023–24[34]. Staffing has increased significantly, including a fourfold expansion of its licensing and enforcement teams and the near doubling of its guidance and engagement function. OFSI has also invested in advanced data analytics, cryptocurrency investigation tools, and specialist corporate and data platform access, materially enhancing its ability to identify sanctions breaches and support proactive, intelligence led enforcement.

2.54 Building on this expansion, OFSI's Strategy 2026–29[35] marks a transition from growth to sustained, risk-based delivery, setting out a clear operating model focused on promoting compliance, enabling legitimate activity, responding quickly and proportionately to breaches, and embedding learning into sanctions design. The Strategy places particular emphasis on deepening threat understanding, targeting resources to areas of highest impact, and strengthening partnerships across government, industry and international allies.

---

[32] Financial Conduct Authority, 'Financial Crime Guide', 3 June 2025, https://handbook.fca.org.uk/handbook/fcg1.

[33] The Public Interest Disclosure (Prescribed Persons) (Amendment) Order 2025, https://www.legislation.gov.uk/uksi/2025/604/made; The Public Interest Disclosure (Prescribed Persons) (Amendment) Order 2014, https://www.legislation.gov.uk/uksi/2025/604/made; The Employment Rights Act 1996, https://www.legislation.gov.uk/ukpga/1996/18/contents.

[34] Office of Financial Sanctions Implementation, OFSI Annual Review 2023 to 2024: Engage, Enhance, Enforce, 21 March 2025, https://www.gov.uk/government/publications/ofsi-annual-review-2023-24-engage-enhance-enforce.

[35] HM Treasury and OFSI, OFSI Strategy: 2026-2029, 15 April 2026, https://www.gov.uk/government/publications/ofsi-strategy-2026-2029.

Introduction of OTSI

2.55 The UK enhanced its trade sanctions framework with the establishment of OTSI in October 2024, within what was then the Department for Business and Trade (DBT).

2.56 OTSI is the UK Government unit responsible for the civil enforcement of trade sanctions, with responsibility for the provision or procurement of certain sanctioned services, the movement, the making available or acquisition of certain sanctioned goods or technology outside the UK, and ancillary services linked to such activities.

2.57 These functions are directly relevant to PF risk, particularly where trade-based activity, services provision or overseas supply chains are used to support the procurement of restricted goods or technology.

2.58 OTSI works closely with other bodies, including HMRC, which has criminal enforcement responsibility for most trade sanctions and leads on enforcement of trade sanctions where goods and technology cross the UK border. Where OTSI investigations identify conduct that may warrant criminal prosecution, cases may be referred to HMRC.

2.59 In addition to enforcement, OTSI plays a central role in supporting business compliance. This includes producing guidance, undertaking industry engagement and outreach, and administering trade sanctions licensing.

2.60 OTSI is equipped with a range of civil enforcement powers, including the ability to impose civil monetary penalties. These powers were provided through the Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations (TASSCER)[36] and are intended to strengthen compliance incentives, deter circumvention and enable the publication of compliance lessons for industry. OTSI has published guidance[37] outlining how it assesses suspected breaches of trade sanctions.

International updates

Multilateral Sanctions Monitoring Team

2.61 In 2024, the UN Panel of Experts on DPRK sanctions was discontinued, creating a gap in international monitoring and reporting on North Korea's sanctions evasion and proliferation related activity. In response, the Multilateral Sanctions Monitoring Team (MSMT) was established by a coalition of eleven countries, including the UK, to coordinate and sustain technical monitoring, analysis and information sharing on DPRK sanctions implementation.

---

[36] The Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, https://www.legislation.gov.uk/uksi/2024/948/contents.

[37] Department for Business and Trade and Office of Trade Sanctions Implementation, How Suspected Breaches of Trade Sanctions are Assessed by the Office of Trade Sanctions Implementation (OFSI), 12 September 2024, https://www.gov.uk/guidance/how-suspected-breaches-of-trade-sanctions-are-assessed-by-the-office-of-trade-sanctions-implementation-otsi.

2.62 The UK has taken on a leading role within the MSMT, including through chairing the mechanism, reinforcing its commitment to maintaining international scrutiny of DPRK proliferation activity. The MSMT supports continued identification of sanctions evasion and PF typologies, and provides an important platform for cooperation outside the UN system.

FATF report on proliferation financing trends

2.63 In June 2025[38], the FATF published its report *Complex Proliferation Financing and Sanctions Evasion Schemes*, to which the UK contributed. The report highlights the increasingly sophisticated methods used by proliferators to evade sanctions and procure sensitive goods, including the use of front companies, intermediaries, complex ownership structures, trade-based schemes and cryptoassets. The report reinforces the importance of firms adopting a risk-based approach that combines sanctions screening with effective customer due diligence, transaction monitoring and wider financial crime controls.

[38] Financial Action Task Force, 'FATF Report: Complex Proliferation Financing and Sanctions Evasion Schemes', June 2025, Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

Chapter 3

Proliferation Financing Threats Facing the UK

3.1 This chapter outlines the primary proliferation financing threats facing the UK. The chapter will provide an overview of the threats, an indication of where those threats have developed since the 2021 PF NRA, and detail the actors involved in PF. Typologies most relevant to the UK are covered in further detail, with case study examples.

3.2 The chapter covers:

i. The role of state and non-state actors;

Typologies involving the abuse of corporate structures, including:

a. Front companies;

b. Intermediaries;

c. Obscuring beneficial interest;

ii. Typologies involving exports and shipping;

iii. Typologies involving remote IT workers in specific jurisdictions;

iv. Typologies involving cryptoassets;

v. Threats from illicit use of Artificial Intelligence.

The role of state and non-state actors

3.3 PF threats to the UK are driven by the interaction between (a) state actors which direct and ultimately benefit from proliferation programmes and sanctions evasion, and (b) non-state actors which enable, facilitate, or profit from those activities. The UK's exposure is heightened by its role as a global financial and trading hub, meaning UK firms can be engaged, often inadvertently and indirectly, at multiple points in cross-border procurement and financing chains.

State actors

3.4 The state actors involved in PF can be split into four broad categories. These are:

i. Jurisdictions subject to UN counter-proliferation sanctions regimes, who aim to evade those sanctions in order to procure restricted materiel and fund their nuclear programmes. These states are currently **Iran** and **DPRK**. Iran poses a sustained proliferation risk as a nuclear threshold state, where it retains the

technical capability, materials, and expertise to develop nuclear weapons at speed.[39] DPRK has continued to develop, test, and invest in its nuclear and ballistic missile programmes, including the recent launch of a ballistic missile on the 19 April 2026.[40]

ii. Partnering jurisdictions which have agreements with Iran and DPRK in breach of UN sanctions. Most notable of these is **Russia**, who have developed "Comprehensive Strategic Partnerships" with both Iran and the DPRK since 2021.[41]

iii. Enabling jurisdictions, which provide a permissive regulatory environment for non-state actors/enablers to facilitate PF. **China**, which maintains strong political ties to the DPRK, is a key example.

iv. Jurisdictions with trade links to the UK who maintain a weak regulatory environment, and/or have free trade zones, which may inadvertently facilitate PF.

3.5 **DPRK** and **Iran** remain the principal state-level PF threats to the UK because they have the incentive and capabilities to evade UN/UK sanctions and export controls, procure controlled goods/technology, and generate revenue for nuclear programmes.

3.6 **Iran** continues to rely heavily on procurement networks to obtain military and dual-use items and sensitive technology.[42] UK-linked risks include attempts to divert UK-origin goods through complex routing, and documentation designed to obscure end users.

3.7 **DPRK** has evolved as a PF actor since 2021, using cybercrime and cryptoasset theft to generate revenue streams which can be laundered and redirected to state priorities, including the state sponsored development of nuclear capabilities.[43] These methods reduce reliance on the mainstream banking system, making detection more difficult. DPRK has also developed its capacity to exploit global labour markets through remote IT work to generate income and access Western IT systems.

3.8 Since 2021, **Russia**'s role as an enabler of PF has grown. Russia has signed formal "Comprehensive Strategic Partnerships" with both DPRK (2024) and Iran (2025). These promise closer political, trade,

---

[39] Intelligence and Security Committee of Parliament, 'Iran', 10 July 2025, https://isc.independent.gov.uk/wp-content/uploads/2025/07/Intelligence-and-Security-Committee-of-Parliament-Iran.pdf.

[40] Foreign, Commonwealth and Development Office, 'FCDO Statement on DPRK ballistic missile launches: 19 April 2026, FCDO statement on DPRK ballistic missile launches: 19 April - GOV.UK.

[41] Transcend Media Service, 'Full Text of Russia-North Korea Strategic Agreement', 24 June 2024, https://www.transcend.org/tms/2024/06/full-text-of-russia-north-korea-strategic-agreement/; Reuters, 'Key Provisions of Russia-Iran Strategic Cooperation Treaty', 17 January 2025, https://www.reuters.com/world/key-provisions-russia-iran-strategic-cooperation-treaty-2025-01-17/.

[42] FATF, 'Complex Proliferation Financing and Sanctions Evasion'.

[43] Multilateral Sanctions Monitoring Team, 'The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities', 22 October 2025, https://msmt.info/Publications/detail/MSMT%20Report/4221.

investment and security ties between the nations. This cooperation has expanded further into direct military and economic exchanges. DPRK and Iran have supplied Russia with significant quantities of munitions, missiles and personnel, to support its war in Ukraine, with reports indicating the deployment of thousands of DPRK troops and large-scale transfers of artillery and weapons. In return, Russia has provided material and economic support to the DPRK, including the supply of oil, transported via maritime shipments and rail transfers, which helps sustain the DPRK economy in contravention of UN sanctions regimes.

3.9 This behaviour is consistent with broader Russian activity that undermines international counter-proliferation efforts, including reported use of prohibited chemical agents in Ukraine.[44] This further highlights the risk posed by state actors willing to disregard established controls on WMD-related materials.[45]

3.10 Russia has also become a major host for DPRK IT workers, who had previously been largely based in China.[46] These IT workers seek employment with UK firms in order to earn income that is remitted to the DPRK regime, supporting their nuclear and ballistic missile programmes. This is set out in further detail at paragraph 3.30.

3.11 **China**'s role has been consistent since 2021. In addition to hosting IT workers, China remains a place where DPRK-linked networks can source goods, set up trading companies, and route shipments and payments in ways which obscure the end user. There is particular risk to the UK due to established trade networks between the UK and China. Where UK firms sell to a China-based trader, or UK finance and insurance is used to support trade, it can be difficult to verify where goods end up and who ultimately benefits. The MSMT have identified that DPRK relies heavily on Chinese banks to access China's formal financial system to facilitate payments and procure materials.[47]

3.12 Finally, the United Nations Interregional Crime and Justice Research Institute (UNICRI)[48], supported by the UK, has worked with countries in **Southeast Asia** to strengthen understanding of PF risks arising from the region's integration into global trade, shipping and financial networks. This work has highlighted vulnerabilities associated with major transhipment hubs, free trade zones and complex cross-

---

[44] BBC, 'Russia using North Korean missiles to strike Ukraine, Zelensky says', 11 August 2026, https://www.bbc.co.uk/news/articles/c151dpzwnvxo.

[45] Foreign, Commonwealth and Development Office and Neil Holland, 'Russia's shameful record-breaking attacks on Ukrainian civilians and use of chemical weapons on the front line in Ukraine are a disgrace: UK statement to the OSCE', 10 July 2025, https://www.gov.uk/government/speeches/russias-shameful-record-breaking-attacks-on-ukrainian-civilians-and-use-of-chemical-weapons-on-the-front-line-in-ukraine-are-a-disgrace-uk-statement.

[46] MSMT, 'The DPRK's Violation and Evasion of UN Sanctions'.

[47] Ibid., 48.

[48] United Nations Interregional Crime and Justice Research Institute (UNICRI), 'CBRN Proliferation Financing: A perspective from Southeast Asia', October 2023, https://unicri.org/Publication-CBRN-Proliferation-Financing-Perspective-from-Southeast-Asia.

border trade flows, which may be exploited by DPRK and Iranian procurement networks to obscure end users, evade sanctions and facilitate proliferation-related activity.

Non-state actors

3.13 Non-state facilitators may be ideologically aligned, coerced, or purely profit-motivated. They can be based in a proliferating state, in third-countries, or in the UK. Common facilitator roles include:

- procurement agents and brokers sourcing controlled items and arranging shipment;
- financial facilitators structuring payments, providing access to accounts, moving value through layered transactions, or through cryptoasset businesses;
- corporate service providers establishing and maintaining entities used as fronts;
- professional service providers (lawyers, accountants, consultants) whose services may be misused to provide legitimacy, manage trusts, or create complex ownership structures;
- other professional enablers who may knowingly facilitate proliferation financing activity, or whose weak risk assessments, customer due diligence, or wider risk management controls may be exploited by PF actors.

3.14 **Proscribed terrorist and militia groups** form part of wider state-aligned networks that may be relevant to proliferation financing risk. In particular, Iran has been identified as providing financial, logistical and operational support to groups including Hizballah, Hamas and other regionally active proxies.[49] These groups operate within broader Iranian networks and may rely on typologies such as front companies, intermediaries and complex financial arrangements to access the international financial system and move funds or economic resources.[50]

3.15 Terrorist and militia groups may also be interested in the development of chemical, biological or nuclear weapons for their own purposes, beyond links with proliferating states. While primarily associated with terrorist financing, these networks may overlap with PF risks where shared financial channels or procurement networks are used to support the development of such technologies. Firms should remain vigilant to any links, direct or indirect, to these organisations.

---

[49] Intelligence and Security Committee, 'Iran'.

[50] US Treasury Financial Crimes Enforcement Network, 'FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations', 8 May 2024, https://www.fincen.gov/system/files/advisory/2024-05-07/FinCEN-Advisory-Iran-Backed-TF-508C.pdf.

Abuse of corporate structures

Front and shell companies

3.16 Front and shell companies provide a seemingly legitimate commercial façade for illicit actors to:

- Access financial systems and facilitate payments;
- Import/export dual-use goods under false pretences; and
- Obscure the end-user by operating under different names and ownership structures, and obscure the beneficiary country.

3.17 Within the UK financial system, such companies may allow actors to open and operate bank accounts, contract with suppliers and logistics providers, obtain credit terms and trade finance, issue invoices and purchase orders that disguise the true end user and/or end use, and create plausible "business rationale" for cross-border payments.

3.18 Despite recent reforms to Companies House (Chapter 2, above), the ease at which companies can be incorporated in the UK continues to put the UK at particular risk. The UK has the second highest number of registered companies in the world, and is consistently the country with the highest number of new incorporations per year, according to data from the International Business Registers Report.[51] Companies House's first Strategic Intelligence Assessment, from October 2024, notes that abuse of the UK company register is a growing issue.[52]

3.19 There is also evidence that overseas front or shell companies, often established in countries with regulatory loopholes, constitute an additional risk, as they can serve as intermediaries, and obscure the true end-user (further detail on these typologies below).

[51] Data from the International Business Registers Report, 'Business Dynamics 2018-2022', quoted in Companies House, 'Strategic Intelligence Assessment', 24 October 2024, https://www.gov.uk/government/publications/companies-house-strategic-intelligence-assessment/companies-house-strategic-intelligence-assessment#exploitation-of-business-and-state.

[52] Companies House, 'Strategic Intelligence Assessment'.

Case Study 1 – Companies House action against UK-registered companies linked to Iranian sanctions evasion and cryptoasset activity

- In 2026, Companies House took action under its strengthened powers to remove UK-registered entities linked to Iranian sanctions evasion and cryptoasset activity from the UK corporate register. **Zedcex Exchange Limited** and **Zedxion Exchange Limited** had been incorporated in the UK, but Companies House identified concerns that the companies were not operating from their registered addresses and that the individual recorded as a director could not be verified.
- Companies House subsequently exercised its powers to remove the companies from the register in May 2026, alongside other entities linked to the wider network. This demonstrated the use of strengthened registrar powers to improve the integrity of the UK corporate register and disrupt the misuse of UK entities.
- Analysis by TRM Labs assessed that Zedcex and Zedxion appeared to operate as a single enterprise, despite being incorporated as separate UK companies, and had processed approximately **USD 1 billion** in funds linked to the IRGC between 2023 and 2025.
- **This case study highlights how UK-incorporated entity creation can be exploited to create a veneer of legitimacy for sanctions evasion and illicit financial activity. It also demonstrates the importance of effective corporate transparency measures, and the ability of authorities to identify and remove companies associated with deceptive or high-risk activity from the corporate register.**
- **For UK firms and individuals, the case reinforces the need to look beyond the existence of UK incorporation when assessing risk.**

Case Study 2 – Operation Hammerhead – Exposing the abuse of UK corporate structures linked to the DPRK

- Operation Hammerhead (2022-25) was a National Economic Crime Centre-led, multi-agency initiative targeting the misuse of UK corporate structures by criminal networks through company formation agents, shell companies, and virtual business addresses. Led by intelligence from the Insolvency Service and Companies House, the operation involved the NCA, UK policing, the FCA, HMRC and other partners. It identified more than 43,000 suspicious companies linked to just 43 UK address clusters, many registered as dormant, sharing directors and addresses, and showing little or no genuine economic activity.
- Investigations revealed how these corporate structures were used to facilitate trade-based money laundering (TBML), movement of illicit funds, investment and visa fraud, and large-

scale online frauds. Many entities were established through Trust and Company Service Providers (TCSPs), with registration payments frequently originating from mainland China and Hong Kong. Financial analysis identified significant cross-border transaction flows, often conducted through Chinese bank accounts and UK electronic money institutions.

- Of particular concern were the national security implications. Insolvency Service intelligence linked elements of the Hammerhead network to DPRK sanctions evasion, proliferation financing, and cyber-enabled crime. One corporate director and service provider associated with the network was identified by the United Nations as owning vessels linked to the North Korean shipping fleet. Further intelligence connected Hammerhead-linked entities to individuals previously implicated in DPRK sanctions-busting activity and the laundering of proceeds associated with the Lazarus Group, the North Korean state-sponsored cybercrime organisation believed to be responsible for major international cyber thefts.
- **The case demonstrates how opaque corporate structures and company formation services can be exploited to conceal beneficial ownership, move illicit funds and support sanctioned actors. Hammerhead ultimately resulted in over 11,500 companies being placed into strike-off processes, enforcement action against 30 TCSPs, the closure of three providers, and the development of a multi-agency model for disrupting shell-company networks linked to economic crime and national security threats.**

Red flag indicators: front and shell companies

The following indicators may suggest that a company is being used as a front or shell structure to facilitate illicit activity, including for proliferation financing:

- Use of Companies House default postcodes and addresses in the company's filing history may suggest that the company has used an address fraudulently.
- Frequent changes to the Registered Office Address or to company officers, especially shortly after incorporation.
- Misuse of the Dormant Company SIC code (99999), where the company is clearly trading.
- Sudden changes in business activity (SIC codes) without clear rationale.
- Multiple companies registered at a single address, especially residential.
- Business activity that doesn't match filing history, online presence, or behaviour.
- Poor filing and compliance behaviour – including late or missing filings, accounts discrepancies, very high share capital for nature of business.

These indicators alone do not necessarily confirm suspicious/criminal activity and should be considered alongside other general indicators around the obfuscation of ownership and control (e.g. no Person of Significant Control, complex/opaque ownership structure, use of nominee directors and shareholders) or links to jurisdictions assessed as presenting elevated sanctions evasion, proliferation financing, money laundering or other illicit finance risks.

Intermediaries

3.20 Intermediaries are used by illicit actors to complicate and mask proliferation financing activity, as they add additional parties between the supplier and the ultimate end-user. Intermediaries facilitate transactions, both in the procurement of restricted, dual-use materials, and in securing the funding to support nuclear programmes.

3.21 Intermediaries can include:

- trading companies and brokers;
- procurement agents and sourcing firms;
- freight forwarders and logistics agents who arrange payments or act as consignees;
- overseas distributors and resellers;
- professional enablers.

3.22 Professional enablers are individuals or organisations that provide professional services that enable criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations. Professional enablers include lawyers, accountants, Trust and Company Service Providers (TCSPs), and any other intermediaries who aid in setting up or administering structures which conceal sanctioned or high-risk parties.

3.23 European intermediaries are often used by Iran to obscure the ultimate destination of goods. Iranian networks divert technology from the UK through mainland Europe or Central Asia in order to disguise the end-user. The funds used to pay for these goods are likely to have originated in Iran.

Case study 3 – Unregulated online remittance platform facilitating transfers between Iran and Western jurisdictions via informal settlement networks and cryptoassets

- An online remittance and foreign exchange platform, advertised money transfer services between Iran and a range of countries, including the UK, EU member states, the USA, Canada, the UAE, Türkiye, and China. The platform offers transfers in multiple fiat currencies as well as USDT, a US dollar-pegged cryptoasset. It displayed live exchange rates denominated in Iranian rial and quotes processing times consistent with those of legitimate regulated remittance providers, giving it a veneer of commercial credibility. The platform displayed no visible regulatory licence, no published AML/CTF or KYC policies and no clear statement of compliance with UK, US or EU sanctions regulations. Its likely operating model involves matching funds collected in Western jurisdictions against local payments made within Iran through partner accounts – a structure consistent with informal value transfer or hawala-style networks – supplemented by cryptoasset settlement to bridge jurisdictions where formal banking channels were unavailable or restricted. This model is specifically designed to avoid the formal banking system and the sanctions controls embedded within it, allowing funds to move to and from Iran without generating the transaction records that would ordinarily be subject to screening.
- **This case study highlights the PF risk posed by unregulated informal remittance platforms. Such platforms can in some cases facilitate the movement of funds that might otherwise be blocked, bypassing the controls maintained by regulated financial institutions.**
- **Although such transactions typically avoid the regulated financial sector altogether, regulated firms – including banks, payment institutions and cryptoasset businesses – should be**

alert to customer activity consistent with the use of such platforms, including unexplained transfers by Iranian nationals to jurisdictions commonly used as intermediary points for Iran-related flows, such as the UAE and Türkiye, and should apply enhanced due diligence accordingly.

Obscuring beneficial interest

3.24 PF actors may obscure the ultimate end user, or beneficiary, of goods and technology in order to defeat sanctions screening and complicate enforcement.

3.25 Common methods which may be used by PF actors, and which firms should be aware of, include:

- **Layered ownership chains:** multiple entities across jurisdictions, often with no clear operating purpose, used to distance the controlling party from the transacting entity.
- **Nominee directors/shareholders:** individuals who appear across many unrelated companies, sometimes linked to formation agents or corporate service providers.
- **Trust and foundation structures:** used to separate legal ownership from control/benefit, and to complicate identification of beneficiaries. (Russian designated persons and persons connected with Russia are prohibited from accessing trust services).[53]
- **Use of relatives/associates:** family members or close associates act as "clean" owners/controllers while the designated person retains de facto control.
- **Frequent changes:** rapid turnover of directors, shareholders, registered addresses, or company names—especially around the time of account opening, onboarding, or adverse media.
- **Fragmentation of control:** splitting ownership into small stakes across multiple persons/entities to complicate ownership structures.
- **Use of personal or third-party accounts**: the use of retail customer accounts, nominees or other intermediaries to consolidate or transfer funds on behalf of another person, including as part of informal value transfer systems (IVTS)

[53] Reg. 18C, The Russia (Sanctions) (Eu Exit) Regulations 2019, https://www.legislation.gov.uk/uksi/2019/855/regulation/18C.

arrangements - arrangements that move value outside formal financial channels through networks of brokers or intermediaries.

Export and shipping typologies

3.26 The UK's maritime and logistics sectors face exposure to PF risks, as proliferators rely on complex shipping routes and intermediary jurisdictions to obscure the end-user of any goods or payments provided. These obfuscation techniques can inadvertently involve UK-linked shipping and service providers, due to the UK's important role in the global shipping industry.

3.27 The most prominent typologies affecting shipping include:

- Complex trade routes and circuitous shipping which mask the true origin or destination of goods. These typologies can include:
    - Routing goods or payments through intermediate jurisdictions to obscure the ultimate beneficiary. Regional trading hubs and countries with weak export controls or sanctions enforcement mechanisms are often targets for this activity, and UK exposure is through links to these jurisdictions.
    - Using multiple shipping legs to break the direct link between origin and end-user.
    - Using freight forwarders and logistics firms as buffers between exporter and end user.
- Inconsistent or falsified shipping documents. Such documents include incorrect port details, consignees, and cargo descriptions.
- Unusual trade and/or financial structures, where the underlying goods or routes do not make commercial sense. These are often combined with layered payment chains involving multiple correspondent banks or intermediaries.
- Opaque ownership and/or management structures. These work to obscure the ultimate beneficiaries of the goods.
- Ship-to-ship transfers of goods. These often take place offshore, or in high-risk, low-regulation jurisdictions.
- Changes to the country of registration (i.e. flag changes), use of flags of convenience, and other masking activity, including manipulation of AIS navigation technology (also known as "going dark").

3.28 These typologies are not mutually exclusive, and often multiple different typologies can be used simultaneously, including in conjunction with financial sector typologies (above), in order to effectively obscure the ultimate destination of goods, or beneficiary of financial services.

3.29 These risks are heightened where firms have inadequate sanctions screening, weak customer due diligence, or limited ongoing monitoring, as proliferators deliberately target entities with weaker controls.

3.30 Maritime-related services such as insurers, brokers and logistics providers may also be exploited through complex corporate structures, front or shell companies, and layered ownership chains used to obscure sanctioned actors, or the nature of goods or destinations involved in specific voyages.

Typologies linked to remote IT workers in specific jurisdictions

3.31 The UK faces an increasing PF threat from DPRK state-linked IT workers fraudulently obtaining remote employment with UK firms to generate revenue for the DPRK regime. Once salaries and other payments have been received, DPRK networks may seek to transfer, convert and repatriate funds through financial institutions, EMIs, MSBs and cryptoasset service providers. As highlighted in **OFSI's Advisory on North Korean IT Workers**, this creates exposure not only for employers, but also for regulated firms involved in the processing, custody or transfer of funds that may ultimately benefit the DPRK regime.[54]

3.32 HMT assesses it to be almost certain that UK firms are currently being targeted by DPRK IT workers operating under false third-country identities to generate revenue for the DPRK regime, in breach of UN sanctions.

3.33 In addition to generating revenue, DPRK IT workers may obtain trusted access to company systems and data, creating a possibility of sensitive or proprietary information being compromised. This compounds the PF threat with wider national security and economic risks.

Case study 4 – threat from DPRK state-linked IT workers

- OFSI has reported an increase in suspected sanctions breach reports involving DPRK state-linked IT workers, reflecting the growing use of this typology to generate revenue for the DPRK regime. These reports highlight the risk that payments made through legitimate employment arrangements may ultimately benefit designated entities or the wider DPRK state, in breach of UK financial sanctions.
- In the United States, law enforcement disrupted and prosecuted

[54] Office of Financial Sanctions Implementation, 'Advisory on North Korean IT Workers', 12 September 2024, https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf.

a scheme in 2024–2025, in which a third-country facilitator (U.S. National) enabled DPRK IT workers to obtain remote IT roles at more than 300 U.S. companies across sectors including technology, media, manufacturing and retail.

- The facilitator bypassed employer controls by providing a domestic address for company-issued devices, creating the false impression that work was being performed in the United States. The facilitator also forwarded company-supplied laptops and other devices overseas, including multiple shipments to a city in China near the border with North Korea. This allowed DPRK workers operating overseas to access corporate networks while obscuring their true identity and location. The scheme relied on the theft and misuse of dozens of personal identities to pass recruitment and payroll checks.
- Payments were made through legitimate payroll channels and routed via financial accounts controlled by the facilitator before being transferred overseas to individuals linked to the DPRK. The scheme generated millions of dollars in income for the regime and exposed affected firms to cyber security, data protection and fraud risks through the trusted system access granted to the workers.
- **Although this case occurred in the United States, it highlights threats inherent from remote hiring and evolving techniques relevant to firms, illustrating how a single illicit scheme can expose many companies simultaneously to direct PF risk.**

Cryptoassets

Illicit use of cryptoassets

3.34 As set out in **OFSI's Cryptoassets Threat Assessment**[55], cryptoassets are increasingly being used by states subject to country-specific sanctions regimes, including Iran and DPRK, and their proxies to evade financial sanctions, facilitate payments for sanctioned goods and services, and move and store value outside the traditional banking system through complex networks of intermediaries.

3.35 Cryptoasset firms face exposure to sanctions evasion linked to Iran, DPRK and Russia, including the processing of transactions involving sanctioned individuals, entities and state-affiliated networks, as well as attempts to recover or reintroduce frozen assets into circulation. Cryptoassets are also increasingly being used by a wider range of OCGs to launder proceeds from crimes. Of USD 158 billion in

[55] Office of Financial Sanctions Implementation,' Sanctions Compliance in the Cryptoassets Sector: Threat Assessment', 21 July 2025, https://www.gov.uk/government/publications/sanctions-compliance-in-the-cryptoassets-sector-threat-assessment.

TRM-identified illicit crypto flows, USD 93 billion (or 59%) is linked to inflows to sanctioned entities and jurisdictions.[56] The generation, use and storage of proceeds derived from sanctions evasion activity typically occurs overseas. However, UK cryptoasset firms may become involved in the movement of these proceeds where threat actors employ sophisticated obfuscation techniques and route assets through international financial and cryptoasset networks. Where there is limited UK nexus to this threat activity, powers for UK authorities including the FCA to directly intervene can be limited.

3.36 Supervisors, law enforcement and OFSI have strengthened their response to the illicit use of cryptoassets for sanctions evasion and PF. This includes enhanced cross-system collaboration between regulators, enforcement agencies and the private sector. FCA-regulated firms are largely used as conduits for activities, whereas unregulated firms are more likely to be more complicit. In January 2026, OFSI worked with the National Crime Agency (NCA), the FCA and other partners to bring together law enforcement, regulators and private sector analytics providers to identify and disrupt sanctions breaches involving cryptoassets.[57]

[56] TRM Labs, 2026 Crypto Crime Report: Illicit Crypto Trends & Typologies, 28 January 2026, https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.

[57] National Crime Agency, 'OFSI and partners clamp down on the abuse of cryptoassets', 29 January 2026, https://www.nationalcrimeagency.gov.uk/news/ofsi-and-partners-clamp-down-on-the-abuse-of-cryptoassets?highlight=WyJjcmltZSIsIm5vIl0=.

3.37 Alongside these operational responses, the UK has strengthened the regulation of cryptoassets and expectations on regulated firms to identify, assess and mitigate PF risks (see Chapters 2 and 4).

OFSI Threat Assessment summary – Transfers involving Iranian cryptoasset firms with suspected links to designated persons

- OFSI assesses it is likely that UK cryptoasset firms are currently facilitating transfers involving Iranian cryptoasset firms with suspected links to designated persons.
- Such activity may expose UK firms to sanctions evasion and PF risks where cryptoassets are used to move value outside traditional financial channels.
- The use of cryptoassets by sanctioned entities increases this risk by obscuring transaction chains and reducing visibility of counterparties, due to privacy-enhancing technologies such as mixers, followed by cross-chain swaps to transfer value across blockchains. The use of such technologies alongside the role of OTC brokers and exchange hubs in sanctioned jurisdictions, make it more difficult for firms to identify and prevent sanctions breaches.
- **UK firms should be aware that this activity is taking place, and ensure that all possible steps are taken to identify the origins of funds before facilitating transfers.**

Cryptoasset theft

3.38 The threat from DPRK cyber activity targeting UK firms persists, with cryptoasset firms around the world at an elevated risk of being targeted for cryptoasset theft.

3.39 As of September 2025, DPRK-linked actors had stolen approximately £2 billion (c. US$2.8 billion) in cryptoassets during the period January 2024 to September 2025. The largest reported crypto theft was in February 2025 with the theft of approximately £1.1 billion (c. US$1.5 billion) in cryptoassets from a global cryptoasset exchange. [58]

3.40 The FCA wrote to all UK registered cryptoasset service providers shortly after the February 2025 theft to notify them of the heightened risk of their platforms being used for PF and associated money laundering.

3.41 More recent reporting indicates a significant escalation in the scale of DPRK-linked cryptoasset theft. In October 2026, approximately £4.5 billion (c. US$6 billion) in cryptoassets were stolen from the world's largest cryptoasset exchange by trading volume, making it the largest reported cryptoasset theft to date. Early assessments by blockchain

[58] MSMT, 'DPRK's Violation and Evasion of UN Sanctions', 31.

analytics companies indicate that the theft was likely conducted by DPRK-linked actors.

3.42 Large-scale thefts are typically followed by rapid laundering through networks of North Korean nationals operating outside the DPRK, with foreign-based facilitators and high-risk Over The Counter (OTC) desks in third jurisdictions, particularly in Russia and China, converting stolen cryptoassets into fiat currency to support procurement and fund the DPRK's unlawful WMD and ballistic missile programmes. Analysis by TRM Labs[59] has highlighted the growing role of Chinese-language escrow services and underground banking networks as key components of the global illicit crypto ecosystem, providing financial services infrastructure that may be exploited to launder stolen assets and move value across jurisdictions.

3.43 Stolen assets may also be routed through multiple exchanges, wallets and services in an effort to obscure their origin, creating opportunities for regulated firms to unknowingly process proceeds linked to DPRK cyber activity.

3.44 Alongside external cyber intrusions, employing DPRK IT workers creates insider-cryptoasset theft risks through their access to company systems and digital infrastructure, while also generating revenue for the DPRK regime (see para 3.30).

3.45 As the scale and sophistication of cryptoasset-related illicit use and theft continues to evolve, UK cryptoasset firms are assessed to face an elevated risk not only as potential targets of cyber-enabled theft, but also as facilitators of the laundering or transfer of stolen cryptoassets. This creates associated money laundering, sanctions and PF risks where illicit funds pass through UK firms as part of complex laundering chains.

Illicit use of artificial intelligence

3.46 Artificial intelligence (AI) enables systems to analyse data, identify patterns, and perform tasks that typically require human judgement or decision-making, improving efficiency, accuracy, and the ability to process large volumes of information at scale.

3.47 Advancements in AI are increasing the tools available to sanctions evasion and PF actors, allowing them to increase both the scale and complexity of their illicit activity.

3.48 The NCA's[60] National Strategic Assessment 2026 identifies AI as a significant enabler of serious and organised crime, noting that increasingly accessible AI tools are lowering barriers to entry and supporting criminal activity, including fraud, cybercrime and money laundering.

---

[59] TRM Labs, 'Crypto Crime Report'.

[60] National Crime Agency, 'National Strategic Assessment 2026 of Serious and Organised Crime', https://www.nationalcrimeagency.gov.uk/nsa-overview-of-soc-2026/nsa-summary-2026.

3.49 For proliferators, AI could be used in a variety of ways to reduce the likelihood of detection and allow PF networks to operate with greater agility against existing systems and controls.

3.50 The Royal United Services Institute (RUSI) highlights that the firms should take steps to mitigate the use of AI by upgrading Know Your Customer (KYC) procedures to account for deepfake capabilities, deploying defensive AI to audit trade documents for inconsistencies, and adopting dynamic compliance modelling using behaviour-based analytics.[61] Regulated firms adopting AI should ensure they adhere to their regulatory requirements whilst doing so.

[61] Royal United Services Institute, 'Algorithms of Evasion: The Rise of AI-Enabled Proliferation Financing', 26 May 2026, https://www.rusi.org/explore-our-research/publications/research-papers/algorithms-evasion-rise-ai-enabled-proliferation-financing.

Chapter 4

UK Sectoral Vulnerabilities

4.1 The UK's status as a leading global centre for financial services, trade and professional activity creates inherent structural exposure to the PF threats and typologies set out in chapter 3, requiring regulated firms to take proportionate steps to identify, assess and mitigate that risk.

4.2 This chapter highlights the sectors and activities assessed as having higher PF vulnerability.

4.3 PF vulnerabilities are not distributed uniformly across the UK economy and for most organisations this exposure is more likely to occur indirectly through commercial relationships that may be exploited by proliferators.

4.4 Since the last Assessment, firms employing remote IT workers, directly or through third party arrangements, have been identified as a cross-cutting typology potentially relevant to firms across all sectors. Further information on how this typology operates, including a case study, is provided from paragraph 3.30, with relevant vulnerabilities and mitigations set out later in this chapter.

4.5 Beyond this, regulated firms in sectors not listed below, which may have lower exposure to PF vulnerabilities, should continue to follow the requirements in the MLRs as lower exposure does not mean no exposure. The evolving threats outlined in Chapter 3 show the importance of understanding how PF risk can manifest through seemingly legitimate economic activity linked to the UK.

4.6 For example, although Estate Agency Businesses (EABs) and Letting Agency Businesses (LABs) are assessed as presenting a low PF risk, with no significant PF activity identified at the time of this Assessment, they still may have interactions with higher risk activity. This includes cases of Iranian ownership of UK property and one DPRK-linked diplomatic property. These examples highlight the potential for PF-related sanctions risks to arise, even for sectors assessed as low risk. Organisations, irrespective of sector, should consider carefully the risks associated with any property transactions and the ultimate beneficial owners involved.

4.7 The chapter covers the following areas in relation to its PF vulnerability:

i. Key UK Financial and Non-Financial Sectors:
    a. Banking and Payment Services
    b. Trade Finance
    c. Insurance (Maritime and Cargo)
    d. Money Service Businesses (MSBs)
    e. Trust and Company Service Providers (TCSPs)
    f. Legal
    g. Cryptoasset firms
ii. UK firms employing remote IT workers
iii. The Maritime and Shipping Industries
iv. Manufacturing of proliferation or dual-use goods
v. The higher education sector
vi. Inadequate business-wide PF risk assessments

The UK's financial and non-financial sectors

4.8 The scale and global connectivity of the UK's financial system mean it remains exposed to exploitation by proliferators seeking access to financial services and technologies. This exposure is often indirect, with activity routed through complex international networks of intermediaries, front companies and third-country jurisdictions, in some instances facilitated by professional services enablers.

4.9 Risk is not distributed evenly across sectors. Regulated firms with significant international operations and exposure to higher-risk jurisdictions may face greater exposure to proliferation financing typologies than firms whose activities are primarily domestic in nature.

Banking and payment services

4.10 Consistent with the 2021 Assessment, banking and payment services are vulnerable to PF risk. Proliferators embed transactions within legitimate-appearing financial flows, using layered financial transactions, correspondent banking relationships and third-country intermediaries to obscure the origin, purpose and beneficiary of funds. Financial institutions and payment service providers face the risk of processing payments that appear commercially routine but ultimately support proliferation activity.

Case study 5 – Attempted transfer of funds between three designated entities via dormant account

- In September 2025, the UK Government designated numerous Iranian entities under the Iran (nuclear) sanctions regime, including through the reinstatement of UN sanctions on Iran under the 'snapback' mechanism in line with EU partners (see 2.19 for further detail). These designations include an Iranian financial services company (Entity X) and a separate Iranian bank (Entity Y). Entity X had a dormant bank account with a UK bank.
- Entity X submits a request to the UK bank to transfer a six-figure sum from its dormant account to Entity Y. No purpose is given for the transfer. The timing of the transfer, immediately after the designations of Entity Y and Entity X, raises the possibility that this is an attempt to move frozen funds out of the UK before the UK bank implements compliance controls to prevent breaches of UK financial sanctions. Aware of its obligations under UK sanctions legislation, the UK bank blocks the transaction and reports to OFSI. Had it been processed, the transaction could have constituted a breach of UK financial sanctions, which prohibit dealing with funds belonging to or controlled by a designated person, and making funds available directly or indirectly to or for the benefit of a designated person.
- **This case study illustrates two risks specific to UK financial sanctions on Iran. The 'snapback' of UN sanctions and fresh designations by the UK Government in September 2025 led to numerous Iranian individuals and entities being captured by UK sanctions, including some for the first time. The period immediately following designations presents a high risk for Designated Persons (DPs) attempting to exploit compliance vulnerabilities and move UK-based funds and assets beyond the reach of UK asset freezing prohibitions. Second, long-dormant accounts held for entities that become designated remain live sanctions risks. The absence of prior activity provides no indication of future intent and sufficient sanctions controls should be in place for all accounts held by designated entities regardless of their activity history.**

Trade finance

4.11 Trade finance services are exposed where they facilitate cross-border trade involving complex supply chains and multiple intermediaries. Proliferators exploit trade ecosystems by combining front companies, brokers and opaque corporate structures to create a credible commercial cover for illicit procurement activity.

4.12 In this context, overseas transactions involving layered ownership structures, offshore vehicles and indirect counterparties can make it challenging to identify the ultimate source or recipient of funds, the true nature of the underlying trade, or the end-use of goods and services. This creates conditions in which PF can be integrated into otherwise legitimate trade finance activity.

4.13 Intangible transfers of controlled technology or software present a particular challenge for enforcement as there are no physical goods presented at the border.

Insurance (maritime and cargo)

4.14 London is a major market for insurance related to the shipping trade, including hull and machinery insurance, cargo insurance and liability insurance. The UK's market dominance is most noticeable in protection and indemnity (P&I) insurance, where the UK hosts the International Group of P&I Clubs. These clubs collectively provide P&I for around 90% of the world's shipping.[62]

4.15 Insurers involved in the shipping trade face unique risks of facilitating PF. UK-insured or re-insured third-country vessels and containers can be directly involved in the trade of dual-use or otherwise restricted goods, or engage in other forms of prohibited trade. The primary risk to the insurance sector is that the insurance of vessels, persons, companies and cargo plays a part in providing an image of credibility to the proliferators, enabling access to fuel, ports and port services which proliferators would otherwise not have access to.

4.16 It is often difficult for insurers to actively investigate shipments due to the practicalities of the shipping trade, and insurers may be reliant on information provided by the customer to assess PF risk. Re-insurance, which can involve a UK-based insurer re-insuring a third country-based insurer, can heighten vulnerabilities, as the UK-based re-insurers are a further step removed from the customer, and are reliant to a significant extent on the initial insurer to ensure that appropriate due diligence has been completed.

4.17 In the context of P&I Clubs specifically, liabilities are indemnified post-event, and while clubs scrutinise claims and underlying activity before reimbursement, rather than relying solely on upfront underwriting diligence, there are practical challenges in assessing

---

[62] International Group of P&I Clubs, 'About the Group', 1 December 2015, https://www.igpandi.org/article/about-the-group/.

claims in real time. This is particularly acute where payments may be time-critical (for example, to release vessels or meet third-party liabilities). This can constrain the extent of checks that can be undertaken before funds flow, meaning controls are partly reliant on pre-existing due diligence and post-event verification.

4.18 Some specific mitigations include:

- **Layered due diligence across the value chain (where relevant).** In commercial placements, there are typically multiple parties undertaking due diligence, including brokers, coverholders and the initial underwriter before risk is accepted. In P&I contexts, while broker involvement may vary, there are still controls at membership onboarding and ongoing monitoring, creating sequential points at which risk can be assessed. While this does not remove risk, it does create sequential control points, particularly in well-regulated London Market placements.
- **Contractual and policy-based mitigants.** Across both models, firms rely on sanctions clauses, exclusions and warranties, enabling them to decline claims, terminate cover or withhold payment where prohibited activity is identified. P&I clubs in particular operate under club rules and circulars that provide a clear basis for refusing claims linked to sanctioned or prohibited activity.
- **Reinsurance considerations.** For reinsurers, although they are further removed from the underlying insured, they can typically rely on cedant due diligence, contractual protections, and portfolio-level risk assessment to support their assessments.

Money Service Businesses (MSBs)

Money Service Businesses (MSBs) remain vulnerable to PF exploitation due to their ability to facilitate rapid cross-border movement of funds, often involving higher-risk jurisdictions, overseas agents, correspondents & branches. The sector may be attractive to proliferation actors seeking to move funds associated with procurement networks, sanctions evasion, front companies or intermediaries supporting, amongst others, Iranian proliferation activity. The vulnerability is primarily linked to the nature of the services provided rather than evidence of widespread sector involvement in PF.

Key MSB PF vulnerabilities include:

- Cross-border fund transfers involving jurisdictions associated with sanctions evasion.
- The use of intermediaries to obscure the ultimate originator or beneficiary of funds.
- Informal value transfer arrangements and remittance corridors which may bypass formal banking channels and associated sanctions controls.

- Overseas branches and agent networks operating in jurisdictions with weaker AML/CTF and sanctions frameworks.
- The potential use of front or shell companies to move funds linked to procurement networks whilst disguising the true purpose or beneficiary of transactions.
- Transactions involving complex ownership structures or customers with links to jurisdictions assessed as presenting elevated sanctions evasion and proliferation financing risks.

Trust and Company Service Providers (TCSPs)

4.19 The relative ease of establishing corporate entities in the UK can be exploited by proliferators seeking to create front or shell companies to facilitate procurement and financial activity. This remains a risk, despite Companies House reforms.

4.20 The use of nominee directors or shareholders, as well as the acquisition of pre-formed (off-the-shelf) companies, indirectly from UK TCSPs through intermediaries can further obscure beneficial ownership and control. For example, a professional in the UK or overseas, may ask a UK TCSP to form numerous UK companies or partnerships for them. They may have a customer in mind, or they may keep these as "stock" for onward sale to customers at a later date – to be bought subsequently by someone aiming to obscure PF activity through a complex structure of companies from many jurisdictions.

4.21 These features can enable proliferators to distance themselves from transactions and disguise ownership, making it more difficult to identify links to sanctioned entities or proliferation-related activity. Since the 2021 Assessment, reforms to Companies House and changes to bring the sale of pre-formed (shelf) firms into the scope of the MLRs have supported strengthened corporate transparency, although vulnerabilities including, but not exclusive to, PF risk assessments done by TCSPs remain.

Legal and accounting

4.22 Similarly to TCSPs, the legal and accounting sectors are vulnerable to PF risk. Legal services could be targeted by PF actors to create legitimate-looking ownership structures, front companies, shell companies, or nominees to hide the identities of those procuring dual-use goods. Accountancy services can similarly facilitate TCSP services, payroll services and the setting up of companies. Companies House reforms and MLR changes since the 2021 Assessment, have strengthened corporate transparency and reduced the risk associated with the misuse of UK corporate structures, although vulnerabilities remain.

Mitigations for all financial and non-financial firms

4.23 This chapter has highlighted financial and non-financial sectors at heightened vulnerability to PF risk.

4.24 Accordingly, all regulated firms should ensure that they meaningfully assess and manage PF risk tailored to their business model, customer base and geographic exposure. Regulated firms should refer to and make use of financial-crime-related guidance and resources issued by their regulatory bodies, applying it accordingly to their business activities.

4.25 Supervisors have provided specific guidance and feedback to help firms strengthen their controls.

4.26 Examples include the FCA's *Sanctions Systems and Controls: our findings*[63] which highlights common weaknesses and examples of good practice relating to governance, customer due diligence, sanctions screening, transaction monitoring, escalation processes and sanctions risk assessments.

4.27 Professional Bodies Supervisors have also published guidance to help legal professionals understand and comply with UK sanctions obligations, such as guidance by the Solicitors Regulation Authority.[64]

4.28 Regulated firms should have regard to relevant supervisory guidance and ensure that their sanctions and wider financial crime controls remain proportionate to their PF risk exposure.

4.29 Regulated firms should develop robust business-wide risk assessments that clearly identify how PF risks arise. These should use clear methodologies and go beyond high-level references, as incomplete assessments limit the effectiveness of wider controls.

4.30 Regulated firms should ensure that risk assessments consider both inherent risks and the effectiveness of existing controls. Assessments should draw on a range of qualitative and quantitative information and clearly document how PF risks are identified, assessed and managed.

4.31 Regulated firms should regularly review and update their risk assessments to reflect evolving PF threats and typologies. Clear methodologies, defined mitigating actions, and strong governance and senior management oversight are critical to ensuring controls remain effective in practice.

4.32 Regulated firms that outsource financial crime activities should ensure that providers incorporate PF risk into their assessments and checks, and that associated operational risks are managed.

4.33 Where regulated firms (or third parties that regulated firms outsource to) employ AI as part of their approach to PF risk, they should ensure adequate oversight and controls are in place for safe, compliant and effective use, including of open-source software. This means firms

---

[63] Financial Conduct Authority, 'Sanctions systems and controls in our firms: our findings', 28 May 2026, https://www.fca.org.uk/publications/good-and-poor-practice/sanctions-systems-and-controls-our-firms-our-findings.

[64] Solicitors Regulation Authority, 'Guidance: Complying with the UK Sanctions Regime', updated 19 June 2026, https://www.sra.org.uk/solicitors/guidance/financial-sanctions-regime/.

should have the capabilities to identify, monitor, and manage external applications, libraries, and services integrated into their networks. Firms should be prepared to address and remediate vulnerabilities identified by third parties at scale.[65] Firms may wish to refer to the FCA's 2024 AI update, and the FCA will be publishing examples of good and poor practice in relation to firm adoption of AI later this year.[66]

Cryptoasset firms

4.34 Firms engaged in cryptoasset-based activities face a distinct set of vulnerabilities that increase their exposure to PF risk beyond those listed for financial and non-financial firms above.

4.35 The borderless and pseudonymous nature of cryptoassets, combined with evolving technologies and typologies, such as privacy coins and mixers, can limit firms' visibility over counterparties, transaction flows and ultimate beneficiaries.

4.36 Sanctioned actors employ a range of obfuscation techniques to mask the ownership and destination of cryptoassets. These may include the use of privacy-enhancing technologies such as mixers, followed by cross-chain swaps to transfer value across blockchains. Cryptoassets may then be routed through blockchains which benefit from liquidity through OTC brokers and exchange hubs in China, Russia and other jurisdictions with weaker AML/CTF controls. This has enabled the laundering of billions of pounds worth of cryptoassets for use in proliferation financing.

4.37 Such activity obscures the link between UK-facing firms and sanctioned actors, increasing the risk that UK-based crypto firms are exposed to sanctions risk, including PF risk.

4.38 Risks increase where UK firms process transactions involving foreign exchanges or other service providers linked to Russia, Iran, China, or other enabling countries subject to weaker implementation of AML/CTF rules. FATF's June 2025 Targeted Update found that significant gaps remain across jurisdictions in the regulation and supervision of the sector, creating opportunities for illicit actors to exploit regulatory arbitrage and move assets through jurisdictions with weaker controls.[67]

---

[65] Financial Conduct Authority, Bank of England and HM Treasury, 'Joint statement on frontier AI models and cyber resilience, 15 May 2026, https://www.fca.org.uk/news/statements/fca-boe-treasury-joint-statement-frontier-ai-models-cyber-resilience.

[66] Financial Conduct Authority, 'AI Update', 22 April 2024, https://www.fca.org.uk/publication/corporate/ai-update.pdf.

[67] Financial Action Task Force, 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers', June 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

4.39 UK cryptoasset firms may be vulnerable to enabling PF related sanctions evasion where customer due diligence, financial sanctions screening and transaction monitoring frameworks are insufficient.

4.40 As discussed in Chapter 3, cryptoasset firms are attractive targets for cyber-enabled theft. UK-based exchanges and DeFi projects have been targeted by state-linked cyber actors, with stolen assets subsequently laundered through facilitators in Russia and China. Such incidents directly contribute to proliferation financing and expose firms to significant financial losses.

Mitigations for cryptoasset firms

4.41 In addition to the mitigations set out under Financial and Non-Financial Sectors above, cryptoasset firms and protocols should prioritise strengthening security practices to effectively mitigate the threat posed by PF actors, such as DPRK-linked hacking groups, as well as taking steps to mitigate the risk of facilitating transactions with sanctioned entities and persons.

4.42 Cryptoasset firms should refer to **OFSI's Cryptoasset Threat Assessment** for further PF-relevant typologies and indicators linked to cryptoasset misuse.[68]

4.43 The FCA intends to provide further guidance for cryptoasset firms as part of FCA Financial Crime Guide.[69]

UK firms employing remote IT workers

4.44 As per **OFSI's Advisory on North Korean IT workers**[70], UK firms in technology-enabled sectors are exposed—particularly where recruitment relies on online recruitment platforms, remote hiring models, including through third-party facilitators that enable DPRK IT workers to operate undetected. UK exposure is driven by the depth of the digital services ecosystem and reduced employer visibility over worker identity, location and payment flows.

4.45 DPRK IT workers use online freelance platforms, and masking tools such as VPNs, proxy servers and remote desktop software to conceal their true location.

4.46 The remote employment of DPRK IT workers exposes UK firms to PF-related sanctions risks, as salaries or other economic resources may ultimately benefit the DPRK regime. It also creates operational and information security risks, as workers may gain trusted access to systems, codebases, and sensitive data.

---

[68] OFSI, 'Sanctions Compliance in the Cryptoassets Sector'.

[69] FCA, 'Financial Crime Guide'.

[70] OFSI, 'Advisory on North Korean IT Workers'.

Mitigations for firms employing remote IT workers

4.47 Firms should familiarise themselves with OFSI guidance on DPRK IT workers, including common typologies, methods of approach and associated red flags.[71] Firms should ensure that relevant staff, particularly those involved in recruitment, onboarding and compliance functions, are aware of these risks and able to identify indicators of potential DPRK-linked activity.

4.48 Firms should implement robust controls over recruitment and employment practices, particularly where remote hiring or third-party providers are used. This includes conducting appropriate due diligence on outsourced providers, verifying worker identity and location, and ensuring transparency over employment arrangements and payment flows. Firms should maintain effective oversight of third-party hiring practices, regularly reviewing performance and practices. Critical systems and data should be configured to prevent unauthorised access, including through appropriate access controls and the use of multi-factor authentication (MFA), particularly where sensitive or confidential information may be accessed remotely. Regulated firms should also have regard to relevant guidance and requirements issued by their supervisors and regulatory bodies. Weak controls may enable DPRK-linked workers to be employed, creating exposure to sanctions breaches and proliferation financing risks.

The maritime and shipping industries

4.49 The UK's maritime and shipping industries are inherently vulnerable to PF risk, as they engage in the trade of dual-use and otherwise controlled goods, and maintain international contacts. The nature of the UK's geography means that around 95% of the UK exports are delivered via sea.[72]

4.50 Strategic export controls (listed at Chapter 2.17-20) focus on what is controlled: i.e. what is being exported, who will use it and for what purpose. However, those involved in the maritime and shipping industries should also consider the roles played by other parties, including those indirectly involved and what they are doing. Those involved in exporting goods are vulnerable to more indirect forms of PF, as these often do not fit within international export controls.

4.51 Intangible transfers of controlled technology or software also present a particular challenge for enforcement as there are no physical goods being presented at the border.

---

[71] Ibid.

[72] Department for Transport, 'UK Port Freight Statistics: 2019', 12 August 2020, https://assets.publishing.service.gov.uk/media/5f32adc4e90e0732df4dd20d/port-freight-statistics-2019.pdf.

Mitigations for maritime and shipping

4.52 To mitigate against these risks, firms involved in the maritime and shipping sectors should focus on undertaking robust due diligence on customers, vessels, and intermediaries to identify potential links to sanctioned actors. Firms should verify the consistency and plausibility of shipping documentation and underlying commercial activity, as falsified documents or transactions lacking a credible economic rationale can indicate PF risk.

4.53 More broadly, firms should consider the full supply chain and indirect participants in shipping and trade activity, recognising that PF often exploits complex networks rather than direct transactions, and ensure that controls are aligned with known typologies and emerging risks.

Manufacturing of proliferation or dual-use goods

4.54 The UK's role as a major arms manufacturer and producer of dual-use goods makes it an attractive target for proliferators. Firms across UK industrial sectors continue to face procurement risk, as recent cases involving Russia, Iran and DPRK demonstrate how controlled or dual-use components can be acquired. Evidence from the conflict in Ukraine shows that North Korean KN-23/KN-24 short-range ballistic missiles—supplied to and used by Russia—have contained a significant proportion of UK and other Western-manufactured components for guidance, control, and propulsion systems.

Mitigations for manufacturing

4.55 Manufacturing firms, distributors and other intermediaries involved in the sale of goods proliferation or dual-use goods should develop an understanding of how PF risks may arise for their products, customers and supply chains to support more effective risk-based controls and reduces the likelihood of inadvertent involvement in proliferation-related activity.

The higher education sector

4.56 Academia remains vulnerable to proliferators. As discussed in the 2021 PF NRA, the UK's world-leading research base, international collaboration and access to advanced scientific expertise can be targeted by proliferators seeking sensitive knowledge, skills and dual-use research, particularly in STEM and emerging technology fields.

4.57 This risk remains. The Intelligence and Security Committee's 2025 report on Iran includes details on the targeting of university students and the acquisition of nuclear-relevant know-how, demonstrating how academic research and knowledge transfer can be targeted to support

proliferation objectives.[73] This risk can arise through students, researchers, visiting academics and collaborative research activity. It may also arise through cyber-enabled activity, including the targeting of university systems, research data, intellectual property and sensitive academic partnerships by hostile states and associated networks seeking to support proliferation objectives.

Mitigations for the higher education sector

4.58 Universities and research institutions should apply a risk-based approach to protecting sensitive research and international engagement. Institutions should refer to the National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC) Trusted Research guidance[74], which supports the identification of sensitive research, due diligence on international partners, and the protection of intellectual property, data and expertise from misuse or exploitation. Institutions should also consider, where relevant, a range of applicable legal, regulatory and advisory mechanisms, including but not limited to the National Security and Investment (NSI) regime, which provides powers to scrutinise and, where necessary, intervene in acquisitions and investments that may give rise to national security risks, or the Export Control Act 2002, which applies to both physical exports and intangible transfers (e.g. sharing software or technical know-how with overseas collaborators).

4.59 Institutions should also ensure adherence with the FCDO's Academic Technology Approval Scheme (ATAS)[75]. ATAS requires prior approval for certain overseas students and researchers in sensitive subject areas, helping prevent the transfer of knowledge that could contribute to weapons of mass destruction or advanced military programmes.

4.60 In addition, institutions can engage with the Department for Business, Innovation, Science and Trade's (BIST) Research Collaboration Advice Team (RCAT)[76]. RCAT provides a dedicated source of government advice on national security risks in international research collaborations, supporting universities to understand relevant legal and regulatory requirements, assess partners and projects, and strengthen research security governance and risk management frameworks.

---

[73] Intelligence and Security Committee of Parliament, 'Iran'.

[74] National Protective Security Authority, 'Trusted Research Guidance for Academia', 18 July 2025, https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia.

[75] Foreign, Commonwealth and Development Office, 'Academic Technology Approval Scheme (ATAS)', 24 March 2026, https://www.gov.uk/guidance/academic-technology-approval-scheme.

[76] Research Collaboration Advice Team, Homepage, https://www.gov.uk/government/organisations/research-collaboration-advice-team.

Business-wide risk assessments

4.61 As discussed in the mitigations section, firms' ability to identify and mitigate PF risk is weakened where business-wide PF risk assessments are absent, incomplete, or lack sufficient depth. While the MLRs require regulated firms and individuals to identify and assess money laundering, terrorist financing and PF risks, in practice there can be variations in how comprehensively these assessments are developed and documented across firms.

4.62 Recent FCA supervisory work on firms' risk assessment processes and controls has identified shortcomings in governance, methodology, documentation and the assessment of financial crime risks, while also highlighting examples of good practice. The FCA has reinforced expectations that firms adopt robust, evidence-based risk assessment methodologies, maintain clear documentation and ensure sufficient granularity in identifying, assessing and mitigating risks, including proliferation financing.[77]

4.63 Supervisory activity is complemented by ongoing engagement with industry, guidance and communications designed to improve firms' understanding of PF risk and how it should be assessed within broader financial crime frameworks. This includes reinforcing expectations that firms consider PF risk across customers, products, services, delivery channels and geographic exposure, and that assessments are kept under regular review.

4.64 This National Risk Assessment is intended to support regulated firms in meeting these obligations by providing a consolidated, national-level view of PF threats, typologies and vulnerabilities relevant to the UK. Regulated firms should use this Assessment, alongside supervisory communications and guidance, to inform and strengthen their own risk assessments and ensure that controls are proportionate to their exposure.

[77] Financial Conduct Authority, 'Risk assessment processes and controls in firms: our findings', 11 November 2025, https://www.fca.org.uk/publications/good-and-poor-practice/risk-assessment-processes-and-controls-firms-our-findings

Chapter 5
Conclusions

The UK maintains a strong regulatory framework to combat proliferation finance

5.1 The UK maintains a robust and comprehensive framework for countering proliferation financing. Since the 2021 Assessment, this framework has been strengthened through regulatory reforms and expanded operational capabilities. Regulatory reforms include enhanced requirements under the MLRs, including for regulated firms to identify and assess PF risk, and reforms to Companies House to improve corporate transparency and reduce the risk of misuse of UK entities. Operationally, the growth of enforcement bodies including OFSI, OTSI and Companies House, has strengthened the UK's ability to detect and disrupt PF activity.

5.2 Together, these measures provide a strong foundation for countering PF activity.

Proliferation financing typologies continue to change and become more complex

5.3 PF threats have continued to evolve in scale and sophistication. Typologies increasingly involve complex, multi-layered structures involving multiple different typologies, including the use of intermediaries, front companies, deceptive shipping practices and cryptoassets. The PF landscape has also changed significantly since 2021. Russia's deepening political, military and economic ties with both DPRK and Iran, the re-imposition of UN nuclear-related sanctions on Iran, and the increasing use of cryptoassets by proliferators have created new challenges for firms and authorities. At the same time, PF activity increasingly overlaps with other forms of illicit finance, including sanctions evasion, money laundering, fraud and cyber-enabled crime. This growing complexity makes PF more difficult to detect and reinforces the need for continuous monitoring and an up-to-date awareness of potential risks to firms, and the ongoing development of systems and controls by firms, supervisors and authorities to identify, prevent and disrupt PF activity.

5.4 In addition, new typologies have emerged. The role of DPRK IT workers and typologies involving cryptoassets have increased risks since 2021, and the use of AI is likely to change the landscape further. Firms should be aware of how these evolving threats may manifest within their business models and ensure they are appropriately reflected in firm-level PF risk assessments.

The UK's vulnerabilities remain in its position as a global financial and trade centre

5.5 The UK's role as a major international financial and maritime hub creates inherent exposure to PF risk, and this has remained broadly consistent from 2021 to 2026. The scale and openness of the UK economy, and extensive cross-border financial flows and global trade links, provide opportunities for actors to embed PF activity within legitimate-appearing transactions. Sectors most exposed to PF risk continue to include banking and payment services, trade finance, cryptoasset firms and services, and maritime-related services, including insurance. UK firms may be exposed even without direct connections to proliferating states.

To help combat PF, firms should ensure that risk assessments are completed to a high standard

5.6 Effective mitigation of PF risk depends on firms undertaking high-quality, proportionate risk assessments. Increased awareness of PF typologies is critical to identify existing and emerging threats. Firms should clearly understand how PF risk arises across their customers, products, services and geographies, and apply robust due diligence, sanctions screening and monitoring accordingly.

5.7 Given the increasing complexity of PF typologies and their overlap with wider illicit finance threats, firms should not rely solely on sanctions screening to identify PF risk. This is particularly important given the increasing use of intermediaries, complex ownership structures, alternative payment methods and deceptive trade practices to conceal links to sanctioned actors.

5.8 Effective mitigation requires a broader risk-based approach, combining sanctions controls with customer due diligence, ongoing monitoring, transaction analysis and an understanding of relevant PF typologies and red flags. Where suspicious activity, potential sanctions breaches or indicators of PF are identified, firms should conduct appropriate investigations and make reports to OFSI and the relevant supervisor (where required).

Glossary

AI	Artificial Intelligence
AML/CTF	Anti-Money Laundering and Counter-Terrorist Financing
ATAS	Academic Technology Approval Scheme
BIST	Department for Business, Innovation, Science and Trade
CPACC	Counter Proliferation and Arms Control Centre
CPF	Counter Proliferation Financing
DBT	Department for Business and Trade
DESNZ	Department for Energy Security and Net Zero
DPRK	Democratic People's Republic of Korea
ECCTA	Economic Crime and Corporate Transparency Act 2023
EMI	Electronic Money Institution
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth and Development Office
HMRC	HM Revenue & Customs
HMT	HM Treasury
IVTS	Informal Value Transfer System
JCPOA	Joint Comprehensive Plan of Action
MLRs	Money Laundering Regulations
MOD	Ministry of Defence
MSB	Money Service Business
MSMT	Multilateral Sanctions Monitoring Team
NCA	National Crime Agency
NRA	National Risk Assessment
NSS	National Security Strategy
OFSI	Office of Financial Sanctions Implementation
OTSI	Office of Trade Sanctions Implementation
P&I	Protection and Indemnity
PF	Proliferation Financing
RCAT	Research Collaboration Advice Team
RUSI	Royal United Services Institute
SAMLA	Sanctions and Anti-Money Laundering Act 2018
STEM	Science, Technology, Engineering and Mathematics
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
UNICRI	United Nations Interregional Crime and Justice Research Institute

UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction

HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gov.uk