UK Finance

Countering Proliferation Finance: A Financial Sector Perspective

March | 2025

Introduction

UK Finance is the collective voice for the banking and finance industry, representative of over 300 Financial Institutions. We act to enhance competitiveness, support customers and facilitate innovation. We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. Our operational activity enhances members' own services in situations where collective industry action adds value.

This paper is the product of the collective work of the UK Finance Proliferation Finance (PF) Working Group, established in November 2022.

This paper highlights the:

1) Key regulatory framework relating to PF;
2) Steps taken to assess PF risks with relevant risk factors;
3) Approaches to mitigate and manage the risks via bank control frameworks; and
4) Challenges and recommendations on improving the effectiveness of counter-PF measures.

PF is not a new topic but the adoption of PF as a risk factor by the Financial Action Task Force (FATF), and the forthcoming inclusion of PF in mutual assessments, has resulted in a heightened focus amongst Financial Institutions (FIs). The Executive Summary pinpoints the key areas identified where challenges are being faced and improvements can be made. Essential to improving our response on PF will be dialogue with the public sector and other relevant parties, requiring a coalition of effort. The current level of dialogue on PF is underdeveloped in comparison to that seen in counter-terrorism, illicit wildlife trade and human trafficking.

Enhancing our collective approach on public-private information sharing with greater thought about who needs to be involved, from both the public and private sectors is essential. Beyond financing or the processing of payments there are other private sector actors (including, but not limited to, shipping lines and airlines, freight forwarders, couriers, insurers, manufacturers and traders in dual use items) who are relevant to the conversation on how we can collectively address the risks posed by PF. The increased focus by sanctions authorities on the supply of goods to Russia's military provides an opportunity to enhance our approach since many of the challenges around identification of such illicit trade are shared with PF.

This document reflects the informed views of UK Finance Limited ("UK Finance") and is aimed to inform readers on the practical implications of countering proliferation finance as of June 2024.

Executive Summary

Recent developments of international standards, particularly at FATF, on PF have triggered a heightened focus on PF threats and vulnerabilities. United Nations Security Council Resolutions (UNSCRs) relating to the nuclear and missile programmes of Iran and the Democratic People's Republic of Korea (DPRK/North Korea), and more generally on any WMD proliferation to non-state actors, lie at the core of countering PF. However, there is a lack of consensus on the extent to which FIs' obligations to assess and manage PF risk extends beyond implementing UNSCR measures and relevant autonomous regulations. The inconsistent scope and definition of PF creates significant challenges with global risk management framework for the financial sector, particularly for international banks when trying to comply with laws and regulations set by multiple jurisdictions.

FIs must assess their PF risk, considering the size and nature of their business. They do not necessarily require a stand-alone, dedicated risk assessment framework to assess their PF risk, provided that the factors relating specifically to PF are assessed. These risk factors are categorised as relating to customers, countries or geographic areas, products or services, transactions, and delivery channels. As well as using these risk factors in assessing PF risk Enterprise-wide/Business-wide, they may also be used in models that assess risk at country, product and customer level. In the UK, FIs are required to take a risk-based approach to managing PF risks.[1] However this is in combination with a strict liability sanctions regime which overlaps when involving PF related sanctions designations.

Customer risk factors relevant to assessing PF risk include a range of industries that produce, trade, move or finance proliferation-sensitive goods and technologies (e.g., the defence and nuclear industries). These may be more vulnerable than other sectors to exploitation by proliferators, often without any complicity on the part of the customer. Industry codes relating to these sectors can be helpful in assessing PF risk, although additional engagement with customers will often be required to understand the risk at a customer level.

Country or geographical risk exposure comes in several forms:

- Countries with proliferation concerns, particularly those with active WMD programmes;
- Countries which are the source of items required by proliferators, such as those with key manufacturing sectors or which are the sources of raw materials;
- Countries that assist proliferating countries to raise the funds to support their WMD programmes, such as by buying sanctioned exports or hosting overseas workers;
- Locations noted for the transhipment of physical items that are moved in association with WMD proliferation, including 'gateway' countries and maritime zones used for ship-to-ship transfers; and
- A broad category of enabling geographies, which include jurisdictions used to register, bank or operate shell companies or where shipping registration requirements are less stringent.

[1] This is a requirement under Reg 19A of the UK MLRs.

Noting the lack of international consensus regarding which states are of proliferation concern, there is even less agreement on the other forms of geographic exposure.

Product and service risk factors for PF are very similar to those for Money Laundering (ML) and Terrorist Financing (TF). Key product risk assessment characteristics are:

- Cross-border nature;
- Limited self-disclosure requirements, where proliferators may exploit jurisdictional differences in disclosure requirements;
- Complexity, especially where this makes it easier to obfuscate beneficial ownership or interpose third parties between the proliferator and the FI; and
- Technologies used, especially where there is less mature regulatory oversight of a new technology e.g., virtual currencies.

Transactional risk factors and delivery channel risk factors for PF are broadly similar to those for other Financial Crime (FC) types. Shell company risk and Digital Assets and Currencies (DACs)/cryptocurrency-related risks are cross-cutting themes that impact across several of the above risk categories.

Identifying typologies indicative of PF is key to distinguishing between illicit activity and legitimate business. Typologies can guide FIs in optimising their control framework. Calibration and leveraging of existing FC processes and controls can be used to address PF risks. These need to be articulated so that existing controls are properly leveraged, and any additional controls required avoid duplication.

In defining the Customer Due Diligence (CDD) or Know Your Customer (KYC) measures required both at onboarding and ongoing due diligence, FIs may utilise the outcome of their PF risk assessment. For Retail customers, CDD or KYC is typically captured without any specific PF questions being asked, beyond any sanctions exposures to Iran and DPRK. CDD/KYC for customers within trade finance or commercial business banking will look to understand the customer's expected business and transaction activity. This could include consideration of the countries involved, including supply chain or downstream exposure via key counterparties and their locations. FIs may use industry codes to help risk rate customers, which can prompt sets of PF related questions such as the exact technology or equipment the customers produce or distribute and what trading countries an FI might expect to see. Identifying customers trading in dual-use goods, beyond customer declarations, would require some expertise or knowledge of such items. The United States (US) Department of Commerce's Bureau of Industry and Security (BIS) Entity List may, if examined on a listing-by-listing basis, indicate whether a particular actor has been added to the list for a proliferation related concern.

Where proportionate under the risk-based approach, FIs may consider implementing targeted measures within their investigations and screening controls, such as:

- Intelligence gathering following sanctions designations by reviewing historical transactions where a true match has been identified. Applying a risk-based approach, FIs may use retrospective analysis or proactive 'look-back' investigations to identify designated individuals and entities trading and/or transacting prior to being sanctioned. Such investigations allow the FI to identify non designated counterparties who may be exposed to PF related activity.
- Enabling internal investigations to be tagged to a PF concern. Internal investigations carried out by FIs are typically not tagged to PF, being instead tagged to sanctions or AML concerns. Systems changes may be required to implement the ability to tag investigations to PF.
- Producing PF-specific Management Information (MI). For example, developing MI on the outcome of alerts and internal investigations, may help senior management have greater

visibility on PF risks. Currently PF alerts are subsumed within sanctions or AML alerts without any further identification. The absence of PF tags means that FIs cannot generate and utilise PF MI to support control adjustments.

The utilisation of dual-use goods lists by FIs is impracticable and ineffective in detecting PF. These lists were designed for the use of manufacturers, importers and exporters, given their proximity to the actual goods and technical expertise in their potential uses. Most financial transactions (non-trade finance or open account trading) do not contain the detail of the goods that would be required to screen for dual-use goods. If authorities aspire for FIs to screen goods via financial transaction data, then a re-specification of transactional data standards, such as relevant fields in payment messages, would be necessary to make relevant goods descriptions available. Data quality issues would remain even if changes were agreed, with the goods descriptions, transaction, documents or data available to FIs not, in isolation, allowing for an effective comparison with the details on the dual-use goods lists.

Multiple definitions of PF and the inconsistent applications of those definitions, even within countries where different agencies or regulatory authorities may apply differing definitions of PF, present challenges to FIs seeking to apply a consistent approach to PF.

It is not always clear which designation regimes do and do not relate to PF risk. OFAC's Non-Proliferation of Weapons of Mass Destruction (NPWMD) list or the UK and EU chemical weapons sanctions regimes are clearly "PF-relevant", it is less clear whether, for example, an "Iran" regime should be similarly counted, as Iranian parties may be sanctioned for a variety of reasons, of which PF is one.

FIs are conducting additional due diligence on Russia-related trade, however, most dual-use goods published by regulators (in Notices to Exporters) are not on any of the published dual-use goods lists.

In the UK, where a licence is granted for controlled items, the granted licence does not contain related financial services provisions for the FI. The FI must apply separately to the Export Control Joint Unit (ECJU) for a licence to process the payment.

FIs do not have a means of verifying that an export licence has been granted where a customer has claimed this to be the case and existing information sharing mechanisms are not currently utilised for such purposes. FIs are not informed about rejected export licence applications so as not to engage in related transactions should the exporter continue to engage in related transactions in the absence of an approved export licence.

Screening List vendors generally do not provide lists in a format which will enable tagging of alerts to PF to be done easily. Specific information related to sanctioned parties, including the sanctions regime under which they were designated, is typically provided in the description, but do not specifically flag PF risk. Consequently, while FIs' screening systems will identify the individual or entity as a sanctioned party, they are unable to automatically flag alerts as being PF-related. Any identification of PF linkages requires manual referral to the description in the listing.

Where tags are available FIs would need to implement screening and other systems changes on their side to enable tagging of alerts and/or investigations to PF. This would enable alerts for sanctioned parties linked to PF to be identified as PF related (in addition to their sanctions handling) and allow for PF related MI to be generated.

Chapter 1: Proliferation Finance Standards and Regulatory Framework

Introduction

The proliferation of nuclear, biological, and chemical weapons,[2] commonly referred to as Weapons of Mass Destruction (WMD), and their associated delivery systems (particularly ballistic or cruise missiles)[3] is a significant and ongoing international security concern. The Treaty on the Non-Proliferation of Nuclear Weapons (NPT)[4] seeks to prevent the spread of nuclear weapons beyond the recognised nuclear weapons states,[5] while the Chemical Weapons Convention[6] and Biological and Toxin Weapons Convention[7] seek to eliminate entirely these classes of weapons. Multilateral and national export control restrictions on the sale of components that could be used to fabricate such systems have similar or supporting aims. UNSCRs have introduced sanctions to prevent the spread of WMD, including the imposition of sanctions on countries known or believed to be seeking to acquire such weapons, notably Iran and North Korea.

Though counter proliferation has been a concern for a considerable time (the NPT was signed in 1968) requirements have historically focused primarily on sanctions and import and export restrictions. Specific requirements for FIs have chiefly related to implementing the financial restrictions imposed by designations of parties (whether individuals, entities, or vessels) involved in proliferation related activity. More recently FATF introduced a recommendation for countries and regulated institutions to assess and mitigate their PF risks. Consequently, increasing numbers of countries have published national PF risk assessments and, in the United Kingdom (UK), this requirement has been passed on to regulated FIs.

This chapter highlights PF-related definitions, standards, and frameworks applicable to the financial sector as set by the UN, FATF, UK, US, EU and the associated definitions of PF adopted. The diversity of definitions of PF poses a challenge to effective implementation of PF risk assessments and associated controls, particularly where an FI operates across multiple jurisdictions with potentially differing definitions applicable in each. In the absence of a definitional consensus, it is important for FIs to approach PF through consistent processes and procedures. While FIs are accustomed to operating in complex legal and regulatory environments, greater inter-jurisdictional consensus on the definition of PF enables international FIs to mitigate and manage the risk in the most coherent manner.

Whilst this paper is written by, and primarily for, the financial services sector, PF cannot be countered by FIs alone. Developing an effective response to PF risk requires broader collaboration, potentially including, but not limited to, export licensing authorities, law enforcement agencies, importers, exporters, shipping companies, customs agencies and screening list vendors. This paper highlights subjects for further engagement within and beyond the financial sector. In particular, FIs are often well placed to further develop intelligence provided by others to enhance visibility of PF related activity. Guided by the Wolfsberg Group's Statement on Effectiveness, this could also apply to a CPF

[2] And under some definitions, radiological weapons.

[3] This includes Unmanned Aerial Vehicles (UAVs) meeting particular technical parameters.

[4] United Nations. "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)". United Nations, 1968. (Accessed 28 August 2024).

[5] The Peoples' Republic of China, France, the Russian Federation, the United Kingdom and the United States.

[6] United Nations. "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and their Destruction". United Nations, 1992. (Accessed 28 August 2024).

[7] United Nations. "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction". United Nations, 1972. (Accessed 28 August 2024).

programme.[8] This includes, complying with AML/CTF laws and regulations; "providing highly useful information" to relevant government agencies in priority areas; and establishing a reasonable and risk-based set of controls to mitigate the risks of an FI being used to facilitate illicit activity.[9]

Regulatory Requirements

Whilst international standards on PF have developed significantly over the last few years, amongst the regulatory framework challenges remain with the absence of an internationally consistent definition of PF. The lack of a consistent definition has resulted in differing approaches across, and even within, jurisdictions. This poses a challenge to the coherence of multilateral responses to the threat of proliferation and risks numerous different and possibly conflicting national definitions of PF being established. As well as potentially hindering international legal co-operation, the lack of an agreed definition complicates the efforts of international organisations, including FIs, to comply with multiple, unaligned, regulatory regimes.

A survey of relevant UN, FATF, UK, US and EU regulatory requirements is contained in Appendix A of this paper.

(1) United Nations (UN)

United Nations Definition

The UN does not provide a definition of Proliferation Finance, however, UNSCR 1540 offers the following relevant provisions:

"Decides that all States, in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or ***finance*** *them".*

"Decides also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall: (d) Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as ***financing****, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations."*[10]

UNSCR 1540 (2004)

As identified by relevant UNSCRs listed below, the proliferation of WMD poses a significant threat to international peace and security. The relevant UNSCRs do not define PF. Instead, within the principle of counter-proliferation, UNSCR 1540 contains a broad provision that requires all States to prevent the provision of funds and financing that could contribute to proliferation through establishing effective measures and controls.

[8] Wolfsberg Group. "Statement on Effectiveness of AML/CTF Programmes". Wolfsberg Group 2019. (Accessed 30 August 2024).
[9] Ibid.

As set out in the joint report published by FATF and The Organization for Economic Cooperation and Development (OECD) in 2010, there are several routes by which countries can meet specific counter PF obligations established by UNSCR 1540.[11]

UNSCR 1718 (2006) and all successor resolutions concerning DPRK.*"*[12]

The UNSCRs authorise an extremely wide-ranging sanctions regime on the DPRK in response to its nuclear weapons and ballistic missile programmes. Among the measures are: a ban on the transfer to the DPRK of materials, technology or expertise relating to nuclear weapons and ballistic missiles; a ban on the import or export of any weapons or military equipment to/from the DPRK; asset freezes and transaction restrictions on a range of individuals and entities; trade restrictions (such as banning the export of key commodities like coal, iron and seafood from the DPRK, a ban on the import of luxury goods and a strict limitation on the import of refined petroleum to the DPRK); measures preventing DPRK ships from accessing international ports; a ban on hosting workers from the DPRK; and travel bans on key individuals.

UNSCR 2231 (2015) endorsed the Joint Comprehensive Plan of Action (JCPOA) on Iran, and replaced previous resolutions related to Iran.[13]

In October 2023, the UN's restrictions on Iran's missile-related activities under UNSCR 2231 expired, on what was supposed to be 'Transition Day', a milestone eight years after the adoption of the JCPOA.[14] Despite this, many States have continued to apply the same restrictions under their unilateral sanctions regimes.[15] 'Termination Day', when UNSCR 2231 is set to expire completely, is set for 18 October 2025. However, if any of the JCPOA participants notifies the UNSC before that date that it believes that the JCPOA's commitments have not been met, there remains the potential for 'snap-back' to the pre-JCPOA UNSC sanctions on Iran.

(2) Financial Action Task Force (FATF)

FATF Definitions

FATF proposed a working definition of an "Act of Proliferation Financing" in their 2010 report.[16]

"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."

In 2021, the 'FATF Guidance on Proliferation Financing Risk Assessment and Mitigation' described "the financing of proliferation" as:

"The risk of 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 or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes. WMD proliferation refers to 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 dual-use technologies and dual use goods used for non-legitimate purposes)."[17]

This description notably includes the "raising" of funds.

The same FATF Guidance describes "proliferation financing risk" in the context of FATF Recommendation 1 as referring:

"[Strictly] and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7."

This is referred to in the Guidance as "the narrow definition of PF risks as covered in the FATF Standards."

(3) United Kingdom (UK)

United Kingdom Definition

The UK's definition of "proliferation financing" is set out in Regulation 16A (9) of the UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended (UK MLRs) and is restricted to ensuring compliance with a "relevant UN obligation". This definition therefore excludes the UK chemical weapons sanctions on Russian and Syrian individuals.

"Proliferation financing" means the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons ("CBRN"), including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

"Relevant financial sanctions obligation" means a prohibition or requirement in regulations made under section 1 of the Sanctions and Anti-Money Laundering Act 2018 (SAMLA) *and imposed for one or more of the purposes in section 3(1) or (2) of that Act so far as it relates to compliance with a relevant UN obligation.*

"Relevant UN obligation" means an obligation that the UK has by virtue of a resolution adopted by the Security Council of the United Nations which relates to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and the financing of such."[18]

N.B. the UK PF definition refers to "CBRN" and so includes "radiological" weapons and related goods and technology, which are not specifically called out in the FATF definition, although they fall within the UK's definition of WMD.

(4) United States (US)

United States Definition

The US PF NRA adopts the FATF definition from the 2021 'FATF Guidance on Proliferation Financing Risk Assessment and Mitigation'.[19]

This refers to 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*.[20]"

The US has had longstanding prohibitions relating to PF and WMD.[21] Trading With the Enemy Act (TWEA), sanctions issued under TWEA applied on North Korea until 2008.[22] Unlike the UK MLRs the US does not have specific regulatory requirements for PF risk assessment by FIs and effective mitigation of the identified risks. The US largely relies on:

- The US International Emergency Economic Powers Act (IEEPA), the primary implementing authority for US counter proliferation sanctions. 23

- The Executive Order 13382 (EO 13382), issued under IEEPA, sets out the framework within which proliferators can be designated.24 Through EO 13382 the US has designated various parties for activities related to PF.

In the context of PF, IEEPA empowers the US government to freeze assets, restrict transactions, and take other measures to combat PF activities.[25] Violations of IEEPA would be a predicate offence to the US Federal crime of Money Laundering.[26] There is therefore an obligation on US FIs to report attempts to violate and/or evade the restrictions imposed by IEEPA as suspicious activity to the relevant US Federal Authorities.

(5) European Union (EU)

European Union Definition

There is currently no definition of proliferation or proliferation finance within the relevant EU Council Decisions and Council Regulations or within the proposed AML/CTF Directive/Regulatory framework.

While there is no definition for PF within the EU AML Regulation and Directive, it is expected that "relevant Union legal acts should be aligned with International Standards on Combating the Financing of Terrorism and Proliferation adopted by the FATF in February 2012" and , alignment with FATF PF recommendations, through adherence to the relevant UN Sanctions implemented by the EU, is expected.[27] Also, whilst international standards and requirements on PF have evolved rapidly in the past few years, within the EU there are challenges across EU Member States with regard to the identification of PF risks and trends including the lack of a common definition. Similarly to the US, the EU does not have specific regulatory requirements for PF risk assessment by FIs and effective mitigation of the identified risks.

Chapter 2: Proliferation Finance Risk Assessment

Introduction

Risk assessments undertaken by FIs rely upon factors relevant to PF. These are seldom explicitly identified by authorities, but our review of the literature has allowed us to highlight a number of potentially relevant risk factors.[28]

Case studies indicate industries that may be more vulnerable than others to exploitation by proliferators, such as involvement in the production, trade, movement or financing of proliferation-sensitive goods and technologies that are required by states seeking a WMD capability. While customers in these industries may have no knowledge or complicity in PF activities, any exploitation of these customers by proliferators could in turn expose an FI that provides them with banking services to PF risks.

Whilst PF risk can crystalise in any location, certain countries or geographic areas may present higher risk than others. This risk takes different forms: countries with active WMD proliferation programmes; locations which manufacture, or export goods, technology or raw materials required by proliferators; locations that assist proliferators to raise funds (such as by purchasing sanctioned exports); locations through which items are transhipped; and jurisdictions hosting PF-enablers, such as shell companies. Customer risk assessments may need to consider how to factor in consideration of these. This Chapter shares the steps taken by FIs to assess their PF risks and highlights PF-relevant risk factors.

An FI does not necessarily require a separate, dedicated risk assessment framework to assess its PF risk, as distinct from ML, TF, sanctions or other FC risks. FATF's guidance on PF risk assessment and mitigation states that "*private sector entities may [identify, assess, monitor, manage and mitigate proliferation financing risk] within the framework of their existing financial sanctions and/or compliance programmes, and are not expected to establish duplicative processes for proliferation financing risk assessment or mitigation*". [29] Similarly, the UK Joint Money Laundering Steering Group (JMLSG) provided guidance following the UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended (UK MLRs) amendment stating that "*a stand-alone PF risk assessment is not required.*" [30]

The UK Finance Proliferation Finance Working Group conducted a survey in June 2023 establishing where within their framework UK Finance Members assessed their PF risk (see figure 1). Members variously used their AML risk assessment framework, their sanctions risk assessment framework, a combination of these, or a separate, bespoke assessment framework for PF. Given the significant overlap in risk factors between PF risk and both AML and sanctions risk, the Working Group judges that all of these are valid approaches to assessing PF risk, providing that the factors relating specifically to PF are assessed.

[28] Refer to the PF Resources Information Repository at the end of this document for a full list. Individual sources are referenced where relevant within the report.

[29] FATF. "FATF Guidance on Proliferation Financing Risk Assessment and Mitigation". FATF, June 2021. (Accessed 20 August 2024).

[30] The Joint Money Laundering Steering Group. "Prevention of Money Laundering/combating terrorist financing. 2023 Revised Version. Guidance for the UK Financial Sector. Part 1." The Joint Money Laundering Streeting Group, June 2023. (Accessed 20 August 2024)

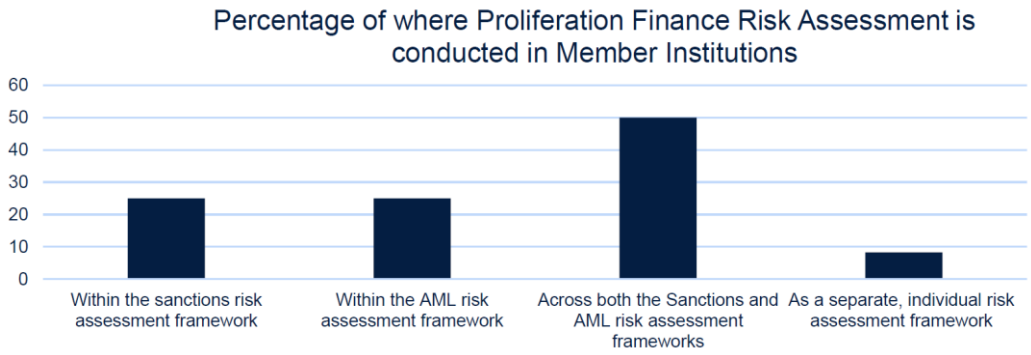

Figure 1: UK Finance member survey on where within their framework proliferation finance risk is assessed.

Risk Factors

In assessing PF risk, the UK MLRs require an FI to take into account risk factors relating to its:

- customers;
- the countries or geographic areas in which it operates;
- products or services;
- transactions; and
- delivery channels.[31]

This chapter presents a variety of potential PF risk factors and cross-cutting themes upon which FIs may draw when designing their own risk assessments. It is not meant to be exhaustive, particularly given that PF typologies and the literature documenting them are developing rapidly. FIs remain responsible for determining which PF risk factors their business is subject to and for reviewing the latest literature that is published by government and regulatory authorities when completing a PF risk assessment. As noted in Section 18A of the UK MLRs, FIs must take into account the size and nature of their business when deciding what steps are appropriate in this risk assessment.[32] Further, Section 19A of the UK MLRs requires that the policies, controls and procedures established to mitigate and manage effectively the PF risks identified by the risk assessment (see Chapter 3) should be proportionate to the size and nature of an FI's business.[33]

The risk factors relating to an FI's customers; the countries or geographic areas in which it operates; its products or services; its transactions; its delivery channels and cross-cutting themes identified in this Chapter may be useful for refining an FI's assessments of risk at country, product, customer and business-wide level to account for PF risk. They are most indicative of risk when used in combination rather than individually.

FIs may judge those that present risks relevant to their operations. To note, many of the risk factors listed below may already be considered to be higher risk for any combination of ML, TF, sanctions

[31] "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Part 2, Chapter 2, Regulation 18A". Legislation.gov.uk, n.d. (Accessed 20 August 2024).

[32] "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Part 2, Chapter 2, Regulation 18A". Legislation.gov.uk, n.d. (Accessed 20 August 2024).

[33] N.a. "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Part 2, Chapter 2, Regulation 19". Legislation.gov.uk, n.d. (Accessed 20 August 2024).

evasion or other FC risks. Therefore, many will feature in FIs' existing risk assessment mechanisms and now need to be considered from a PF perspective.

(1) Customer

When assessing an FI's PF risk arising from its customer base, it can be helpful to frame this in terms of the customer's potential role in PF activities. Customers may be wittingly or unwittingly involved in the raising of funds to be used in support of illicit proliferation programmes, the sourcing of proliferation-sensitive items, or enabling the movement of these items. The 2021 UK PF National Risk Assessment (PFNRA) frames the risks as being either direct or indirect:

(1) **Direct Risks.** These arise from those customers who are closest to the production, funding or movement of proliferation-sensitive goods or the evasion of financial sanctions regimes or export controls.
(2) **Indirect Risks.** These arise from activities in which there are a greater number of steps between the financial source and the proliferating actor. They typically arise through the use of front or shell companies or intermediaries that enable the true source of funds and the destination of the goods to be masked from the producer of those goods as well as FIs supporting the transactions. [34]

Business Sector Risks

The literature on PF risk does not provide any consolidated list of industries or business sectors that are considered to be high risk. However, multiple case studies[35] identify several industries that may be more vulnerable than others to exploitation by proliferators. This may be because they produce, trade, move or finance proliferation-sensitive goods and technologies that are required by proliferators. While customers in these industries may have no knowledge or complicity in PF activities, any exploitation of these customers by proliferators could in turn expose an FI that provides them with banking services to PF risks. In many cases, NACE2 industry codes may assist in identifying customers operating in these business sectors.[36] However, in many cases the code covers a significantly wider segment than the specific areas identified as more vulnerable to exploitation by proliferating actors and would require further analysis, such as engagement with the customer, to determine whether they fall within a vulnerable sector. In other cases, we could not identify any relevant NACE2 industry codes.

Many of the business sectors identified below produce or trade in items specifically designed or modified for military use and/or in "dual-use items." Dual-use items are recognised as having both civilian and military (WMD or conventional weapons) uses. Many jurisdictions have export control mechanisms governing the trade in such items. The UK includes such items within the Department

---

[34] HM Treasury. "National Risk Assessment of Proliferation Financing." HM Treasury, September 2021. (Accessed 20 August 2024).

[35] Contained, for example, in: HM Treasury. "National risk assessment of proliferation financing". HM Treasury, September 2021. (Accessed 20 August 2024).; Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024).; Australian Government – AUSTRAC. "Proliferation Financing in Australia." AUSTRAC, 2022. (Accessed 20 August 2024).; Asia Pacific Group. "Documents". Asia Pacific Group, n.d. (Accessed 20 August 2024).; FATF. "Guidance on Proliferation Financing Risk Assessment and Mitigation". FATF, June 2021. (Accessed 20 August 2024); Dr Daniel Salisbury. "North Korea's Diplomatic Sanctions-Busting Network Adapts to Changing Times". Royal United Services Institute (RUSI), November 2023. (Accessed 20 August 2024).; United Nations Security Council. "Resolution 1540 (2004)". United Nations, April 2004. (Accessed 20 August 2024).; United Nations. "Information Note." United Nations, n.d. (Accessed 20 August 2024).

[69] FIs that use industry codes other than NACE2 in their risk assessments (e.g. SIC or ISIC codes) may be able to map these NACE2 codes to their preferred system.

for Business and Trade's Strategic Export Control Lists.[37] While businesses operating in some of the sectors identified below may be more likely to trade in military or dual-use items than businesses in other sectors, this does not mean that PF risk cannot crystallise in other sectors.

Business Sector (including potentially relevant NACE2[38] codes)	**Sources[39]**	**Comments**
Arms manufacturers and suppliers 2540 (Manufacture of weapons and ammunition)	APG Aus PFNRA UK PFNRA US PFNRA	The UK PFNRA states "*All UK sectors connected to production of military and dual-use items can be exploited by proliferating actors" however, "Major defence suppliers tend not to supply to private entities unless supported by a verified government contract*". Typically, the "*Most at risk are medium-sized defence sub-contractors and the dual-use items sector, where there may be less awareness of proliferation risks and suppliers' export control*." The US PFNRA states "*the role of US manufacturers in producing military and proliferation-related technology (including dual-use items) continue[s] to make the United States a target of exploitation by PF networks*"
Nuclear industry 2446 (Processing of nuclear fuel) 0721 (Mining of uranium and thorium ores) 2660 (Manufacture of irradiation/electromedical equipment)	UK PFNRA	The UK PFNRA notes that "*goods which can be used in the nuclear industry which are also used in everyday items or for use in commercial industry, such as carbon fibre, vacuum pumps, electronic components and testing equipment*" can be procurement targets for proliferators.
Chemical industry 4612 (Agents involved in the sale of fuels, ores, metals and industrial chemicals) 4675 (Wholesale of chemical products) 0891 (Mining of chemical and fertiliser minerals) 2013 (Manufacture of other inorganic basic chemicals) 2014 (Manufacture of other organic basic chemicals) 2059 (Manufacture of other chemical products n.e.c.)	UK PFNRA US PFNRA	The UK PFNRA notes chemical production as being directly relevant to the production of military and dual-use items, and states "*chemical… materials and related equipment, are types of items that attract procurement attempts from overseas actors." As an example, it notes that chemicals used as flame retardant can be considered as dual-use items as they may also be precursors for chemical weapons.* *The US PFNRA notes that "chemical science advancements…[could be used] to develop new or enhanced agents*".
Life Sciences industry	UK PFNRA US PFNRA	The UK PFNRA includes life sciences as being directly relevant to the production of military and dual-use items, and notes that "*biological materials and related equipment, are*

[37] Export Control Joint Unit. "Consolidated List of Strategic Military and Dual-Use Items that Require Export Authorisation." Department for Business and Trade, April 2024. (Accessed 20 August 2024).

[38] Eurostat. "NACE Rev. 2 Statistical classification of economic activities in the European Community." European Commission, 2008. (Accessed 28 August 2024).

[39] HM Treasury. "National risk assessment of proliferation financing". HM Treasury, September 2021. (Accessed 20 August 2024).; Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024).; Australian Government – AUSTRAC. "Proliferation Financing in Australia." AUSTRAC, 2022. (Accessed 20 August 2024).; Asia Pacific Group. "Documents". Asia Pacific Group, n.d. (Accessed 20 August 2024).; FATF. "Guidance on Proliferation Financing Risk Assessment and Mitigation". FATF, June 2021. (Accessed 20 August 2024); Dr Daniel Salisbury. "North Korea's Diplomatic Sanctions-Busting Network Adapts to Changing Times". Royal United Services Institute (RUSI), November 2023. (Accessed 20 August 2024).; United Nations Security Council. "Resolution 1540 (2004)". United Nations, April 2004. (Accessed 20 August 2024).; United Nations. "Information Note." United Nations, n.d. (Accessed 20 August 2024).

7211 (Research & experimental dev on biotechnology)		*types of items that attract procurement attempts from overseas actors*." The US PFNRA's primary concern under the "Emerging Technologies" section is that "*advances in life sciences and biotechnology… can also bring new security risks from potential intentional misuse*".
Aerospace industry 4614 (Agents involved in the sale of machinery, industrial equipment, ships and aircraft) 3030 (Manufacture of air and spacecraft and related machinery) 5110 (Passenger air transport) 5121 (Freight air transport) 7735 (Renting and leasing of air transport equipment) 3316 (Repair and maintenance of aircraft and spacecraft) 5122 (Space transport)	APG Aus PFNRA UK PFNRA	The UK PFNRA gives a case study where items from the aerospace industry were purchased by an Iranian illicit procurement network. The Aus PFNRA gives the aerospace industry as an example of a sector targeted by procurement networks to obtain restricted, sensitive or dual-use goods and knowledge.
Electronics, Telecommunications and optics industry 2651 (Manufac instruments – measuring/testing/navigation) 2670 (Manufacture optical instruments & photographic equipment) 2611 (Manufacture of electronic components) 2612 (Manufacture of loaded electronic boards) 2620 (Manufacture of computers and peripheral equipment) 2640 (Manufacture of consumer electronics) 4222 (Construction of utility projects for electricity and telecommunications) 4651 (Wholesale of computers, computer peripheral equipment and software) 4652 (Wholesale of electronic and telecommunications equipment and parts) 4741 (Retail sale of computers, peripheral units and software in specialised stores) 6110 (Wired telecommunications activities) 6120 (Wireless telecommunications activities) 6130 (Satellite telecommunications activities) 6190 (Other telecommunications activities) 9521 (Repair of consumer electronics)	APG UK PFNRA US PFNRA	The UK PFNRA highlights that UK-manufactured electronic components were found in the debris of a 2012 missile test by the DPRK. The US PFNRA provides multiple examples of cases in which US-manufactured dual-use electronics were illicitly procured for shipment to Russia or Iran. These included highly sensitive and heavily regulated electronic components which could be used in the development of nuclear and hypersonic weapons (Russia) and in the production of UAVs (Iran).
Petrochemical industry 0610 (Extraction of crude petroleum) 0620 (Extraction of natural gas)	APG Aus PFNRA UK PFNRA	The UK PFNRA highlights Iran's practice of selling oil and other petrochemicals to China and Syria as a means to fund its proliferation programmes. It also highlights petroleum as a commodity involved in instances of DPRK evasion of proliferation-linked sanctions.

0910 (Support acts petroleum and natural gas extraction) 4671 (Wholesale of solid, liquid and gaseous fuels and related products) 1920 (Manufacture of refined petroleum products)		The Aus PFNRA highlights the vulnerability of its exports of crude and refined petroleum to Asia, which could be diverted to the DPRK. It notes the role of ship-to-ship transfers in this activity, as well as direct shipments to the DPRK. The same report gives a case study involving an Australian citizen and a series of Australia-based front companies involved in brokering trade involving crude oil on behalf of the DPRK, including purchasing Iranian petrol for the DPRK.
Maritime sector 5020 (Sea and coastal freight water transport) 4614 (Agents involved in the sale of machinery, industrial equipment, ships and aircraft)	APG Aus PFNRA FATF UK PFNRA US PFNRA	FATF notes this sector as presenting a higher risk of exposure to PF sanctions evasion. The US PFNRA explains that "*the utilization of the maritime sector to facilitate the illicit movement of proliferation-sensitive goods or natural resources trade in violation of UN or US sanctions*" is a critical component of PF typologies. It also notes that this activity is conducted by networks of front and shell companies. The UK PFNRA notes the vulnerability of the maritime sector in general to this risk and includes a specific focus on the UK maritime insurance and the London reinsurance market as being a key source of PF exposure for the UK. It notes that in some instances UK insurance providers may be removed from the underwriting process of the primary insurer, and therefore have limited visibility of the risks and mitigations applied.
DACs / Crypto sector No relevant NACE2 code identified	Aus PFNRA FATF UK PFNRA US PFNRA	FATF notes this sector as presenting a higher risk of exposure to PF sanctions evasion. DACs/crypto can be used to transfer value between pseudonymous parties, including proliferators. Large scale cybercrime, including the theft of DACs and ransomware extortion, is a significant fundraising stream supporting the DPRK's proliferation programmes. See the "Cross-cutting themes" section below for a more detailed discussion of PF risk associated with the DACs / Crypto sector.
Luxury goods sector 1101 (Distilling, rectifying and blending of spirits) 1102 (Manufacture of wine from grape) 1200 (Manufacture of tobacco products) 4634 (Wholesale of beverages) 4635 (Wholesale of tobacco products)	APG RUSI UK PFNRA UNSCRs	The UK PFNRA assesses that "*the UK could potentially act as a source of luxury goods for North Korea*", noting that UNSC proliferation-related sanctions prohibit such trade. RUSI notes that DPRK diplomats can be involved in luxury goods procurement.
Professional Service Providers, especially Trust & Company Service Providers (TCSPs) 6910 (Legal activities) 6920 (Accounting, bookkeeping and auditing activities, tax consultancy) 6430 (Trusts, funds and similar financial entities)	Aus PFNRA FATF UK PFNRA	Given the prominence of front or shell companies within PF activities, the industry that is often used to create, provide or service such companies is regarded as higher risk. The UK PFNRA explains that "*these firms allow individuals to buy 'shelf' companies with established banking and credit histories, in order to create the impression of a reputable company, or use a nominee shareholder or directors, in order to increase the anonymity of the beneficial owners of a company*." FATF notes this sector as presenting a higher risk of exposure to PF sanctions evasion.

		See the "Cross-cutting themes" section below for a more detailed discussion of PF risk associated with shell companies.
Dealers in precious metals and stones 2441 (Precious metals production) 4648 (Wholesale of watches and jewellery) 4777 (Retail sale of watches and jewellery in specialised stores) 3212 (Manufacture of jewellery and related articles)	Aus PFNRA FATF RUSI	FATF notes this sector as presenting a higher risk of exposure to PF sanctions evasion. RUSI details how this sector is exploited by the DPRK, noting gold as the most common precious metal / stone featuring in PF case studies and wholesale / trading as the most common activity / stage. The Aus PFNRA notes that Australian mining expertise and technology and some of the materials the industry produces may also be of interest to other proliferation actors, either for their value (in the case of gold or other precious metals) or for their application in industry, including for military or WMD purposes (in the case of aluminium, iron or uranium).
Import / Export agents, trading companies and freight forwarding firms in countries identified as having Transhipment risks 4690 (Non-specialised wholesale trade) 5229 (Other transportation support activities)	Aus PFNRA FATF	Companies that provide these types of services are required in order to actually move goods around the world. They may do this knowingly or unknowingly. The Aus PFNRA notes that professionals working in Australia's import-export sector may be targeted by proliferators. FATF notes that freight forwarding firms listed as a shipment's final destination is a PF risk indicator.
Extractives / Mining Sector 0710 (Mining of iron ores) 0721 (Mining of uranium and thorium ores) 0729 (Mining of other non-ferrous metal ores)	Aus PFNRA FATF	The Aus PFNRA explains that Australia's globally significant mining industry is vulnerable as it exports metals and materials subject to UNSC restrictions, which could be diverted to DPRK and Iran. Aluminium, iron and uranium mining in particular are noted. FATF notes the DPRK's involvement in gold mining in Sub-Saharan Africa.
DPRK Embassies and diplomatic staff 8421 (Foreign affairs) – note that this industry code is much wider in scope than the identified sector.	UK PFNRA UN PoE	The UK PFNRA notes that DPRK representatives engage in revenue generation, access to the financial system and movement (via diplomatic bags) of cash or goods, and that diplomatic property has been used to generate revenue. The UN Panel of Experts highlights multiple examples of such activity.
DPRK Overseas Workers	UK PFNRA UN PoE US PFNRA	The UK PFNRA notes that overseas working of DPRK citizens has been banned by UNSC sanctions since December 2019. Such workers generate revenue for the regime and can assist in the procurement of items. It further notes that DPRK students studying overseas may find opportunities to generate revenue. The US PFNRA highlights the particular prevalence of skilled DPRK overseas workers in the IT industry, noting that these are primarily located in China and Russia. The UN PoE highlights multiple examples of such activity.

(2) Countries or Geographic Areas

Whilst PF risk can crystalise in any location, certain countries or geographic areas may present higher risk than others. The majority of such locations correspond to sovereign states or territories, but there are also instances where the sources identified higher geographic risk relating to specific provinces, cities and maritime zones. This paper does not record references in the literature to whole regions or widely-defined geographic areas, such as "located in Asia" or "a Middle Eastern country", as such generalised locations are challenging to operationalise within a risk management framework.

Geographical PF risk presents in a variety of forms. Our analysis identified five primary categories of geographical PF risk. Any given location may be at heightened risk from multiple categories:

(1) **Proliferation Concerns.** This category applies to countries with reported active chemical, biological, radiological or nuclear (CBRN) weapons programmes which have been noted by one or more of our key sources. The wording of FATF Recommendation 1 and the MLR definition of "proliferation finance" limit the scope of the required risk assessment to contraventions of UNSC sanctions relating to CBRN proliferation. However, many countries' PFNRAs, sanctions regimes and export controls or reports by international organisations take broader views of PF risk and highlight additional countries with active CBRN weapons programmes that present concerns. Examples include:

a. The UK, US, EU and others have thematic financial sanctions programmes relating to the proliferation and use of chemical weapons (current listings under these programmes feature parties from Syria and Russia).[40]
b. The US PFNRA highlights that China, Pakistan, Russia and Syria all exploit the US financial system and other US private sector actors to finance their WMD proliferation programmes in violation of international and/US financial or trade sanctions or export controls.[41]

There is little international consensus on which countries, beyond the DPRK and Iran, should be considered as presenting proliferation concerns. Many UK FIs have CPF obligations that extend beyond implementing UNSC sanctions and they may need to reflect these in their PF risk assessments.

(2) **Source Geographies.** This category applies to locations containing targets attractive to proliferation procurers, such as manufacturers or exporters of CBRN-related goods and technology (see section above on customer risk factors), or locations from which raw materials may be sourced. Inclusion in this category does not imply intentional participation in illicit CBRN proliferation programmes, or even that proliferation procurement has occurred, but simply indicates an inherent vulnerability to illicit procurers.

[40] Foreign, Commonwealth & Development Office. "UK sanctions relating to chemical weapons". Foreign, Commonwealth & Development Office, March 2019. (Accessed 20 August 2024); Ambassador Bonnie Denise Jenkins in "Remarks at a UN Security Council Briefing on Chemical Weapons in Syria". US Department of State, February 2013. (Accessed 20 August 2024).; U.S. Department of Treasury. "Treasury Sanctions Russian Operatives and Entities Linked to the Poisoning of Alexey Navalny, Chemical Weapons Program." U.S. Department of Treasury, August 2021. (Accessed 20 August 2024).; Council of the EU. "Chemical weapons: EU imposes further restrictive measures on ten individuals and one entity." Council of the European Union, November 2022. (Accessed 20 August 2024).

[41] Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024).

(3) **Fundraising Geographies.** CBRN proliferation programmes are expensive and proliferating governments need to raise funds to support them. This fundraising activity is itself often sanctioned, either by the UNSC or unilaterally, in order to constrain the illicit CBRN proliferation programmes. Such sanctions turn activity that would in normal circumstances be legitimate economic activity, such as the export of goods and services or labour, into illicit proliferation activity. Where geographies other than the proliferating states themselves are involved in enabling this activity, such as by purchasing sanctioned commodities from proliferating states, they are categorised here as fundraising geographies.

(4) **Transhipment Geographies.** This category covers geographies frequently noted for the transhipment of physical items that are being moved in association with illicit CBRN proliferation programmes. Transhipment means the movement of cargo or goods from one location to another via an intermediary location, in which they are 'transhipped' from one means of transportation to another. This includes the use of 'gateway' countries sharing a land or maritime boundary with a country with reported active CBRN weapons programmes. The transhipment geography may be falsely described as the 'end destination' of the items to assist in evading export controls.

(5) **Enabling Geographies.** This is a broad category that encompasses geographies associated with any form of activity that enables or assists illicit CBRN proliferation programmes but is not covered by one of the above categories. Examples include jurisdictions frequently noted as the registering location or banking location of shell or front companies used to handle funds associated with PF activity and jurisdictions whose shipping registries are frequently noted as the flags of vessels associated with PF-related illicit maritime activity.

Where one or more of the sources has noted an active CBRN proliferation programme of concern, it is listed in the table below by the relevant country by name, complete with an indication of which key sources refer to it and a brief commentary on the nature of the source's concerns. In several cases, the sources note that these countries have additional PF fundraising and/or enabling concerns relating to their interactions with another country of proliferation concern, which has been commented on.

More widely, geographical PF risk factors relating to sourcing, fundraising, transhipment and enabling can apply to large numbers of countries. We have listed the main forms of these risks and the characteristics of geographies that may be vulnerable to them (e.g., countries with a major manufacturing or supply sector in proliferation-relevant items) without attempting to list every country mentioned, however briefly, by our sources. However, where our sources have identified a specific country as being particularly prone to one of these risks (for example, that a certain country is "the usual routing" for freight movement to Iran), then we have mentioned this in the comments section for that country.

Country or Geographic Area	Sources[42]	Comments
DPRK	Aus PFNRA FATF IAEA UN PoE UNSCR UK PFNRA US PFNRA	**Proliferation Concerns** The DRPK's status as a nuclear weapon state is not recognised under the NPT, from which the country withdrew in 2003. Its nuclear activities are not under IAEA safeguards, and countries that are NPT parties are prohibited by the treaty from supporting the DPRK's nuclear weapons activities in any way. The DPRK's illicit CBRN proliferation programmes are the subject of ten UNSCRs and FATF identifies the DPRK as a country with proliferation concerns. The UK PFNRA identifies the DPRK as "*the primary PF state actor". The US PFNRA identifies the DPRK, jointly with Russia, as "the highest-risk threat actors… because of the scope and sophistication of their illicit procurement and revenue-generation efforts*". While the DPRK's nuclear weapons and ballistic missile programs receive the most attention, the 2022 edition of the US PFNRA also highlighted concerns relating to chemical and biological weapons, including the DPRK's use of a chemical weapon to conduct an assassination at Kuala Lumpur airport in Malaysia in 2017. See the sections below on Russia and China for PF fundraising links between the DPRK and these states.
Iran	Aus PFNRA FATF IAEA UNSCR UK PFNRA US PFNRA	**Proliferation Concerns** Iran is a party to the NPT. However, the IAEA has criticised Iran's cooperation with its safeguards, noting the challenges this presents to its ability to assure Iran's compliance with the NPT. Iran's nuclear and ballistic missile proliferation programmes are the subject of UNSCR 2231 (2015), although the remaining Targeted Financial Sanctions (TFS) authorised under this UNSCR expired in October 2023. FATF identifies Iran as a country with proliferation concerns. Along with the DPRK, the UK PFNRA identifies Iran as a key actor behind PF networks impacting the UK financial system. The US PFNRA states that "*Iran is increasing the size and enrichment level of its uranium stockpile and is conducting advanced centrifuge research and development*". The US PFNRA also states concerns relating to Iran's missile and UAV programmes, the latter of which presents WMD delivery risks as well as non-WMD concerns relating to Russia's war in Ukraine and use by terrorist proxy groups. See the sections below on Syria, Russia and China for PF fundraising links between Iran and these states.
Syria	OPCW UK PFNRA US PFNRA	**Proliferation Concerns** Syria is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation financing" contained in Section 16A of the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator.

[42] HM Treasury. "National risk assessment of proliferation financing". HM Treasury, September 2021. (Accessed 20 August 2024).; Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024).; Australian Government – AUSTRAC. "Proliferation Financing in Australia." AUSTRAC, 2022. (Accessed 20 August 2024).; Asia Pacific Group. "Documents". Asia Pacific Group, n.d.. (Accessed 20 August 2024).; FATF. "Guidance on Proliferation Financing Risk Assessment and Mitigation". FATF, June 2021. (Accessed 20 August 2024).; Dr Daniel Salisbury. "North Korea's Diplomatic Sanctions-Busting Network Adapts to Changing Times". Royal United Services Institute (RUSI), November 2023. (Accessed 20 August 2024).; United Nations Security Council. "Resolution 1540 (2004)". United Nations, April 2004. (Accessed 20 August 2024).; United Nations. "Information Note." United Nations, n.d. (Accessed 20 August 2024).; International Atomic Energy Agency. "Safeguards Agreements". International Atomic Energy Agency, n.d. (Accessed 20 August 2024).; Organisation for the Prohibition of Chemical Weapons. "OPCW Fact-Finding Mission." OPCW. (Accessed 28 August 2024).; Department of State; Department of the Treasury; United States Coast Guard. "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities." Department of State; Department of the Treasury; United States Coast Guard, May 2020. (Accessed 20 August 2024).

		However, investigations by the Organisation for the Prohibition of Chemical Weapons (OPCW) have found that chemical weapons were used or likely used in 20 instances during the ongoing conflict in Syria. The EU, UK, US and other governments have used their autonomous sanctions regimes on chemical weapons to designate individuals and entities from Syria. **Fundraising Geography** (with respect to Iran) The UK PFNRA notes that Syria has purchased Iranian oil and other petrochemicals, making it a fundraising geography with respect to Iranian proliferation.
Russia	UK PFNRA US PFNRA	**Proliferation Concerns** Russia's status as a nuclear weapon state is recognised under the NPT. Russia is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation financing" contained in Section 16A of the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator. However, the US PFNRA identifies Russia, jointly with the DPRK, as "the highest-risk threat actors due to scope and sophistication of their illicit procurement and revenue-generation efforts". The US PFNRA notes that Russia has reduced or suspended its participation in a number of international WMD-related treaties, including the New Strategic Arms Reduction Treaty (New START) and the Comprehensive Nuclear Test Ban Treaty. The US PFNRA also highlights that Russia seeks to procure from overseas goods and technologies that it cannot source domestically. It presents several case studies involving networks attempting to procure such items covertly from the US in violation of export controls, including highly sensitive and heavily regulated electronic components which could be used in the development of nuclear and hypersonic weapons. Additionally, individuals and entities from Russia have been designated under the UK and US autonomous sanctions regimes on chemical weapons, and the US PFNRA states that "*the United States continues to certify that Russia is in breach of its commitments to the Chemical Weapons Convention, based on Russia's use of chemical weapons in targeted assassinations, support for the Assad regime's use of chemical weapons, and its ongoing, undeclared offensive chemical weapons programme*". **Fundraising Geography** (with respect to Iran and DPRK) **Iran:** The US PFNRA states that Iran has transferred UAV technology to Russia for use in its war in Ukraine. While this activity has not been linked directly to WMD proliferation, such transfers prior to 18 October 2023 may have violated proliferation-related UNSCR 2231 on Iran and constitute PF fundraising risk with respect to Iran, and transfers after that date would potentially violate multiple unilateral sanctions regimes. **DPRK:** The EU, Japan, the Republic of Korea (South Korea), the UK and the US have accused Russia of purchasing ballistic missiles and conventional munitions from the DPRK for use in its war in Ukraine. If true, this would implicate Russia in violations of UNSCRs relating to the DPRK, and in PF fundraising risk with respect to the DPRK. The US PFNRA notes that Russia and China are the primary locations in which thousands of skilled DPRK IT workers reside, working remotely on a freelance basis in contravention of UNSC sanctions, with their earnings helping to support the DPRK's WMD programmes.
China	Aus PFNRA UK PFNRA US PFNRA UN PoE	**Proliferation Concerns** China's status as a nuclear weapon state is recognised under the NPT. China is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation financing" contained in Section 16A of

		the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator. The US PFNRA states that it "has seen persistent efforts by PF networks, operating on behalf or at the direction of… the People's Republic of China… to exploit the US financial system and other US private sector actors to finance WMD proliferation." **Fundraising Geography** (with respect to Iran and DPRK) **Iran:** The UK PFNRA notes that China purchases Iranian oil and other petrochemicals, creating significant PF income for the Iranian regime. **DPRK:** The UK PFNRA notes the importation of DPRK-origin coal and sand into China, particularly in the **Ningbo-Zhoushan area**, and multiple cases of illicit ship-to-ship transfers in Chinese jurisdiction, all breaching UNSC sanctions and assisting the DPRK in raising funds which may be used to support its CBRN programmes. The US PFNRA notes that China and Russia are the primary locations in which thousands of skilled DPRK IT workers reside, working remotely on a freelance basis in contravention of UNSC sanctions, with their earnings helping to support the DPRK's WMD programmes. Other than the DPRK itself, China is by far the most frequently mentioned country in the UN PoE reports, linked to 694 (12.9%) of all entities in the dataset. The majority of these entities are companies (potentially including shell and front companies). Addresses in **Dalian**, **Dandong** and **Shenyang** (all cities in **Liaoning Province**, which borders the DPRK), **Beijing**, and the **Ningbo-Zhoushan area** feature prominently. For reporting of China's role as a Transhipment Geography, see the "Countries used to tranship physical items en route to countries with proliferation concerns" section below.
Pakistan	IAEA US PFNRA	**Proliferation Concerns** Pakistan is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation finance" contained in Section 16A of the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator. Pakistan has publicly-declared its nuclear weapons capability. It is not a party to the NPT, and its status as a nuclear weapon state is not recognised under the NPT. Countries that are NPT parties are prohibited by the treaty from supporting Pakistan's nuclear weapons activities in any way. Pakistan has item-specific agreements with the IAEA, meaning that it voluntarily observes some international safeguards associated with the NPT. The US PFNRA states that it "*has seen persistent efforts by PF networks, operating on behalf or at the direction of… Pakistan, to exploit the US financial system and other US private sector actors to finance WMD proliferation.*" It also states that Pakistan has an active ballistic missile development programme, and that "individuals and entities acting on behalf of Pakistan have engaged in illicit procurement for specific US-origin goods, violating relevant US export control laws". The US Department of State has imposed unilateral sanctions on several entities and individuals for transferring equipment and technology that may be used in the development of Pakistan's ballistic missile capability.
India	IAEA	**Proliferation Concerns** India is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation finance" contained in Section 16A of the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator.

		India has publicly-declared its nuclear weapons capability. It is not a party to the NPT, and its status as a nuclear weapon state is not recognised under the NPT. Countries that are NPT parties are prohibited by the treaty from supporting India's nuclear weapons activities in any way. India has item-specific agreements with the IAEA, meaning that it voluntarily observes some international safeguards associated with the NPT.
Israel	IAEA	**Proliferation Concerns** Israel is not the subject of UNSCR proliferation-related sanctions and consequently does not meet the definitional criteria of "proliferation finance" contained in Section 16A of the UK MLRs. Similarly, it does not meet the definitional criteria of FATF Recommendations 1 or 7 relating to PF, and it is not named by FATF as a proliferator. Israel is widely considered to possess a nuclear weapons capability; it neither confirms nor denies this. It is not a party to the NPT, and its status as a nuclear weapon state is not recognised under the NPT. Countries that are NPT parties are prohibited by the treaty from supporting Israel's nuclear weapons activities in any way. Israel has item-specific agreements with the IAEA, meaning that it voluntarily observes some international safeguards associated with the NPT.
Countries with large international finance centres	UK PFNRA US PFNRA	**Enabling Geography** The UK PFNRA states that "*Given the UK's role as a global financial centre, the UK's financial system presents unique opportunities for proliferating actors to access wide ranging financial services and technologies to support their proliferating activities*." The US PFNRA makes a similar point: "*The US financial system's size, sophistication, stability, and openness makes it particularly vulnerable to misuse by illicit proliferation networks*." The UK and US PFNRAs each include a case study in which Iranian proliferation-related payments originated from bank accounts in the UAE, another major international financial centre. We assess that a similar inherent vulnerability to this form of enabling activity is likely to exist in any country hosting a large, international finance centre.
Countries used to tranship physical items en route to countries with proliferation concerns	Aus PFNRA UN PoE UK PFNRA US PFNRA	**Transhipment Geographies** Transhipment can happen anywhere. However, typically those countries sharing a land or maritime border with a country with proliferation concerns, or major trade hubs in relative proximity to such countries, are most frequently cited in case studies as transhipment locations. **To Iran:** The UK PFNRA, within a case study on dual-use machinery shipments to Iran, states that "*the usual routing is through Turkey or the UAE*". It notes that the former's ease of movement of items from the UK and land border to Iran, and the latter's Freeport / free trade zone status, contribute to this. **To the DPRK:** The UK PFNRA notes that "North Korean front companies… often route shipments through **Liaoning** province in China". The Aus PFNRA similarly reports that "China is a conduit for sanctioned and smuggled goods into and out of the DPRK." A number of instances of the transhipment of physical items via Hong Kong are given by the UN PoE (transhipped to the DPRK) and the US PFNRA (transhipped to Russia and Iran). Please see the section below on "Ship-to-Ship Transfer Areas" for additional information on DPRK transhipment risk in maritime areas.
Countries with major manufacturing or supply sectors in	UK PFNRA US PFNRA	**Source Geography** The UK NPFRA states that "*The UK's role as a major arms manufacturer and supplier, as well as producer of dual-use items – such as nuclear related material –*

proliferation-sensitive items.		*increases the attractiveness of the UK to proliferation actors involved in these procurement networks*." Similarly, the US PFNRA concludes that "*industrial and technological factors also contribute to proliferation networks seeking to illicitly acquire goods from firms based in the United States*." It notes that the US has the largest defence sector in the world. We assess that a similar inherent vulnerability to being targeted by proliferation procurement networks as a source geography is likely to exist in any country with a major manufacturing or supply sector in proliferation-relevant items (see Section (1) Customers for relevant industries). National control frameworks, including export controls, act to mitigate this inherent vulnerability. Therefore, this factor is of most concern where a major manufacturing / supply sector for proliferation-sensitive items coexists with a weak framework for countering proliferation financing (see below).
Countries used to register, bank or operate front and shell companies	Aus PFNRA UK PFNRA UN PoE US PFNRA	**Enabling Geography** The UK PFNRA judges that "*Corporate registration [in the UK] can serve as a green flag for companies wishing to access the UK financial system and may allow proliferation-linked companies to access financial services in proliferation and PF-exposed countries*." The US PFNRA makes a similar point: "*PF networks often create multiple front or shell companies in the United States and third-country jurisdictions*." It notes that the recent implementation of the Corporate Transparency Act (CTA) will help to mitigate this risk in the US but points out that "only slightly more than half of countries have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial ownership or controllers of companies" and that even fewer meet FATF effectiveness requirements in this respect. The UK and US PFNRAs and the UN PoE reports all include numerous case studies featuring front and shell companies registered in, banking in or operated from a very wide range of countries. We assess that the vulnerability to being used to register, bank or operate front and shell companies exists across many countries, particularly those with weak controls over company registration. Many FIs already assess geographical vulnerability to shell and front companies with respect to money laundering and terrorist financing risk. We note that the shell and front companies highlighted in proliferation financing case studies share the same characteristics as those highlighted in case studies for other economic crimes case studies. This suggests that existing risk assessments may have significant utility in assessing jurisdictional vulnerability to shell and front companies involved in proliferation financing.
Countries used to register ships	US Adv	A sanctions advisory notice issued jointly by the US Department of the Treasury, Department of State and United States Coast Guard makes it clear that shipping "flag registries" are vulnerable to abuse by proliferators, highlighting techniques such as "flag hopping" (frequent changes of country of ship registration) used to avoid detection. We assess that a vulnerability to being used to register ships used in proliferation exists in countries with weak controls on their shipping registries.
Countries with weak frameworks for countering proliferation financing	FATF	FATF Mutual Evaluation Reports (MERs) can be invaluable in assessing countries' implementation and effectiveness of measures to counter proliferation financing, as part of the wider assessment of geographical PF risk. MERs may already feature in FIs' assessments of their geographical risk relating to ML and TF risks. [43] While Recommendation 7 and Immediate Outcome 11 are particularly relevant to assessing a country's counter-PF framework, many of the wider points within the MER process are also relevant to assessing PF risk even though they may not be

[43] FATF. "Consolidated assessment ratings". FATF, n.d. (Accessed 20 August 2024).

		expressly labelled as such (for example, those relating to beneficial ownership information (BOI) and DACs).
Ship-to-Ship Transfer Areas	Aus PFNRA UN PoE US Adv	The UN PoE reports and the US Advisory detail a number of maritime areas in the **East Sea** (also known as the **Sea of Japan**), the **Yellow Sea**, the **East China Sea** and the **Gulf of Tonkin** that have been noted for ship-to-ship transfer activity associated with DPRK sanctions evasion. The precise areas favoured are liable to change from time to time.

(3) Products or Services

The risk of PF through products is not dissimilar to many of the risk attributes of traditional ML/TF typologies. The key product assessment characteristics to consider for PF are as follows:

- **Cross-border nature:** Products and services supporting the trade in CBRN weapons, or other goods used to fund a proliferating state, are required to be functional across borders, especially since the settlement of such goods are predominantly in US dollars.
- **Limited self-disclosure requirements:** In tandem with the cross-border nature of a product, the movement of goods between jurisdictions with varying levels of disclosure requirements can be exploited by proliferators to hide the underlying purpose of a transaction. Products that enable the cross-border movement of goods or services may be at greater risk of encountering limited disclosure jurisdictions.
- **Complexity:** Proliferators will target complex transactional products, including those which make it easier to obfuscate beneficial ownership or to interpose third parties between them and the FI, to evade identification. The extent to which products allows payments, transfers or redemption requests from third parties or transactions to be undertaken on behalf of the customer's customer should be considered when analysing complexity.
- **Technologies:** Proliferators will look to exploit new and existing technologies. For new technologies, the lack of mature regulation such as in the Virtual Asset Service Provider (VASP) industry provides a route for proliferators to make payments and launder their proceeds. Conversely, as discussed below, the technologies used for vessel tracking can be manipulated to the point in which the control environment of a trade finance transaction can be compromised.

As noted above under Customer risk factors, the UK PFNRA distinguishes direct and indirect PF risks. From a product risk perspective, direct PF risks are typically related to financial products vulnerable to enabling the procurement of sensitive goods, services or training, or of sanctions or export controls circumvention by proliferating states. Indirect PF risks may arise from financial infrastructure which could be used as part of a wider network to enable PF activity, such as front or shell companies or intermediaries which can be used to obfuscate, for example, the true source of funds or the destination of the goods. This is why FIs should consider that a product that has the potential to be exploited for money laundering may be part of a wider PF risk.

PF – Trade Based Money Laundering and associated Financial Crimes risks

Trade Based Money Laundering (TBML) typologies exploiting trade finance services are well known to FIs and are the focus of UK authorities, as exemplified by an FCA “Dear CEO” letter on trade finance activity and the tightening of trade-based sanctions on Russia from its annexation of Crimea

through to the current war in Ukraine. [44] The UK Economic Crime Plan 2023-2026 supports the creation of a TBML Strategy.[45]

Trade finance creates a vulnerability to direct exposure to PF risk by potentially enabling the movement of:

A. Proliferation-sensitive items (including dual use items) to a proliferating state, or
B. Goods with the potential to raise funds to support a proliferating state's WMD programmes.

Well-known TBML risk factors, as outlined in several national risk assessments and the JMLSG Part II Sector 15 guidance on Trade Finance, are given in the table below, re-scoped to focus on the PF risk.[46] The table also indicates whether the risk attributed is most likely to be associated with scenario A. or B. as outlined above.

Transactional Factors	**Risk**	**Type A or B risk (see above)?**	**Comments**
Purpose	Dual-use goods	A	An instrument may cover a good which is listed on a dual-use/controlled goods list and therefore potentially subject to licensing. Such goods by their nature have both commercial and military (potentially including WMD) applications. Goods that are not listed on relevant export control lists but would otherwise be subject to "catch all" controls should also be considered.
	Vague goods description	A	Presentation of documents with vague goods descriptions. The MT/MX700 series will usually have a high-level description and/or abbreviation of the good covered. For atypical goods which do not have an alphanumeric identifier this is of particular risk when within the same categories as controlled goods (i.e. catch all). For example descriptions like "fan parts" or "bearings" do not provide enough information to ascertain whether they are controlled goods.
	Commodities and high value goods with state funding capacities	B	Several typologies involve the export of commodities and luxury goods to finance proliferation programmes. The UK PFNRA states that the UK could potentially act as a source of luxury goods that can be purchased for use by the DPRK in contravention of UNSC sanctions. The resale of these goods to affluent members of the DPRK population can generate revenue for the regime which can be used for proliferation purposes.
Structure	Physical Delivery Terms	A and B	**Ship-to-ship and transhipment/partial transfers**. When considered with customer type and geographical inherent risk factors, both of these shipping practices can present an increased risk of PF due to the potential for obscuring an overall movement of items to/from a sanctioned proliferating state.

[44] Edwin Schooling Latter; David Geale; Rebecca Jackson; Melanie Beaman. "Trade Finance Activity." The Financial Conduct Authority, September 2021. (Accessed 20 August 2024).

[45] HM Government. "Economic Crime Plan 2, 2023-2026". HM Government, 2023. (Accessed 20 August 2024).

[46] The Joint Money Laundering Steering Group. "15: Trade Finance". The Joint Money Laundering Steering Group, n.d. (Accessed 20 August 2024).

	Ongoing services and projects	A and B	Ongoing services, projects as well as the safeguarding of such initiatives until they have materialised are usually covered by guarantee or stand-by type instruments. While the underlying service or project may be established, covered with appropriate due diligence, at the point of instrument issuance, this does not cover any underlying invoicing for goods used for the ongoing services and projects (which could have dual-use applications).
Involved Parties	Indirect Relationship in Trade Finance and non-risk partaking roles	A and B	**Advising or confirming roles**: When an FI fulfils one of these roles, PF risks may be higher when: - The jurisdiction of the issuing bank is within the proximity of a proliferating state or; - The jurisdiction of the issuing bank is one at increased risk of being used to register, bank or operate front and shell companies. The advising/confirming FI may have limited due diligence on the issuing party. **Back-to-back:** It is key to understand the rationale for the issuing party should they request a back-to-back instrument. Although this is commonly and legitimately done to reduce the number of Letter of Credits (L/Cs) the customer would have to undertake for forward shipment and instead take the credit risk of the underlying exporter as its own, it should not be ruled out that the underlying exporter may be a proliferating actor attempting to remain anonymous. Typically, in these scenarios, the issuing bank will only have conducted CDD on their customer undertaking the credit risk, rather than the exporter in which the instrument is issued in the name of. This creates a "Correspondent Customer" type scenario, in which, without having conducted full CDD on the exporter, reliance is placed on the FI's customer's supplier/third party due diligence procedures, process and controls in order to mitigate the risk.
Geographical and Geopolitical factors	Ports of loading, discharge and territorial waters	A and B	Terms of delivery by which the goods will be delivered to a location in proximity to a proliferating state could be an indicator of potential transhipment and onwards movement to that state. Standby Letters of Credit where, at the point of issuance, there is limited or no indication of where the goods will be delivered will be riskier. For example, terms may include "*any port within X jurisdiction"* or "*any of the ports X/Y/Z"*
	Counterparty location	A and B	PF risks may be higher if the product enables trade with counterparties based in jurisdictions identified as having weaknesses in their AML/CTF, PF or sanctions regimes. Such weaknesses could indicate a lower degree of regulation and therefore less well embedded compliance among regulated sector participants, and voluntary compliance among other stakeholders.

Other financial products are more indirectly linked to the potential underlying movement of proliferation-sensitive goods or technologies. Where the nature or purpose of a product or service requires trust to be placed in a third party, such as another regulated FI, or in a regulated market and its participants (often in equivalent regulated jurisdictions), this puts an onus on understanding the PF policies, procedures, and controls of that third party. Although not a comprehensive list, below are some product areas in which PF risks should be considered:

- **Correspondent Banking (CB):** FATF notes that CB services "have been increasingly exploited by designated persons and entities as they often make use of international trade to conduct sanctions evasion activities".47 The US PFNRA similarly notes that "to disguise their activity as legitimate commerce, proliferation networks leverage corporate entities to gain access to financial services, including correspondent banking."48 FATF acknowledges that risk is not uniformly high in this area and recommends that "risk assessment of correspondent relationships should be done on a case-by-case basis, and should always take account of the internal controls and risk mitigation measures applied by the respondent bank."49

  Whilst the Wolfsberg Group's Correspondent Banking Due Diligence Questionnaire (CBDDQ) does not specifically have a policy, procedure and control section highlighting the institution's PF preventative measures, FIs should consider both the AML/CTF and sanctions sections holistically when determining whether the institution has an adequate counter-PF programme in-place (for example, customer and payment screening and monitoring).50 Further understanding can also be gained from the FI's business restriction policy. For example:

  - FIs which do not outline their stance on their involvement in the defence and/or munitions related sectors may present an increased risk of facilitating PF.
  - Evolving climate policies throughout the financial sector may lead to widespread and rapid changes in financing arrangements within the hydrocarbons sector. As hydrocarbon sales form an important part of the PF fundraising strategies of the DPRK (coal) and Iran (petrochemicals), this may lead to a shift in the risk profiles of correspondent banks with respect to this activity.

- **Cash products:** The UK PFNRA notes that DPRK embassies and diplomatic staff have been known to move physical cash and goods in diplomatic bags in violation of UNSCRs.51 Financial products that enable cash to be deposited into or withdrawn from the financial system, particularly in bulk, may therefore present greater risk to FIs of exposure to this activity.52 Additionally, FATF highlights that PF risk is heightened where a counterparty of a corporate customer that is a manufacturer or trading firm wishes to use physical cash for the purchase of industrial items (especially if these might be considered to be sensitive or dual use in nature), or

---

[47] FATF. "Draft Guidance on Proliferation Financing Risk Assessment and Mitigation (for public consultation)." FATF, April 2021. (Accessed 20 August 2024).

[48] The Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." The Department of the Treasury, February 2024. (Accessed 20 August 2024).

[49] FATF. "Draft Guidance on Proliferation Financing Risk Assessment and Mitigation (for public consultation)." FATF, April 2021. (Accessed 20 August 2024).

[50] The Wolfsberg Group. "Publication of the CBDDQ, FCCQ, Guidance, Glossary, and FAQs." The Wolfsberg Group, February 2023. (Accessed 20 August 2024).

[51] HM Treasury. "National Risk Assessment of Proliferation Financing." HM Treasury, September 2021. (Accessed 20 August 2024).

[52] *Ibid.*

for trade more generally where physical cash is not the normal medium of exchange.53 Oversight of cash-related risks can be further complicated when an FI is in an agency arrangement with a second FI that handles cash deposits/withdrawals on the first FI's behalf.

- **Capital Markets:** There are limited case studies highlighting the risk of PF through capital markets products. However, case studies pertaining to other risks such as TF can be illustrative of how a proliferator could use hedging activities, swaps and derivatives with an underlying physical asset as a way to exploit the financial system. Commodities such as hydrocarbons play a major part in funding the proliferation programmes of states such as Iran and the DPRK. Capital Markets products by their very nature remove the FI further from the oversight of the underlying commodity which is being traded, especially when executed on non-deliverable terms.
- **Insurance Industry:** The UK PFNRA highlights the maritime insurance and reinsurance industry as being at higher risk of PF.54 FIs may be indirectly exposed to a vessel through offering credit risk protection for a maritime insurer. As such, the FI does not have any direct due diligence means to mitigate any PF risk on the underlying asset. The FI buys non-payment insurance from the maritime insurer through a broker, which is used as collateral to offset the risk of one underlying syndicated/bilateral loans. The FI pays insurance premiums directly to the FI approved broker, who subsequently passes them (less their agreed brokerage fee) to an approved insurance company. The insurer will immediately reinsure this risk back to the relevant FI counterparty. There is no movement of funds between the FI and the insurer, unless the borrower defaults and a claim is made under the policy.
- **Receivables Purchasing facility:** Universities and higher education institutions face proliferation risks relating to research and development (R&D) on technologies which could be used for CBRN weapons or their means of delivery. The institutions appetite on its R&D can usually be found within its Research Code of Conduct/Ethics or equivalent document. The UK PFNRA states that increased levels of funding from overseas to British academic institutions makes the sector vulnerable to exploitation by states with proliferation ambitions, especially where there are links to CBRN-relevant research.55 FIs may support higher education institutions through Receivables Purchase instruments. The underlying receivables which an FI purchases could be anything from the installation of new computer systems, specific lab equipment or facilities which have the potential to be exploited by proliferating actors.

[53] FATF. "Guidance on Proliferation Financing Risk Assessment and Mitigation" FATF, June 2021. (Accessed 20 August 2024).
[54] *ibid*
[55] FATF. "Guidance on Proliferation Financing Risk Assessment and Mitigation" FATF, June 2021. (Accessed 20 August 2024).

(4) Transactional and Delivery Channel

The review of the sources listed within this document resulted in little information relating to potential PF risk factors relating specifically to *individual* transactions. While a transaction from a customer in a higher risk industry sector, using a higher risk product, to a higher risk jurisdiction might of course be considered to be a higher risk transaction, as might an aggregate large value or volume of such transactions, the relevant risk factors have already been noted under the respective customer/country/product sections above.

However, the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation notes a number of transactional indicators in which a *pattern* of transactional behaviour that may be indicative of proliferation financing.[56] For example: long periods of account dormancy followed by a surge of activity; financial transactions conducted in a circuitous manner or transactions that don't make commercial sense; sudden influxes of physical cash deposits by a customer where this would not be normal; or use of a personal account for transactions associated with industrial purchases.[57] We note that these could also be indicative of financial crimes other than PF. In general, our expectation is that patterns of transactions traditionally considered to be high risk for money laundering and other financial crimes, such as funnelling or pass-through payments, should similarly be considered as high risk for PF purposes. We have not identified any "uniquely PF" transactional pattern in our analysis of our sources.

Our sources reported little regarding delivery channels, and this form of risk factor may be one that could benefit from further research. Our expectation is that, in common with other financial crimes, PF risk will be relatively greater in those channels where there is greater separation between the FI and the customer. Hence, non-face-to-face channels may be higher risk than face-to-face interactions if appropriate risk mitigation is not in place, but in contrast, may be standard or even lower risk when effective risk mitigation is applied.[58] Similarly, operating via intermediaries, agents or other third parties may be higher risk than dealing directly with the customer.

Cross-Cutting Themes

Several risk factors do not fit neatly into a primary risk category of Customers, Countries or Geographic areas, or Products or Services, but rather cut across multiple categories. These are referred to under the appropriate headings above, but a more holistic analysis is offered below.

(1) Shell Companies

FIs will face the risks associated with shell companies directly (through a customer relationship with the shell company) or indirectly (through the shell company being a customer's counterparty, or through CB relationships). As discussed above, proliferating states make use of such entities to support all stages of their process. Proliferators seek to exploit the differences in the regulatory regimes of countries. Therefore, where shell companies may be established or misused with relative ease, the risks associated with PF tend to be greater. For instance, the UK PFNRA refers to the ease with which companies can be registered in the UK and the risks that this brings to the financial system,

[56] ibid

[57] ibid

[58] FATF. "Guidance on Digital Identity." FATF, March 2020. (Accessed 20 August 2024).

and the US PFNRA explains the vulnerabilities previously experienced due to the absence of a BOI reporting framework in the US prior to the recent implementation of the CTA.[59]

We note from wider experience of the use of shell companies by financial criminals that shell company risk frequently cuts across jurisdictional boundaries. A company may be registered in country A (where the proliferators perceive there to be a vulnerable company registration regime), have its bank account with an FI in country B (where the proliferators perceive there to be a vulnerable financial system in general, or perhaps a specific vulnerable FI), trade with counterparties in country C (perhaps where the items that it wishes to procure are produced or traded), all while the proliferators operating the shell company are physically located in country D.

Other red flags to consider relating to this risk factor are the incorporation date of a company, its trading history and any missing information about ownership. The case of Li Fangwei, commonly known as Karl Lee, provides an illustration of this risk.[60] Li is on the Federal Bureau of Investigation's most wanted list as a principal supplier to Iran's ballistic missile program. A network of hundreds of companies set up in offshore jurisdictions enabled Li to stay ahead of US Treasury sanctions by simply substituting a new, unknown company whenever one of his shell companies was designated, thus bypassing bank screening systems.[61]

(2) DACs / Cryptocurrency

The US PFNRA 2024 describes cyber-enabled PF as "The "new" digital evasion model".[62] The risks presented through DACs mainly arise due to two factors:

- **Cybercrime.** Proliferating states, particularly the DPRK, raise, launder and move funds using DACs. The DPRK's hackers have stolen DACs from a wide variety of victims in the VASP industry. To a lesser extent they have also extorted funds, in the form of DACs payments, via ransomware attacks. The victims of these can come from any industry. The US PFNRA offers a number of examples where stolen or extorted DACs were subsequently laundered through virtual asset mixer services to obfuscate their origin, destination and counterparties. While the 2022 US PFNRA stated that "*there is no evidence that a proliferation network has used a virtual asset to procure a specific proliferation-sensitive good or technology as an input to a WMD or ballistic missile programme*," it notes that DACs "*play an essential role in revenue generation and moving assets across borders*".[63] As most trade transactions continue to be conducted in fiat currency rather than DACs, our expectation is that proliferators are likely to

[59] HM Treasury. "National Risk Assessment of Proliferation Financing." HM Treasury, September 2021. (Accessed 20 August 2024).; The Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." The Department of the Treasury, February 2024. (Accessed 20 August 2024).

[60] U.S. Department of State. "Li Fangwei". US Department of State, n.d. (Accessed 20 August 2024).

[61] *ibid*

[62] The Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." The Department of the Treasury, February 2024. (Accessed 20 August 2024).

[63] The Department of the Treasury. "National Proliferation Financing Risk Assessment." The Department of the Treasury, February 2022. (Accessed 20 August 2024). https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf

convert their stolen or extorted DACs into fiat currency prior to using the funds for proliferation purposes.

- **Differing levels of regulatory scrutiny over the industry.** Jurisdictions around the world have been forced to adjust quickly to provide regulatory oversight of a new industry. Where regulatory scrutiny over the sector is lacking, vulnerabilities to sanctions evasion increases. Proliferating states could use these vulnerabilities to mask their role as the source of funds to obtain the materials required for WMD. For example, a proliferating state may purchase or sell digital assets from an exchange based in a jurisdiction with lax AML/CTF/PF controls and therefore hide their identity. By also using shell/front companies in other jurisdictions, the proliferating state may then procure the materials required for its WMD programme. FATF has published a status report on the implementation of FATF Recommendation 15 (new technologies) for jurisdictions with materially important VASP activity, which specifically references the risk of DPRK proliferation-related risks.[64]

Within their PF risk assessment and control framework, FIs may wish to consider the exposure presented by the use of DACs in two ways. Firstly, if their customer base includes VASPs, the PF risks associated with this should be assessed and mitigated. Secondly, non-VASP customers may be vulnerable to facilitating PF through their use of DACs. For example, a company which decides to meet a ransomware demand via a payment of DACs may in fact be providing funds that are subsequently used to resource an illicit WMD programme.[65]

Integrating Risk Factors into Risk Assessments

As noted at the beginning of this chapter, each FI will have its own risk assessment framework and remains responsible for deciding which of the above-identified potential PF risk factors their business is subject to and how best to integrate these factors into their frameworks. However, we note that these factors may be useful in informing risk assessment at several levels:

- **Country Risk Assessments.** Many FIs maintain models or other methodologies to determine the relative levels of FC risk inherent in different countries or jurisdictions. The potential PF risk factors identified above, particularly those in the 'Countries or Geographic Areas' section, may be useful to integrate into these models to reflect the PF dimension of country risk.
- **Product Risk Assessments.** Similarly, many FIs maintain models or other methodologies to determine the relative levels of FC risk inherent in their different financial products and services. The potential PF risk factors identified above, particularly those in the 'Products and Services' section, may be useful to integrate into these methodologies to reflect the PF dimension of product risk.

---

[64] FATF. "Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity." FATF, March 2024. (Accessed 20 August 2024).

[65] See, for example, UNSC. "Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)." UNSC, March 2024. (Accessed 15 October 2024) for reporting of DPRK-linked cybercriminals raising funds for ultimate use in supporting the DPRK's WMD programmes, including via ransomware attacks.

- **Customer Risk Assessments.** Many FIs maintain models or other methodologies to determine the relative levels of FC risk inherent in their customers. While we recognise that customer-level PF risk assessments are not mandated by the UK MLRs, such assessments may draw upon any of the potential PF risk factors identified above to reflect the PF dimension of customer risk.
- **Enterprise-wide/Business Wide Risk Assessments.** Many FIs maintain models or other methodologies to determine overall levels of FC risk inherent in their business, and potentially to segment this to determine relative levels of risk between different aspects of their business. Again, any of the potential PF risk factors identified above may be useful here to reflect the PF dimension of business wide risk.

While the factors in the customer, country and product risk sections may be useful when used separately, they can be more indicative of risk when used in combination. So, for example, a customer in a high-risk business sector, operating in a high-risk country, using high risk products and services, accessed through a non-face-to-face delivery channel may be considered higher risk than a customer meeting only one of these criteria.

Chapter 3: Bank Control Framework

Introduction

This Chapter shares the approaches taken by many FIs to mitigate and manage their PF risks across their control framework. This chapter examines approaches to the following aspects of PF related controls:

1) Application of PF Typologies;
2) KYC and CDD;
3) US Bureau of Industry Security Lists Screening and Alert Handling;
4) Transaction and Name Screening; and
5) Goods Screening Methods and use of Goods Lists.

FIs have adopted a range of approaches to address PF risk depending upon the size and nature of their business, their risk appetite, application of a risk-based approach (where applicable) and an understanding of the regulatory requirements applicable to them. In many cases PF controls rest upon existing AML or sanctions controls, particularly KYC, CDD, screening and alert handling. AML and sanctions controls frequently address PF risk factors negating the need to implement bespoke solutions. Whilst this creates efficiencies there are consequences such as a difficulty in producing PF specific MI. Considerations of whether, and if so how, to address the various lists of dual use goods in an FI's control framework also present ongoing challenges for many FIs.

FIs are required to have policies setting high-level requirements relating to the management of PF risk, supported by more detailed procedures. These do not necessarily need to be standalone documents dealing exclusively with PF risk but rather may be integrated within related, wider policies (e.g. Financial Crime, AML or Sanctions Policies) where appropriate. Due to overlaps with AML and Sanctions requirements (such as sanctions name screening or KYC/CDD) the need for standalone PF policies and supporting documents may be diminished but, whatever approach is adopted, a FI needs to understand how its policies and supporting documents address PF risk. In determining their policy requirements relating to PF, some FIs have undertaken a stock-take of their existing FC controls following a PF risk assessment (or consideration of PF risks within a broader FC risk assessment) to understand where existing controls address PF risks or where there are policy gaps that need to be addressed.

Beyond sanctions name and transaction screening, developing effective controls to mitigate and manage PF related risk requires examination. This paper includes examples of how FIs have adapted their wider control framework to counter the risk of PF. However, poorly conceived ideas of what FIs can realistically do to identify PF related activity, such as transaction screening using dual-use goods lists which were produced for other purposes, risk creating cumbersome and ineffective control requirements that could harm the endeavour to counter PF.

(1) Application of Proliferation Finance Typologies

PF typologies can be used to identify certain patterns of behaviour that indicate the raising of funds for an illicit WMD programme or the procuring of technology and goods for it. To enable FIs to determine what measures they need to mitigate the risks of PF, the specific risks need to be properly understood. Provision of typologies and their associated indicators (also known as red flags) in academia and industry guidance can be used to assist in identifying the threats posed. FIs may have processes in place to identify these typologies in customer activity through their control frameworks and risk assessments.

Following the 2008 FATF typologies report, FATF produced a working definition on PF in 2010[66] which refers to financial support with the activities required to develop a WMD programme such as manufacturing, acquiring, development, export, brokering and transport activities on nuclear, chemical and biological weapons. [67] The majority of work undertaken to counter the proliferation of WMD is not focused on the weapons systems themselves, but on preventing the supply of the underlying technologies, goods and materials required by a WMD programme. It is identifying those component goods and materials that is a substantive challenge. This is where a broad range of industry and academic-identified typologies become useful for an FI as the typologies will assist in identifying realistic scenarios of proliferation-related fundraising activities and the acquisition of underlying technologies, goods and materials. Where these scenarios are seen in transaction monitoring and customer reviews and are not indicative of the types of behaviour one would expect to see from the customer in question appropriate risk mitigation steps can be taken.

As with other FC types, there are challenges in being able to identify and combat PF as certain behaviours and transactional patterns can potentially be indicative of legitimate activity when considered in the context of the customer relationship and their business practices. Identifying certain typologies that are indicative of illicit behaviour is therefore essential to distinguish between illicit activity and legitimate business. FIs can optimise their control frameworks by incorporating consideration of these typologies into the design of their controls such as KYC and due diligence processes, transaction monitoring or proactive monitoring, proactive lead-generation exercises, FC investigations (including internal and external reporting) and training programmes.

Dr Jonathan Brewer's King's College London report on the "Study of Typologies of Financing of WMD Proliferation" (KCL report) suggests that as indicators can reflect other financial crime or legitimate activity, to narrow identifying a large number of "false positive" identifications, FIs can then weight the typologies depending on the FI in question, the customer base, its geographical footprint and whether some indicators are applicable at different stages of a financial transaction cycle.[68]

The KCL report also identifies that typologies need to constantly develop to capture modern and evolving FC risks associated with newer technologies such as digital currencies and cybercrime opportunities.[69] An FI will need to adapt to change, aligning with the regulations and understanding

---

[66] FATF. "Combating Proliferation Financing: A Status Report on Policy Development and Consultation". FATF, February 2010. (Accessed 20 August 2024)

[67] FATF. Proliferation Financing Report. FATF, June 2008. (Accessed 20 August 2024).; FATF. "Combating Proliferation Financing: A Status Report on Policy Development and Consultation". FATF, February, 2010 (Accessed 20 August 2024).

[68] Dr Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation". King's College London, October 2017. (Accessed 20 August 2024).

[69] *ibid*

developments in technology that may be of relevance to PF. The KCL report included typologies that have been updated and supplemented based on insights from several states and FIs. The 60 case studies contained within the report included a large number relating to sanctions evasion without the direct nexus to PF activity being made explicit, highlighting the complexity. The updated FATF Guidance on Counter Proliferation Financing published in 2018, containing further information on typologies, and the FATF June 2021 Guidance on PF Risk Assessment and Mitigation, contained updated indicators.[70] The information and guidance in these can help FIs to understand the typologies related to PF and apply these in the design, or enhancement, of their control frameworks.

(2) Know Your Customer and Customer Due Diligence

PF typologies may assist in defining CDD/KYC requirements to identify specific indicators of PF risk where present.. However, the relevance, or applicability, of indicators drawn from the typologies will depend on the type of FI and the products and/or services it may offer.

In defining the CDD/KYC controls required at onboarding and ongoing due diligence, FIs may utilise either the outcome of the existing inherent risk assessment or a stand-alone PF risk assessment. The FI can determine where specific PF and or FC controls, such as enhanced due diligence, are required. This allows an FI the ability to deploy additional controls where appropriate and based on a perceived/known risk. FIs can utilise relevant PFNRAs and other useful information such as FATF guidance to determine their approach.

Customer identification, verification, and levels of CDD/KYC is undertaken at onboarding and refreshed periodically or whenever certain triggers are met. The degree and level are dependent on the customer / industry e.g., trade finance, individuals, commercial businesses and the products or services they require based on a risk-based approach. This is usually undertaken to encompass all FC risks e.g., sanctions, AML, fraud. The FI will typically deploy real-time screening controls which can assist in the identification of customers who are of a higher risk or prohibited (such as sanctioned parties). For Retail customers, CDD/KYC is typically captured without any specific PF questions being asked, beyond determining any linkages to sanctioned countries such as Iran and DPRK. Customers within trade finance or commercial business banking will face a different approach to CDD/KYC with questions covering all aspects of FC risk. Specific business, industry or trading questions will be asked to allow FIs to understand the customer's business based on their industry. FIs may use this information to assign the customer in their internal systems using specific industry codes (to either internal bespoke or UN, US or EU standards). The FI will also gather a greater level of expected activity information and in some instances, an understanding of payments expected to and from the account, including the countries involved, supply chains and some knowledge of the customer's customers (typically names, account details, locations and transaction volumes with the customer). This can be used to understand if there are any high-risk indicators, or red flags, to industries and/or activity that may present PF risks. These could include:

- customer reluctance to provide information, being vague or omitting information;
- connections to a country of proliferation or diversion concern;

[70] FATF. "FATF Guidance on Counter Proliferation Financing". FATF, February 2018. (Accessed 20 August 2024).; FATF. "FATF Guidance on Proliferation Financing Risk Assessment and Mitigation". FATF, June 2021. (Accessed 20 August 2024).

- customer is dealing with dual use goods;
- complex trade deals;
- customer counterparties links with dual use goods, countries of proliferation or diversion concern; or
- links to sanctioned countries or parties.

Red flags may be associated with more than one risk type e.g., sanctions and PF risk. Some FIs may also put in place specific PF risk questions at the onboarding stage. There is no uniform method or approach that has been universally adopted by FIs.

Some FIs may onboard the majority of their customers in a non-face-to-face environment due to their particular business model. This may pose significant barriers and complexity in their ability to collect the relevant information from customers in a manner proportional to the risk that they present. FIs may use industry codes to help classify customers, which can prompt sets of PF related questions such as the exact technology or equipment the customers produce or distribute and what trading countries an FI might expect to see. Such information might be captured in risk assessments or other due diligence documentation.

Some FIs may be limited in their ability to identify specifically PF risk through the capture of CDD/KYC at onboarding as the existing high-risk indicators may not lend themselves to identify PF risk alone without additional information. Some FIs may identify generic FC risks at onboarding through known, well established "modus operandi" for the likes of sanctions and AML, and these can help to protect against PF risk. Publicly available information on typologies, such as the KCL report, can be utilised to inform an approach on appropriate controls. However, for new customers, the FI will have limited experience of them, their business and expected activity. Thorough CDD should set a baseline understanding of the customer for assessing their risk and applying an appropriate control framework.

The approach taken by the FI will largely depend on the customer type. It is difficult to deploy a ‘one approach fits all’ framework when the highest risk may only be identifiable within trade finance or another commercial customer offering. Even then challenges will remain. For example, identifying customers trading in dual-use goods, beyond customer declarations, would require in-depth expertise or knowledge of such items. Identifying PF risk during onboarding may be easier for those FIs that undertake screening by using customer data collected during the product/service process and screening against agreed external and internal lists such as UN, Office of Foreign Assets Control (OFAC) and OFSI sanctions lists and adverse media to identify parties subject to sanctions.

FIs may, where proportionate, selectively deploy additional controls at onboarding or choose to deploy further targeted controls during the customer lifecycle in line with a risk-based approach. These controls could include:

1) ongoing transaction reviews on a deal-by-deal basis either within the trade finance control environment due to use of trade finance instruments or triggered by additional credit lines; or
2) retrospective account activity reviews on a periodic basis to identify whether actual account activity remains in line with expected account activity and whether there are any red flags, including those associated with PF typologies. This may be a mandatory requirement in certain jurisdictions under specified circumstances.

The controls can then focus on the risk of the activity being undertaken. Consideration on the need and timing of additional controls can be based on multiple factors such as: the jurisdiction(s) where the customer is based, where the customer operates and the products and services provided, basing

their decision on the holistic perceived and informed risk. Some FIs may choose to take a differing risk-based approach to their onboarding control environment based on their risk assessment(s).

For FIs that provide trade finance products or commercial products and services there is sometimes the opportunity to include an additional feature of either enhancing existing sanctions or AML questionnaires with PF related questions or implementing an in-depth PF specific questionnaire in addition to the routine CDD/KYC conducted at on-boarding. For FIs providing trade finance and or commercial products and services there may be a prohibitive and or restrictive risk appetite in accepting customers dependent on their involvement in certain activity e.g. the defence sector. Additional due diligence will be required to determine the customer's involvement in these sectors. FIs may choose to create bespoke processes or adopt those offered by the likes of the Wolfsberg CDD questionnaire to support the additional CDD/KYC required.[71]

Comparing the defence sector with dual-use goods manufacturers highlights some of the challenges in identification of PF risk. Customers primarily operating in the defence sector are relatively easy to identify given the often overt and single use of much military hardware, whereas traders in dual-use items may be very challenging to identify with expertise required to distinguish dual-use goods from benign items. Whilst 1LOD and 2LOD teams can be trained to identify PF activity, identifying a PF angle solely due to the goods would be challenging due to the huge numbers of dual-use items and the technical specifications of many of them requiring specialised expert analysis. Such expertise would not ordinarily be found in an FI and will also likely not be readily available externally. As the joint Wolfsberg Group, International Chamber of Commerce (ICC) and Bankers Association for Finance and Trade (BAFT) paper on trade finance stated, expecting FIs to attempt to identify dual use goods might require them to replicate the expertise of specialist scientific research institutions – something which is clearly impracticable.[72]

When it comes to ongoing CDD/KYC, FIs have the added advantage of already banking the customer and the ability to understand their activity and transactional behaviour, linking possible transactional risk/activity risk or links to known PF actors. The use of dynamic risk driven reviews will allow FIs the ability to update and capture ongoing CDD/KYC on a risk-based approach. These may not be specific to PF risks/high risk indicators alone but could be identified via other FC concerns (e.g. where the use of cover or front companies is identified this could conceal a proliferation angle).

Where risk is identified through other FI deployed frameworks such as transaction monitoring or screening, FIs might be able to use these to gather additional data to give a greater understanding on the perceived risk of the customer to their organisation. This should enable an informed decision on the customer and their activity to determine when and how much ongoing CDD/KYC is required, enhancing the ability to detect PF occurrences. External or internal threats and high-risk indicators data will develop over time, allowing FIs to react and deploy changes to their onboarding and ongoing customers CDD/KYC controls based on known typologies.

Many customers who are at a heightened risk of involvement in PF-related activity may not themselves be consciously or intentionally involved. Often, innocent-but-vulnerable companies may

[71] The Wolfsberg Group. "Publication of the CBDDQ, FCCQ, Guidance, Glossary, and FAQs". The Wolfsberg Group, February 2023. (Accessed 20 August 2024).

[72] 'The Wolfsberg Group, ICC, BAFT. "The Wolfsberg Group, ICC and BAFT Trade Finance Principles, 2019 amendment". The Wolfsberg Group; ICC; BAFT, 2019. (Accessed 20 August 2024).

be targeted by covert procurement networks to supply dual-use goods, ostensibly for legitimate purposes. The goods are then subsequently diverted to illicit use. For this reason:

1) some ('intentionally bad') PF risk customers may attempt to deceive FIs during CDD, whereas others, who have been unwittingly exploited may be perfectly honest during CDD – an FI needs to account for both types in its PF controls; and
2) for selected customers (risk-based again), an FI may need to understand the customer's own compliance / controls framework e.g., if they operate in the defence industry or supply dual-use items, how do they vet their customers and what controls do they have in place to monitor their supply chain?[73]

CDD/KYC for an FIs customers can be an effective control for detecting PF concerns in an FI's own customers and Enhanced Due Diligence (EDD) can be applied to transactions; however it is not proportionate or practical for an FI to replicate the same level of customer CDD on a transactional level for non-customers, counter-parties, and other related parties. If this were attempted, it is likely that payments would simply be re-routed to avoid such scrutiny. It would also be likely to cause extensive delays whilst RFIs were issued to obtain the information. More importantly, in the absence of any specific concern it is highly unlikely that the transaction would alert in the first place meaning that an FI would not find itself in the position of being able to request such information in any case.

(3) US Bureau of Industry Security Lists Screening and Alert Handling

The Bureau of Industry and Security (BIS)[74] within the US Department of Commerce has as its stated mission to "advance US national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued US strategic technology leadership."[75] It goes on to state that *"…in the area of dual-use export controls, the Bureau will vigorously administer and enforce such controls to stem the proliferation of weapons of mass destruction and the means of delivering them, to halt the spread of weapons to terrorists or countries of concern, and to further important US foreign policy objectives. Where there is credible evidence suggesting that the export of a dual-use item threatens US security, the Bureau must act to combat that threat*."[76] BIS is directly relevant, therefore, to considerations of PF, particularly where there is a US Nexus.[77]

---

[73] Recent actions in respect of Executive Order 14114 and OFAC enforcement actions against corporates have heightened the focus on companies control over their supply chains.

[74] Subsequent to the drafting of this paper, BIS published a 'New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations' on 9 October 2024. https://www.bis.gov/media/documents/guidance-financial-institutions-best-practices-compliance-export-administration (accessed 10 October 2024).

[75] The Bureau of Industry and Security (BIS). "Mission Statement" U.S. Department of Commerce – Bureau of Industry and Security, n.d. (Accessed 20 August 2024).

[76] *ibid*

[77] OFAC. "11. Who must comply with OFAC regulations." OFAC, January 2015. (Accessed 20 August 2024).

In furtherance of its stated aims BIS is responsible for four "Lists of Parties of Concern" (below).[78]

1	**The Denied Persons List**	Individuals or entities which have been denied export privileges.
2	**The Entity List**	Non-US Parties presenting risks of diversion to WMD programmes, terrorism, or activities contrary to US national security and/or foreign policy interests.
3	**The Unverified List**	Parties whose details BIS has been unable to confirm.
4	**The Military End User List**	Non-US Parties determined to be military end-users.

These four lists are available on the BIS website and are typically to be used in tandem with the Export Administration Regulations (EAR) to understand the restrictions applicable to the entity listed and the relevant licensing requirements which might apply to them in a particular context[79].

The EAR[80]

§ 734.3 ITEMS SUBJECT TO THE EAR

(a) Except for items excluded in paragraph (b) of this section, the following items are subject to the EAR:

(1) All items in the United States, including in a U.S. Foreign Trade Zone or moving in transit through the United States from one foreign country to another;

(2) All U.S. origin items wherever located;

(3) Foreign-made commodities that incorporate controlled U.S.-origin commodities, foreign made commodities that are 'bundled' with controlled U.S.-origin software, foreign-made software that is commingled with controlled U.S.-origin software, and foreign-made technology that is commingled with controlled U.S.-origin technology:

(i) In any quantity, as described in § 734.4(a) of this part; or

(ii) In quantities exceeding the de minimis levels, as described in §§ 734.4(c) or 734.4(d) of this part;

(4) Certain foreign-produced "direct products" of specified "technology" and "software," as described in §734.9 of the EAR; and

NOTE to paragraph (a)(4): Certain foreign manufactured items developed or produced from U.S.-origin encryption items exported pursuant to License Exception ENC are subject to the EAR. See § 740.17(a) of the EAR.

(5) Certain foreign-produced products of a complete plant or any major component of a plant that is a "direct product" of specified "technology" or "software" as described in § 734.9 of the EAR.

Being listed on one of the BIS Lists does not, in and of itself, prohibit other parties from transacting with the listed party. The restrictions are limited to the specified licensing prohibitions or requirements. Typically, a US Person would need to request a licence from BIS to transact in items subject to the EAR where these are to be supplied to a party on, for example, the Entity List. A presumption of denial would be expected for all licence requests where the goods being exported are subject to the EAR.

[78] The Bureau of Industry and Security (BIS). "Lists of Parties of Concern." U.S. Department of Commerce – Bureau of Industry and Security, n.d. (Accessed 20 August 2024).

[79] Bureau of Industry and Security. "Introduction to Commerce Department – Export Controls." U.S. Department of Commerce – Bureau of Industry and Security, November 2018. (Accessed 20 August 2024).

[80] Code of Federal Regulations. "15 CFR 734.3." National Archives and Records Administration, August 2024. (Accessed 20 August 2024).

The BIS Lists and additions to them have increasingly derived from current US foreign policy and related actions beyond a narrow focus on export licensing restrictions.[81] This has increased the focus for FIs and raised questions as to whether and how these lists should be incorporated into their FC controls. The lists are offered by screening list vendors and can be incorporated into an FI's screening controls. Determining the actions once an alert has been generated is not necessarily straightforward due to determination of a US Nexus to the activity and subsequently considerations as to the applicability of EAR requirements for example.

BIS List Transaction Screening – An FI may determine that it will decline all transactions where an alert has been confirmed or subject them to some form of review. A transaction generating an alert may be a trigger or red flag for further investigation into the goods being traded, who the counterparties are and possibly checks on whether the appropriate licence is in place for the supply of the goods. This can be further complicated by the lack of a US Nexus to the transaction for example, where screening generates an alert against the BIS lists, but both the remitter and beneficiary are outside of the US and goods are not being shipped through or via the US. In such instances payment may be made in US dollars (including through the US financial system) but where there is no other US nexus to the transaction the parties would be unable to apply for a licence from BIS, meaning that questions around export licences may not be applicable. Where the goods being traded are clearly not subject to the EAR, there may be unnecessary or extended reviews of transactions. This is often due to unfamiliarity with the requirements of the EAR by FIs and a reluctance to approve a transaction where they know that there is a concern around the customer or counterparty. Examples of this include where the export of goods subject to the EAR has been restricted for a certain entity but that entity has a significant business trading in items which are not subject to the EAR. An FI may struggle, due to its lack of familiarity with US export control requirements, in distinguishing between such items, causing lengthy delays or unnecessarily declined transactions.

BIS List Customer Name Screening – An alert generated where a customer is involved could trigger a CDD review of the relationship. This might explore the nature of the goods traded, the customer's counterparties and whether any of these are located in, or provide services to, sanctioned countries. Depending on the concerns their listing by BIS creates, an FI may determine to exit the relationship or, if the customer relationship is to be maintained, apply EDD measures.

The expansion in the application of the use of the Entity List beyond its initial focus to broader US foreign policy objectives means the utility of referring to a listing as a possible indicator of PF concern has lessened. Nevertheless, the list may, if examined on a listing-by-listing basis, indicate whether a particular actor has been added to the BIS lists for a proliferation related concern. The Unverified List, for example, may seem of lesser direct relevance to PF risk since a reason for listing may be due to an inability to establish contact with the entity, however it is the reason *why* BIS decided to contact the entity which in itself may be the cause of concern.

[81] Tanner J. Wadsworth. "'Contrary to National Security': The Rise of the Entity List and Individualized Export Controls." Columbia Journal of Transnational Law, November 2021. (Accessed 20 August 2024).

(4) Transaction and Name Screening

Augmenting Controls and other checks

PF controls falling within transaction and name screening are primarily designed to prevent and/or mitigate the circumvention of sanctions regimes, whether these are local/national or applied globally (e.g. UNSCRs). Sanctions name screening is a fundamental aspect of any PF control framework and it is covered in Part II of the JMLSG Guidance. Paragraph 15.49 explores real time screening and the possibility/feasibility of FIs screening against those entities/individuals designated for both financial crime reasons and proliferation concerns. [82] Name screening is also covered in the FATF 2010 report: *Combating Proliferation Financing: A Status report on Policy development and consultation*.[83] Paragraphs 71, 72 and 92 contain similar messages to the JMLSG guidance in respect of FIs utilising real time screening and lists of entities as part of their PF programmes.[84]

Name screening is an important control however, industry-wide screening means that named proliferators are no longer able to transact freely using their real identities and instead must operate through cover or front companies or trusted associates. This results in most of the individuals involved in PF activity being far removed from the entities and listed parties known to FIs as being sanctioned, by the UN, for their involvement in WMD programmes in nations such as the DPRK and Iran. Consequently, screening largely defends only against undisguised attempts to conduct financial activity by designated parties. Even where an alert is generated, a PF angle may not be apparent unless the designation is expressly for PF reasons. Paragraph 15.50 of the JMLSG guidance part II also cautions against the unintentional consequences of treating all lists as financial sanctions lists, which may result in an FI prohibiting all business with the listed entities and jurisdictions.[85] The BIS Lists may be applied in such a way by an FI, where instead of checking against the requirements under the EAR, all dealings are deemed to be prohibited. Where an alert results in funds being frozen (or blocked in US parlance) and compliance with sanctions freezing mechanisms may take precedence over any exploration of potential PF risk.

Where proportionate under the risk-based approach, FIs may consider targeted reviews of historical transactions where there has been a true match. FIs may use retrospective screening or proactive 'look-back' investigations to identify designated individuals and entities trading and/or transacting prior to being sanctioned. Such investigations allow the FI to identify non designated counterparties who may be exposed to PF related activity. Where FIs have undertaken proactive investigations, they have looked back over time to identify the point at which the individual/entity became subject to sanctions to identify counterparties, the extent of the exposure and whether any parties' transactions with the individuals/entity have subsequently been designated for PF reasons.

---

[82] The Joint Money Laundering Steering Group. "Prevention of money laundering/combating terrorist financing, 2023 Revised Version, Guidance for the UK Financial Sector, Part: II Sectoral Guidance."https://www.jmlsg.org.uk/wp-content/uploads/2023/09/JMLSG-Guidance-Part-II_June-2023_revised-Sept-2023.pdf The Joint Money Laundering Steering Group, September, 2023. (Accessed 20 August 2024)

[83]https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf FATF. "Combating Proliferation Financing: A Status Report on Policy Development and Consultation". FATF, February 2010. (Accessed 20 August 2024).

[84] *ibid*

[85] The Joint Money Laundering Steering Group. "Prevention of money laundering/combating terrorist financing, 2023 Revised Version, Guidance for the UK Financial Sector, Part: II Sectoral Guidance." The Joint Money Laundering Steering Group, September 2023. (Accessed 20 August 2024)

PF Specific Alerts

Currently, name screening systems generate hits on listed individuals/entities but does not categorise or label these according to the reason for their designation (PF, terrorism, human rights abuses, organised crime etc). Rather, alerts are flagged as a Specially Designated National (SDN) alert or similar: categories that cover multiple underlying crimes or national policy drivers. Sometimes the specific sanctions regime under which the designation was made implies PF-relevance (e.g. the Non-Proliferation of Weapons of Mass Destruction (NPWMD) list). Other times it is more challenging to know whether a given designation ought to be considered as proliferation-relevant or not (e.g. individuals/entities listed under various "Iran" designation regimes may include, but not be limited to, those with a proliferation-relevant reason for designation). This is compounded when also considering that PF-relevant alerts may be generated from non-sanctions lists e.g. non-designated parties mentioned in UN PoE reports or internal screening lists (e.g. where an FI has noted a non-designated entity as having previously transacted with a subsequently-designated party, this might be added to an internal 'grey list'). Therefore, while screening controls generate, assess, escalate and mitigate alerts on subjects designated for PF-reasons. Addressing this would require FIs undertaking systems changes at the back end to enable tagging to PF and vendors providing lists in a format which will enable the tagging to be done easily. The majority of UK Finance member FIs do not currently possess the capability to automatically tag a subset of these as "PF Alerts".

Similarly, internal investigations carried out by FIs, whether triggered by a screening alert or by a different form of detection control, often involve multiple FC categories. PF cases frequently overlap with sanctions, export controls or AML concerns.

PF cases may also involve sanctions and/or AML concerns, meaning that a single case might fit multiple FC categories. Identifying the SDN as being linked to PF designations might require a close review of the underlying entry or tagging the alert entry to PF. In the absence of either of these, funds for a PF linked entity may be frozen but the linkage back to PF would not be identified and no MI on PF cases would be generated. Screening against other lists, such as non-designated parties mentioned in UN PoE on DPRK reports or against internal lists (e.g. where an FI has noted a non-designated entity as having previously transacted with a subsequently-designated party, this might be added to an internal 'grey list') would face similar challenges with tagging to PF. Whilst an entry might contain such details the narrative instruction would need to provide some guidance on how to consider potential PF related risks and also how to dispose of the alert. Operationalisation of such entries may be harder for live transactions compared to post-transaction monitoring or investigations.

Some investigative case management systems are constrained in their abilities to tag one case with multiple FC categories or to generate MI that accounts for these overlapping categorisations. Tagging internal investigative cases as PF-relevant may also assist staff who file Suspicious Activity Reports (SARs) / Suspicious Transaction Reports (STRs) in applying the appropriate tags or labels to those reports to highlight their PF-relevance to authorities.[86]

Challenges with tagging alerts, investigations and SARs/STRs as PF-related may result in a corresponding lack of PF MI. If PF MI was available on alerts, internal investigations and external reports, senior management would have visibility on PF related cases rather than the situation in which such risk is subsumed within sanctions or AML MI without any further identification. Tagging to

[86] E.g. the UK National Crime Agency (NCA) requests that glossary code XXPCPXX is applied to SARs relating to Counter-proliferation. NCA. Guidance on submitting better quality Suspicious Activity Reports (SARs). June 2023. (Accessed 14 October 2024).

PF would allow for controls to be adjusted or enhanced based on PF MI supporting such changes. Some FIs are investigating the work that will be required to enhance systems to provide this capability. This is likely to involve extensive system changes including 'back end' work to create multiple tags, flags and/or alerts (covering Sanctions, AML and PF concerns as a minimum) and is likely to be complex and will take time to complete. Any changes would only be effective if done in tandem with changes to the list feed from the vendor .

System Changes Implications

Whilst it is possible for sanctions lists to be flagged and/or linked to PF rather than other sanctions or FC tags, this would require investment in systems changes. Any assessment of proposed system changes will focus on whether the proposed changes could be addressed through alternative options, such as manual reviews of alerts generated and PF SARs submitted. In making such a determination, an FI will have to consider and assess the proportionality and effectiveness of any proposed system changes, and whether alternatives, such as manual reviews, would be genuinely effective. In addressing PF concerns FIs need to leverage their existing AML/CTF and sanctions control processes to best advantage and to mitigate against the risk of creating costly stove-piped categorisations of FC risks and corresponding processes.[87] Proper calibration and leveraging of existing FC processes and controls can be used to address PF risks. A bespoke assessment comparing assessed relevant PF risks against an FI's existing FC controls is one way of justifying utilisation of existing controls and identifying any such gaps that will require additional investment. The absence of such an assessment may lead to consequences due to poorly understood and articulated PF risks, such as inadequate alert generation, too many false alerts or alerts not being generated.

Where systems investments are required, an FI will want to understand the implications of such changes and the likely number of alerts that it can expect to be generated. They may deploy a sandbox to test the new controls against historic data in making that assessment. This can then be used for tuning of screening tools and planning staffing requirements against the expected number of alerts requiring human intervention. Correct assessment of PF risks is therefore critical in ensuring resources are adequate for filtering false alerts and addressing those appropriately identified. If PF specific MI was available to report the number of alerts and the outcome of investigations into these, senior leaders would have visibility on the number and type of PF related cases.

The benefit of PF specific MI would be that controls could be adjusted or enhanced based on the information produced in the MI supporting any such changes. If changes to systems are to be adequately justified, the ability to extract PF-related MI would need to be prioritised in order to accurately identify and report the number of PF alerts and triggers generated and subsequently worked.

[87] UK Regs on PF also speak to the expectation that FIs can utilise their existing processes when addressing PF.

(5) Goods Screening and use of Goods Lists

Goods screening refers to the screening of payment messages and other documentation, such as bills of lading or letters of credit, that an FI may have in its possession against lists of goods – typically the dual-use goods that comprise the strategically controlled goods listed by the international control regimes: the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), the Australia Group and the Wassenaar Arrangement (the goods lists).[88]

These goods lists are designed for specialist analysis by experts or exporters and were not intended for the use of FIs in their controls. Consequently, FIs have adopted various approaches to these goods lists, creating their own bespoke lists of key items using terms that lend themselves to screening or referring to the goods regime lists on an ad hoc basis.

When approaching referral to the goods lists there is no single solution or approach that FIs have adopted. Goods screening has limited effectiveness in isolation, and a variety of approaches will be appropriate dependent on the specific circumstances of FIs.

Use of the Goods Lists

FIs cannot approach goods screening in the same manner as a sanctions list, due to the lack of in-depth details on goods provided in transaction messages and documentation, unlike the names of counterparties involved mandated under FATF Recommendation 16 requirements.[89] The UK and EU goods lists are primarily consulted as reference documents. This use of these lists is not implemented as a specific PF control but is rather usually used as part of existing sanctions and AML/CTF controls. Some FIs have created their own bespoke or internal lists of dual-use goods to be checked as part of customer assessments. Such lists may be applied as part of a risk-based application against products and industries that present heightened risk, such as in trade finance investigations and a port of loading/discharge being based in a known PF hotspot. These lists are consulted manually on a case-by-case basis through eyeball checks and not screened. Specific goods that present heightened risk may be shared for awareness and education (for example, from the National Crime Agency or law enforcement alerts) to increase the knowledge of FI staff and enable them to identify some dual use goods. Given the great number and specialist nature of such items this can only be on a best-efforts basis. Where FIs have utilised information from Schedule 2 of the Export Control Order (2008) and the dual-use goods detail taken from Annex 1 of the EU Regulations to create an internal list these have been created utilising key words to screen against, though this practice is not widespread or established and the effectiveness is unproven.

[88] NSG; The Missile Technology Control Regime. “Annex Handbook”. The Missile Technology Control Regime, 2017. (Accessed 20 August 2024).; The Australia Group. “Australia Group Common Control Lists”. The Australia Group, n.d. (Accessed 20 August 2024).; The Wassenaar Arrangement. “Control Lists.” The Wassenaar Arrangement, December 2023. (Accessed 20 August 2024).

[89] FATF. “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. FATF, 2012-2023. (Accessed 20 August 2024).

Ongoing Challenges

Three key challenges with goods screening are that:

1) most financial transactions (non-trade finance or open account trading) do not contain the detail of the goods that would be required to screen;
2) there are multiple potentially relevant goods lists, none of which have been formulated for goods screening; and
3) whilst manufacturers, exporters are experts in the specific products, technologies and services they produce and export and the requirements around export controls, even if the data was available, FIs could not realistically be expected to have the same level of technical understanding of all the potential uses of all types of items across all relevant sectors and industries.

A large proportion of global trade is completed through open account trading and not trade finance products. The bulk of PF risk associated with trade activity likely involves open account trades. Unlike trade finance, where documentary information about the traded items is available, open account trades lack information around the items being traded. Most of the discussion around utilisation of HS codes or screening for dual-use goods is largely irrelevant in the context of open account trading. Making such information available for open account trades would require a re-specification of transactional data standards, such as relevant fields in payment messages (e.g. field 70 of SWIFT messages). Whilst there are annual updates to SWIFT, agreeing and implementing changes is not a fast process and one subject to a rigid control framework given the impact to global finance.

Even if such changes were made, data quality issues would likely remain. Limitations on space (number of characters available) would make it challenging to capture the often lengthy goods descriptions found in the goods lists.[90] Furthermore, the multiple and frequently changing ways that a particular item may legitimately be described (e.g. using brand names) complicate efforts to identify even those items which are honestly and openly described, an ambiguity that criminal actors can exploit to obfuscate the dual-use nature of an item.

There are multiple potentially relevant goods lists, none of which have been designed for screening. Lists that are available relate to the export control requirements of individual countries, which vary. These lists were designed for the use of manufacturers, importers and exporters, given their proximity to the actual goods and trade activity; they were not designed for use in financial transaction screening systems. The details on the goods lists do not, in isolation, allow for productive/effective comparison with the goods descriptions, transaction documents or data available to FIs. In the absence of expertise in both the various industries where dual-use goods are created and utilised, and the specifics of these items, there is a natural inclination to lean into straightforward reference to the lists. However, this is utilising the lists in a way that they were never intended to be used.

The JMLSG Part II Sectoral Guidance (15.22) states that "*DUG [dual-use goods] destined for proliferation use are difficult to identify, even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised*

[90] Field 70 of SWIFT MT103 payment messages, used for other information, is limited to a maximum of four lines of up to 35 X characters each. See: 'SWIFT MT103 message example with optional fields 53B, 70 and 71G explained', 30 July 2018 (Accessed on 11 September 2024).

knowledge and experience is often needed to determine if a good may be used for proliferation. Dual-use items can be described in common terms with many uses."[91]

As noted by the JMLSG, even if the above challenges were successfully addressed, it would require a high level of technical expertise in the specific relevant industries and goods in order to assess the potential uses of each item. The UK Strategic Export Control List, for example, details dual-use items as one of five types of controlled goods; these are broken down into nine broad categories, each of which are further divided into five separate sub-categories.[92] While the manufacturers, exporters and importers of these goods have the relevant expertise in their own specific sub-categories, FIs do not have the same level of in-depth technical expertise across all potentially relevant non-financial industries.

Key Word Screening

Reviewing the published content to determine key words for inclusion in screening lists is a heavily manual task, and requires review of other legislation, not only dual use goods lists (for example, including the Luxury Goods List, or goods subject to trade embargoes). This also includes a requirement to continue the manual review process on an ongoing basis to ensure updates are incorporated. When screening is conducted based on key words, there is limited benefit: multiple alerts can be generated with limited true matches but high resource demand and, where potential matches are identified, the result is often still ambiguous as it may not be definitively known that the good is truly dual use.

Even with screening key words, the details and terms that are used by customers often differ resulting in mismatches. Customers will use brand names and common industry terms, which cannot easily be identified by FIs. Where customers may use different terms to purposely conceal dual use goods, this can also mean the terms used change rapidly. These challenges extend beyond PF, for example, FIs are conducting additional due diligence on Russia-related trade, however, most Russia-related dual use goods published by regulators (in Notices to Exporters) are not on any of the goods lists. Additionally, the known Russian-Belarusian goods of concern do not all have Harmonised Commodity Description and Coding System (HS) codes, meaning manual mapping is required. Therefore, even where FIs are utilising the published lists, there are limitations and gaps.

Licensing and Public-Private Information Sharing

Where a licence is granted to an importer or exporter for controlled items, the granted licence does not currently contain related financial services provisions for the FI. The FI themselves must make a separate application to the Export Control Joint Unit (ECJU) for a licence in order to process the trade transaction. This requires time and administration on the part of the FI and the ECJU resulting in avoidable delays in processing the trade transaction and potentially shipping of the goods.

There are other situations in which checking or verifying the status of an export licence is not a tool available to FIs. Firstly, to verify that an export licence has indeed been granted when a customer claims this to be the case and where a specific concern has arisen regarding a shipment. In such

[91] The Joint Money Laundering Steering Group. "Prevention of money laundering/combating terrorist financing, 2023 Revised Version, Guidance for the UK Financial Sector, Part: II Sectoral Guidance." The Joint Money Laundering Steering Group, September 2023. (Accessed 20 August 2024)

[92] Department for Business and Trade. "UK Strategic Export Control List. The consolidated list of strategic military and dual-use items that require export authorisation from the United Kingdom." Department for Business and Trade, April 2024. (Accessed 20 August 2024).

instances FIs are frequently forced to rely on the claims of the customer e.g. that no export licence is required as they have no means of verifying the status. Secondly, FIs have no means of knowing of any rejected export control licence applications by exporters, making them more vulnerable to exploitation by any unscrupulous exporter who continues to seek to export in defiance of a rejected licence application.

Whilst there are established means of sharing information with FIs through public-private information sharing mechanisms, these are not utilised for sharing information regarding issued or denied export licences. Governments hold information about licence applications granted and rejected which is not currently shared with FIs. The lack of access to such information to FIs hampers a FI's ability to manage export control risk, as well as increasing the possibility of friction for licensed trade.

Annex A: Proliferation Finance Survey of Key Regulatory Sources

This Annex details the different published PF-related definitions, standards and frameworks of the:

1. United Nations
2. Financial Action Task Force
3. United Kingdom
4. United States of America
5. European Union

(1) United Nations (UN)

Today, there are 14 ongoing UN sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism, known as UN Security Council Resolutions (UNSCRs).

UNSCR 1540 (2004)

UNSCR 1540 **"***and all successor resolutions"* require all States to prohibit any non-state actor from financing the manufacture, acquisition, possession, development, transfer, or use of WMDs.[93]

UNSCR 1540 requires jurisdictions to take "*effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery…*". PF measures have the potential to prevent the provision of financial services for the development of WMD and their means of delivery by:

- preventing financing for individual shipments related to WMD proliferation;
- contributing to stopping funding and to seizing funds under specific circumstances if sufficient information is available on time;
- protecting the international financial system from abuse by proliferators;
- providing financial investigative support to existing counter proliferation investigation systems;
- hindering the financial activities of proliferators to the extent possible; and
- contributing to the identification and disruption of proliferation networks.

[93] *Ibid,* United Nations. "UNSCR 1673". United Nations, 2006. (Accessed 20 August 2024).; United Nations. "UNSCR 1810". United Nations, 2008. (Accessed 20 August 2024).; "UNSCR 1977". United Nations, 2011. (Accessed 20 August 2024).; United Nations. "UNSCR 2325". United Nations, 2016, (Accessed 20 August 2024).

UNSCR 1718 (2006) and all successor resolutions concerning DPRK."[94]

The UN PoEs are tasked with gathering, analysing and reporting on incidents of non-compliance with certain UN sanctions regimes. UN PoE have focused on sanctions regimes relating to WMD proliferation by the DPRK and worked with Member States to improve their understanding of PF and its continually evolving methods. On 3 April 2024 Russia vetoed a UNSCR to extend the DPRK UN PoE mandate for another year, weeks after the UN PoE said it was investigating reports of arms transfers between Moscow and Pyongyang. The DPRK UN PoE mandate expired at the end of April 2024.

UNSCR 2231 (2015) endorsed the Joint Comprehensive Plan of Action (JCPOA) on Iran, and replaced previous resolutions related to Iran.[95]

There are no UNSCRs relating to the declared nuclear programmes of Pakistan or India or the widely assessed nuclear weapons programme of Israel, none of which are recognised nuclear weapons states under the NPT, nor to the assessed chemical weapons capabilities of Syria or Russia.

(2) Financial Action Task Force (FATF)

As an independent international organisation, FATF develops and promotes standards and guidance aimed to safeguard the world financial system against money laundering and terrorist financing, as well as the financing of proliferation.

FATF Recommendations

CPF related recommendations were first included in FATF's recommendations in 2012 with countries required to implement TFS in accordance with the UNSCRs pertaining to PF. Another recommendation called on countries to ensure national cooperation and coordination among their competent authorities, inter alia, in the prevention of the financing of proliferation. Since October 2020, FATF has included PF risk assessments for countries, FIs and Designated Non-Financial Businesses and Professions (DNFBPs) within its standards. The current FATF Standards relating to CPF are Recommendations 1, 2, 7, and 15. In addition, FATF evaluates CPF regimes of its members, utilising Immediate Outcome 11 and certain elements of Immediate Outcome 1 to prevent money laundering and the financing of terrorism and proliferation.

Recommendation 1 (revised in October 2020) states that *"proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7."*[96] This recommendation requires FATF members to take proportionate action aimed at ensuring that PF risks are mitigated effectively, including

---

[94] United Nations. "UNSCR 1718". United Nations, 2006. (Accessed 20 August 2024).; United Nations. "UNSCR 1718". United Nations, 2006. (Accessed 20 August 2024); United Nations. "UNSCR 1874", United Nations, 2009 (Accessed 20 August 2024).; United Nations. "UNSCR 2087". United Nations, 2013. (Accessed 20 August 2024).; United Nations. "UNSCR 2094". United Nations, 2013. (Accessed 20 August 2024). United Nations. "UNSCR 2270". United Nations, 2016. (Accessed 20 August 2024).; United Nations. "UNSCR 2321". United Nations, 2016. (Accessed 20 August 2024). United Nations. "UNSCR 2356". United Nations, 2017 (Accessed 20 August 2024).; United Nations. "UNSCR 2371." United Nations, 2017. (Accessed 20 August 2024). United Nations. "UNSCR 2375". United Nations, 2017 (Accessed 20 August 2024).; United Nations. "UNSCR 2397." United Nations, 2017 (Accessed 20 August 2024).

[95] United Nations. "UNSCR 2231". United Nations, 2015. (Accessed 20 August 2024).

[96] FATF. "Public Statement on Counter Proliferation Financing". FATF, October 2020. (Accessed 20 August 2024).; FATF. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". FATF, November 2023. (Accessed 20 August 2024).

designating an authority or mechanism to coordinate actions to assess risks and allocate resources efficiently for this purpose.

"Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.

Financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes."[97]

Recommendation 2 (revised in October 2020) requires countries to put in place effective national cooperation and coordination mechanisms, which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the proliferation financing of WMD.[98]

Recommendation 7 requires countries to implement proliferation financing related TFS made under UNSCRs or resolutions under Chapter VII of the Charter of the UN, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of Weapons of Mass Destruction.[99]

Recommendation 15 requires member states to consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value" and to apply the relevant measures under the FATF Recommendations to virtual assets and VASPs. In accordance with Recommendation 1, "*countries should identify, assess, and understand the money laundering, terrorist financing and proliferation financing risks emerging from virtual asset activities and the activities or operations of VASPs*."[100]

Immediate Outcome 1 (Risk, Policy and Coordination) requires countries to understand money laundering and terrorist financing risks and, where appropriate, actions co-ordinated domestic action to combat money laundering and the financing of terrorism and proliferation.[101]

Immediate Outcome 11 (PF Financial Sanctions) requires countries to "*prevent persons and entities involved in WMD proliferation from raising, moving and using funds, consistent with the relevant UNSCRs*." [102]

---

[97] FATF. "Public Statement on Counter Proliferation Financing". FATF, October 2020. (Accessed 20 August 2024).; FATF. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". FATF, November 2023. (Accessed 20 August 2024).

[98] Ibid

[99] Ibid

[100] Ibid

[101] FATF. "Methodology. For Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CTF Systems." FATF, June 2023. (Accessed 20 August 2024).

[102] Ibid

Whilst amended Recommendation 1 and the Interpretive Note appears in the FATF Recommendations, the FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CTF systems does not currently include a requirement to assess compliance with this element of the measure. It is expected to be introduced in 2024 when the fifth round of Mutual Evaluations commences.[103]

(3) United Kingdom (UK)

The UK created an obligation for regulated entities to identify, assess and mitigate the risk of proliferation financing within the Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations 2022 which came into force in September 2022.

The UK assessed itself as having a "robust" bespoke regulatory framework in place to combat the threat posed by PF. [104] Within the latest UK PFNRA, a key focus was the implementation of the UK and UN sanctions regimes on DPRK and Iran.[105] This was pursuant to the UNSCRs, FATF Recommendation 7 and Immediate Outcome 11, and on chemical weapons activity in respect of individuals and entities from Syria and Russia.[106]

The UK meets the requirements of Recommendation 1 of the FATF Recommendations in respect of PF through the provisions of Regulations 16A and 18A of the UK MLRs. [107]

Regulation 16A of the UK MLRs requires that HM Treasury make arrangements for a PF risk assessment to be undertaken to identify, assess, understand and mitigate the risks of PF affecting the UK. The assessment must, where appropriate, identify the sectors or areas of lower and greater risk of PF. The current assessment was published in 2021[108] and covers activities which directly or indirectly finance an actor's procurement of CBRN technology that has a UK nexus and threatens the UK financial system and/or UK national security.

[103] Ibid

[104] HM Treasury. "National Risk Assessment of Proliferation Financing." HM Treasury, September 2021. (Accessed 20 August 2024).

[105] N.a "The Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019". Legislation.gov.uk, 2019. (Accessed 20 August 2024); N.a. "The Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019". Legislation.gov.uk, 2019. (Accessed 20 August 2024). (*Inter alia gave effect to* UNSCR 2231**.** The remaining targeted financial sanctions under this UNSCR expired on 18 October 2023).

[106] N.a. "Chemical Weapons (Sanctions) (EU Exit) Regulations 2019". Legislation.gov.uk, 2019. (Accessed 20 August 2024).

[107] N.a. "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017." Legislation.gov.uk, n.d. (Accessed 20 August 2024).

[108] HM Treasury. "National Risk Assessment of Proliferation Financing." HM Treasury, September 2021. (Accessed 20 August 2024).

Regulation 18A of the UK MLRs requires relevant persons working within the UK's regulated sector to take appropriate steps to identify and assess the risks of PF to which its business is subject to, which would breach a PF financial sanction obligation imposed on the UK by the UNSCRs.[109] In carrying out a risk assessment, a relevant person must take into account the information in HM Treasury's PF risk assessment and risk factors, including factors relating to its:

- customers;
- countries or geographic areas in which it operates;
- products or services;
- transactions; and
- delivery channels.

In deciding what steps are appropriate, the relevant person must take into account the size and nature of its business. A relevant person must keep an up-to-date record in writing of all the steps it has taken, unless its supervisory authority notifies it in writing that such a record is not required, and provide the risk assessment it has prepared, the information on which that risk assessment was based, and any record required to be kept, to its supervisory authority on request.[110]

HM Treasury's Office of Financial Sanction Implementation (OFSI) was established in March 2016 to enable financial sanctions to contribute to the UK's foreign policy aims and national security goals.[111] It acts to support the integrity of and confidence in the UK financial sector by imposing financial sanctions on selected targets and issuing guidance and licences to allow activities that are otherwise prohibited under financial sanctions and to detect and investigate suspected breaches, taking action where necessary.[112]

In November 2023, OFSI updated its guidance on ownership and control in UK sanctions regulations to provide a more detailed list of indicators of control by a designated person. The guidance applies to all relevant UK sanctions regimes, including CPF regimes[113].

UK sanctions measures[114] apply whenever there is a UK nexus, which includes, but is not limited to, action taken by a UK national outside of the UK and to companies incorporated in the UK.[115] As per OFSI's guidance, financial sanctions apply to all persons within the UK's territory, and to all UK persons, regardless of location.[116] This includes individual and legal entities and their branches.[117] As

---

[109] N.a. "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Regulation 16(A)(9)" Legislation.gov.uk, n.d. (Accessed 20 August 2024).

Note: Regulation 16(A)(10) restricts the definition of PF for the purposes of the UK MLRs to UNSCRs, which relate to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and the financing of such. At the time of writing, there are no financial sanction obligations imposed by UNSCRs in respect of Iran.

[110] N.a. "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Regulation 18" Legislation.gov.uk, n.d. (Accessed 20 August 2024).

[111] OFSI. "About Us." OFSI, n.d. (Accessed 21 August 2024).

[112] *ibid*

[113] OFSI. "Guidance. Ownership and Control: Public Officials and Control guidance." OFSI, August 2024. (Accessed 20 August 2024).

[114] Foreign, Commonwealth & Development Office. "The UK Sanctions Regimes." Foreign, Commonwealth & Development Office, August 2024. (Accessed 20 August 2024).

[115] N.a. "Sanctions and Anti Money Laundering Act 2018", Section 21, Legislation.gov.uk, (Accessed 20 August 2024)

[116] OFSI. "Guidance. UK Finance Sanctions General Guidance." OFSI, May 2024. (Accessed 20 August 2024).

[117] *ibid*

with UK Persons, such entities must also comply with UK financial sanctions irrespective of where their activities take place.[118]

A UK nexus might be created by such things as a UK person or company working overseas, transactions using clearing services in the UK, actions by a local subsidiary of a UK company (depending on the governance), action taking place overseas but directed from within the UK, or financial products or insurance bought on UK markets but held or used overseas.[119] These examples are not exhaustive or definitive and will depend on the facts in the case.

Obligations under the measures imposed by the UNSCRs and relevant CPF measures are set out in UK legislation, such as CPF sanctions regimes implemented under SAMLA.[120]

Section 1(1) of SAMLA provides the power for an appropriate Minister to make sanctions regulations for the purposes of compliance with a UN or any other international obligation, or for a purpose set out in section 1(2) of SAMLA.[121] This lists nine purposes, including: national security; promoting international peace and security; furthering a foreign policy objective of the Government; or to contribute to multilateral efforts to prevent the spread and use of weapons and materials of mass destruction.[122]

Sections 3 to 8 of SAMLA set out the types of sanctions that may be imposed. These include financial, immigration, trade, aircraft, shipping, and other sanctions for the purposes of complying with UN obligations.[123]

In addition to the above, the **Export Control Act 2002** and the **Export Control Order 2008** provide the legal framework for export controls in respect of strategic military and dual use items.[124]

The creation of the Office of Trade Sanctions Implementation (OTSI), part of the Department for Business and Trade, was announced in December 2023[125], to strengthen the UK's implementation and enforcement of trade sanctions. It aims to support businesses with compliance, including by issuing licences, but also to take civil enforcement action where businesses are breaching UK sanctions or seeking to circumvent them. OTSI will work in partnership with HMRC to enforce trade sanctions and it is not yet clear how this will operate in respect of PF obligations.

[118] *Ibid*

[119] OFSI. "Guidance. UK Financial Sanctions FAQs." OFSI, August 2024. (Accessed 20 August 2024).

[120] *n.a.* "Sanctions and Anti-Money Laundering Act 2018." Legislation.gov.uk, 2018. (Accessed 20 August 2024).

[121] n.a. "Sanctions and Anti-Money Laundering Act 2018." Section 1(2) Legislation.gov.uk, 2018. (Accessed 20 August 2024).

[122] n.a. "Sanctions and Anti-Money Laundering Act 2018." Legislation.gov.uk, 2018. (Accessed 20 August 2024).

[123] n.a. "Sanctions and Anti-Money Laundering Act 2018." Sections 3 to 8 Legislation.gov.uk, 2018. (Accessed 20 August 2024).

[124] n.a., ''Export Controls Act 2022''. Leigslation.gov.uk 2022 (Accessed 20 August 2024); n.a., ''Export Control Order 2008'' Legislation.gov.uk, 2008. (Accessed 20 August 2024)

[125] Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulation 2024 (Accessed 12 November 2024)

(4) United States (US)

Whilst the US and the UK share a common goal in combating PF, there are nuanced differences in the approach to regulatory requirements. This can be observed in various aspects of regulatory authorities' legal frameworks and their specific measures.

The US has had longstanding prohibitions relating to PF and WMD.[126] Sanctions issued under the Trading With the Enemy Act (TWEA) applied on North Korea until 2008.[127] Unlike the UK MLRs the US does not have specific regulatory requirements for PF risk assessment by FIs and effective mitigation of the identified risks. The US largely relies on:

- **The US International Emergency Economic Powers Act (IEEPA**), the primary implementing authority for US counter proliferation sanctions. 128
- **The Executive Order 13382 (EO 13382),** issued under IEEPA, sets out the framework within which proliferators can be designated.129 Through EO 13382 the US has designated various parties for activities related to PF.

In the context of PF, IEEPA empowers the US government to freeze assets, restrict transactions, and take other measures to combat PF activities.[130] Violations of IEEPA would be a predicate offence to the US Federal crime of Money Laundering.[131] There is therefore an obligation on US FIs to report attempts to violate and/or evade the restrictions imposed by IEEPA as suspicious activity to the relevant US Federal Authorities.

Under IEEPA, the President can declare a national emergency and based on that declaration, issue Executive Orders to impose various sanctions, including those targeting individuals, entities, or countries involved in proliferation activities.[132] PF, which involves the funding of activities related to the spread of WMD, is often a specific focus of these sanctions.

The Office of Foreign Assets Control (OFAC) within the US Department of the Treasury is the primary agency/regulatory authority responsible for implementing and enforcing sanctions under the IEEPA, particularly in relation to PF.[133] The US regulatory framework for PF primarily involves measures outlined by OFAC. OFAC administers and enforces economic and trade sanctions, including those related to PF.

Entities engaging in financial transactions are required to comply with OFAC regulations, which include identifying and blocking assets associated with individuals, entities, or countries involved in

---

[126] CFR 539: eCFR:: 31 CFR Part 539 -- Weapons of Mass Destruction Trade Control Regulations; and CFR 544: eCFR :: 31 CFR Part 544 – Weapons of Mass Destruction Proliferators Sanctions Regulations.

[127] U.S. Lifts N. Korea Trade Sanctions, 26 June 2008 (Accessed 11 September 2024)

[128] N.a. "Chapter 35 - International Emergency Economic Powers", US Congress, n.d. (Accessed 20 August 2024).

[129] US Department of the Treasury. "Executive Order 13382, "Blocking Property of Weapons of Mass Destruction Proliferators and their Supporters"; the Weapons of Mass Destruction Trade Control Regulations (Part 539 of Title 31, C.F.R.); and the Highly Enriched Uranium (HEU) Agreement Assets Control Regulations (Part 540 of Title 31, C.F.R.)". US Department of the Treasury, September 2012. (Accessed 20 August 2024).

[130] N.a. "Chapter 35 - International Emergency Economic Powers", US Congress, n.d. (Accessed 20 August 2024).

[131] U.S. Department of Justice. "2101. Money Laundering Overview." U.S. Department of Justice, n.d. (Accessed 20 August 2024).
Note: 18 U.S.C. § 1956(c)(7) lists the specified unlawful activities

[132] N.a. "Chapter 35 - International Emergency Economic Powers", US Congress, n.d. (Accessed 20 August 2024).

[133] OFAC. "About Us." OFAC, n.d. (Accessed 20 August 2024).

proliferation activities. Additionally, FIs are obligated to implement robust AML and CTF programmes to detect and prevent PF.

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the US Department of the Treasury, responsible for tackling financial crime.[134] The agency collects, analyses, and disseminates financial intelligence to support law enforcement and regulatory actions. FinCEN focuses on a range of financial crime, including ML and TF; its priorities are not exclusively tied to PF. FinCEN AML/CTF Priorities are established pursuant to Section 6101 of the Anti-Money Laundering Act of 2020 (AMLA), which assist FIs in allocating resources within their own AML programmes.[135] From a PF perspective, FinCEN Priorities outline the principal threat of PF to the US financial system, calling out global correspondent banking as a "principal vulnerability and driver of [PF] risk within the [US]".[136]

As a counter measure to these potential risks, FIs must comply with sanctions programmes and, as part of a risk-based AML programme, should also be aware of economic and trade sanctions issued by the federal government, such as OFAC, the Department of Commerce's BIS, and the Department of State's Bureau of International Security and Non-proliferation.

The US government conducts National Risk Assessments (NRAs) to assess the risks associated with ML, TF and PF . On 4 February 2024, the US government published the third iteration of its PFNRA.[137] The results of the PFNRA inform the development of US national strategies and policies to address these risks, detailing the evolving challenges within the illicit finance landscape and the adaptability of criminal networks in exploiting the global financial system.

The US PFNRA, whilst similar in approach to other PFNRAs, takes a broader scope than the UK PFNRA 2021. Whereas the UK PFNRA focusses on relevant UNSCRs and unilateral UK sanctions on chemical weapons as applied to Syria and Russia, the US PFNRA additionally highlights PF risk relating to Pakistan and highlights proliferation concerns with Russia and China's nuclear weapons programmes, notwithstanding the fact that both are recognised nuclear weapons states under the NPT.

The 2024 US PFNRA explores new methods from the misuse of digital currencies and legal entities to the sophisticated methods employed by state and non-state actors to bypass international sanctions.[138] The assessments underscore the necessity for robust, dynamic, and collaborative approaches in the AML and counter-financing of terrorism efforts. Notably, the reports call attention to the significant threats posed by ongoing global conflicts in Ukraine and Israel that have shaped the illicit finance risk environment in the US.

---

[134] FinCEN. "What We Do". FinCEN. (Accessed 29 August 2024).

[135] FinCEN. "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities." FinCEN, 2021. (Accessed 20 August 2024)

[136] *Ibid.*

[137] Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024)

[138] Department of the Treasury. "2024 National Proliferation Financing Risk Assessment." Department of the Treasury, February 2024. (Accessed 20 August 2024)

Relationship between FinCEN and the PFNRA

The relationship between FinCEN priorities and the US PFNRA lies in the broader context of financial intelligence and security. [139] FinCEN contributes to the overall efforts to combat illicit finance, which encompasses various threats, including proliferation financing.

(5) European Union (EU)

On 12 December 2003, the European Council (the Council) of the European Union (EU) adopted the 'Strategy against Proliferation of Weapons of Mass Destruction' (the Strategy) with the ultimate objective "*to prevent, deter, halt and, where possible, eliminate proliferation programmes of concern worldwide*". [140] This was the Council's first public document on non-proliferation of WMD. The Strategy was prepared within the EU's Common Foreign and Security Policy ("CFSP") and is a part of the European Security Strategy.

Its basic principles are:

- **Multilateralism.** Strengthening international non-proliferation mechanisms and working to improve systems to verify violations of rules laid down in multilateral treaties.
- **Prevention.** Promoting a regionally and internationally stable environment by strengthening programmes to promote disarmament and incorporating the non-proliferation aim in all EU political, diplomatic and economic activities.
- **International cooperation.** Working closely with the UN and other international organisations and key partners such as The North Atlantic Treaty Organization (NATO) and the US and assisting non-EU countries in improving their procedures and fulfilling their obligations under multilateral conventions and regimes.

The Strategy was complemented by the 'Council Conclusions and new lines for action by the EU in combating the proliferation of WMD and their delivery systems', in 2008, a comprehensive document setting out the implementation of the Strategy through several targeted actions and deliverables.[141]

The latest 'Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction (2022)' published 11 October, 2023, identified several challenges: the DPRK and Iranian nuclear programmes; the repeated use of chemical weapons; the development and fielding of new advanced ballistic, cruise and hypersonic missiles; the expansion of Russia's and China's nuclear arsenals; Russian nuclear threats in the context of its invasion of Ukraine; and the erosion of the arms control architecture in Europe.[142]

The EU's monitoring body, The Council of Europe Committee of Experts on the Evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL), is a FATF-style regional

---

[139] FinCEN. "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities." FinCEN, June 2021. (Accessed 20 August 2024).

[140] Council of the European Union. "Fight against the proliferation of weapons of mass destruction - EU strategy against proliferation of Weapons of Mass Destruction." Council of the European Union, December 2023. (Accessed 20 August 2024).

[141] Council of the European Union. "Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems". Council of the European Union, December 2008. (Accessed 20 August 2024).

[142] n.a. "Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction (2022)". Official Journal of the European Union, October 2023. (Accessed 20 August 2024).

body and an associate member of the FATF. The MONEYVAL Strategy on AML, combatting the financing of terrorism and proliferation financing (2023-2027) was formally adopted on 25 April 2023.[143] MONEYVAL's evaluation reports are public and widely used by intergovernmental structures, national authorities, non-governmental organisations, financial and non-financial institutions in the Europe region in determining AML/CTF policies and measures.

There is currently no AML/CTF regime requiring EU Member States or obliged entities to conduct an entity-level PF risk assessment. However, the provisional text of the latest EU Anti-Money Laundering Regulation includes financial sanctions (including PF-related sanctions) in scope of risk assessment obligations.[144]

Currently, the EU relies upon Council Decisions and Council Regulations to align to the FATF recommendations and the UNSCRs relating to the prevention, suppression and disruption of proliferation of WMD and its financing.[145]

Those obligations as implemented at EU Member State level remain strict rule-based obligations binding on all natural and legal persons within the EU. Mainly but not exclusively with:

- Council Decision (CFSP) 2023/2195 amending Decision 2010/413/CFSP and Council Implementing Regulation (EU) 2023/2196 implementing Regulation (EU) 267/2012 **concerning restrictive measures against Iran**.[146] This *inter alia* gives effect to UNSCR 1737 (2006), UNSCR 1747 (2007), UNSCR 1803 (2008) and UNSCR 1929 (2010) and UNSCR 2231 (2015).[147]
- Council Decision 2016/849/CFSP as well as Council Regulation (EU) 2017/1509 **concerning restrictive measures against DPRK**, which *inter alia* give effect to UNSCR 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2371 (2017), 2375 (2017) and 2397 (2017).[148]

[143] Council of Europe. "MONEYVAL Strategy on anti-money laundering, combating the financing of terrorism and proliferation financing (2023-2027)." Council of Europe, April 2023. (Accessed 20 August 2024).

[144] European Parliament. "Anti-Money Laundering Regulation." European Parliament, April 2024. (Accessed 20 August 2024).

[145] FATF. "International Standards of Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations." FATF, November 2023. (Accessed 20 August 2024).

NOTE: Recommendation 1 (R.1) and its Interpretive Note (R.1 and INR.1) to require countries and private sector entities to identify, assess, understand and mitigate their proliferation financing risk. In the context of R.1 proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7 (R.7)

[146] Eur-Lex. "Council Implementing regulation (EU) 2023/2196 of 16 October implementing Regulation (EU) No 267/2012 concerning restrictive measures against Iran." Eur-Lex, October 2023. (Accessed 20 August 2024).

[147] Eur-Lex. "Council Decision (CFSP) 2023/2195 of 16 October 2023 amending Decision 2010/413/CFSP concerning restrictive measures against Iran." Eur-Lex, October 2023. (Accessed 20 August 2024).

[148] Eur-Lex. "Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP". Eur-Lex, May 2016. (Accessed 20 August 2024).; Eur-Lex. "Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007". Eur-Lex, August 2017. (Accessed 20 August 2024).

- Council Decision 2018/1544 and 2019/1722/CFSP as well as Council Regulation (EU) 2018/1542 **concerning restrictive measures against the proliferation and use of chemical weapons**.[149]
- Council Regulation (EU) 428/2009 **which provides for the setting up of a Community regime for the control of exports, transfer, brokering and transit of dual-use items**, and Commission Delegated Regulation (EU) 2023/66 and Regulation (EU) 2021/821 with regards to **the list of dual-use items that are subject to controls in the Union.**[150]

Restrictive measures are an important component of the EU's foreign and security policy toolbox. They can consist of, for instance, asset freezes, travel bans and import/export restrictions. The enforcement of EU sanctions is a member state responsibility. But the types and levels of penalties in member states can vary as national systems that deal with the violation of EU sanctions differ significantly.

EU member states were not required to criminalise violations and could thus apply administrative measures instead. To limit sanctions circumvention and tighten their enforcement, the EU introduced a directive on the definition of criminal offences and penalties for the violation of Union restrictive measures on 24 April 2024.[151]

[149] Eur-Lex. "Consolidated text: Council Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons." Eur-Lex, October 2018. (Accessed 20 August 2024).; Eur-Lex. "Council Decision (CFSP) 2019/1722 of 14 October 2019 amending Decision (CFSP) 2018/1544 concerning restrictive measures against the proliferation and use of chemical weapons." Eur-Lex, October 2019. (Accessed 20 August 2024).; Eur-Lex. "Council Regulation (EU) 2018/1542 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons." Eur-Lex, October 2018. (Accessed 20 August 2024).

[150] Eur-Lex. "Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a community regime for the control of exports, transfer, brokering and transit of dual-use items." Eur-Lex, May 2009. (Accessed 20 August 2024).; Eur-Lex. "amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items". Eur-Lex, October 2022. (Accessed 20 August 2024).; Eur-Lex. "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items." Eur-Lex, May 2021. (Accessed 20 August 2024).

[151] Eur-Lex. "Directive (EU) 2024/1226 of the European Parliament and of the Council on 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673". Eur-Lex, April 2024. (Accessed 20 August 2024).

Annex B: Acronyms

1LoD	First Line of Defence
2LoD	Second Line of Defence
3LoD	Third Line of Defence
AIS	Automated Identification System
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Act 2020
AMLD	Anti-Money Laundering Directive
APG	Asia Pacific Group
ATM	Automated Teller Machine
Aus	Australia
Aus PFNRA	Australian Transaction Reports and Analysis Centre Proliferation Finance National Risk Assessment 2022
BAFT	Bankers Association for Finance and Trade
BIS	Bureau of Industry and Security
BOI	Beneficial Ownership Information
BWC	Biological Weapons Convention
CB	Correspondent Banking
CBDDQ	Correspondent Banking Due Diligence Questionnaire
CBRN	Chemical, Biological, Radiological and Nuclear
CDD	Customer Due Diligence
CFSP	Common Foreign and Security Policy
CPF	Counter-Proliferation Financing
CTA	Corporate Transparency Act
CTF	Counter-Terrorist Financing
CWC	Chemical Weapons Convention
DACs	Digital Assets and Currencies
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	The Democratic People's Republic of Korea (North Korea)
DUGs	Dual Use Goods
EAR	Export Administration Regulations
ECJU	Export Control Joint Unit
EP	European Parliament
EU	European Union
FATF	Financial Action Task Force
FC	Financial Crime
FCA	Financial Conduct Authority
FI	Financial Institution
FinCEN	Financial Crimes Enforcement Network
HK	Hong Kong
HKMA	Hong Kong Monetary Authority
HMT	His Majesty's Treasury
HRTC	High Risk Third Country
HS	Harmonised Commodity Description and Coding System
IAEA	International Atomic Energy Authority
ICC	International Chamber of Commerce
IEEPA	International Emergency Economic Powers Act
IP	Internet Protocol
JMLSG	UK Joint Money Laundering Steering Group

KYC	Know Your Customer
MERs	Mutual Evaluation Reports
MI	Management Information
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
MLRs	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended (UK)
NACE2	Statistical Classification of economic activities in the European Community, Revision 2.
NATO	North Atlantic Treaty Organization
NCA	National Crime Agency
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
NPWMD	Non-proliferation of Weapons of Mass Destruction
OECD	Organization for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control (US Department of the Treasury)
OPCW	Organisation for the Prohibition of Chemical Weapons
PF	Proliferation Finance
PFNRA	Proliferation Financing National Risk Assessment
PFRA	Proliferation Financing Risk Assessment
PPI	Peddling Peril Index
PPP	Public Private Partnership
R&D	Research and Development
RM	Relationship Manager
RUSI	Royal United Services Institute
SAMLA	Sanctions and Anti-Money Laundering Act 2018
SAR	Suspicious Activity Report
SDN	Specially Designated National
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBML	Trade Based Money Laundering
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TM	Transaction Monitoring
TWEA	Trading with the Enemy Act
UAE	United Arab Emirates
UAV	Unmanned Aerial Vehicle
UBO	Ultimate Beneficial Owner
UK	United Kingdom
UK NPFRA	HM Treasury National Risk Assessment of Proliferation Financing 2021
UN	United Nations
UN PoE	UNSC Panel of Experts to the UNSCR 1718 Sanctions Committee
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
US	United States
US Adv	US Department of the Treasury, Department of State and United States Coast Guard Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities.
US NPFRA	US Department of the Treasury 2024 National Proliferation Financing Risk Assessment
VASP	Virtual Asset Service Provider
WMD	Weapons of Mass Destruction

Annex C: PF Information Resources Repository

Proliferation Financing National Risk Assessment Source Review: UN

Number	Source Link	Year
1	UN PoE	2024
2	UNSC Resolutions relating to DPRK (1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017))	2006-17
3	UNSC Resolutions relating to Iran (2231)	2015
4	DPRK Reports A body of 20 reports by the UNSC Panel of Experts (UN PoE) to the UNSCR 1718 Sanctions Committee, dated between November 2010 and March 2024, and the associated UNSC sanctions resolutions." Also in that description text, the statement, containing over 7,000 entities in all. We note that this data refers only to DPRK-related proliferation, hence PF risk relating to other proliferators, such as Iran, is not represented. There is currently no equivalent dataset to draw upon for non-DPRK related proliferation.	Nov 2010 AND Sept 2023
5	UNSC 1540	2004

Proliferation Financing National Risk Assessment Source Review: UK

Number	Source Link	Year
1	The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022	2022
2	UK National PF Risk Assessment	2022
3	JMLSG Guidance	2022
4	Financial Crime Guide: A firm's guide to countering financial crime risks (FCG), FCA	2022
5	How does a global trade and receivables finance mitigate against proliferation finance, ICC	2019
6	UK Export Control Order 2009	2009
7	Radiological weapons: how real is the threat? RUSI	2007

Proliferation Financing National Risk Assessment Source Review: US

Number	Source Link	Year
1	US National PF Risk Assessment	2024
2	US National PF Risk Assessment	2022
3	Treasury Targets Iranian Oil and Petrochemical Trade Network	2022
4	Guidance of the Democratic People's Republic of Korea Information Technology Workers	2022
5	FinCEN Priorities	2021
6	Countering North Korean Procurement Networks Through Financial Measures: The Role of Southeast Asia	2020
7	North Korea Ballistic Missile Procurement Advisory	2020
8	Guidance to Address Illicit Shipping and Sanctions Evasion Practices	2020
9	Guidance of the North Korean Cyber Threat	2020
10	Sanctions Risks Related to Petroleum Shipments involving Iran and Syria	2019
12	Updated Guidance on Addressing North Korea's Illicit Shipping Practices	2019
13	The Financing of Nuclear and other Weapons of Mass Destruction Proliferation	2018
14	The Financing of WMD Proliferation: Conducting Risk Assessments	2018

Number	Source Link	Year
15	Risks for Businesses with Supply Chain Links to North Korea	2018
16	What You Need To Know About Treasury Restrictions – Nonproliferation	2012
17	EO 13382 Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters	2005
18	Background to EO 13382	2005

Proliferation Financing National Risk Assessment Source Review: US

Number	Source Link	Year
1	Commission Delegated Regulation (EU) 2023/66	2022
2	Regulation (EU) 2021/821	2021
3	Combatting Proliferation Finance: A European Banking Perspective	2012
4	Free E-Learning: EU Non-Proliferation and Disarmament	N/A

Proliferation Financing National Risk Assessment Source Review: FATF

Number	Source Link	Year
1	Procedures for the FATF AML/CFT/CPF Mutual Evaluations, Follow-Up and ICRG	2024
2	The FATF Consolidated Assessment Ratings (MERs)	2024
3	The FATF Recommendations (As amended March 2022 – specifically Recommendations 1 and 7 and their respective Interpretive Notes)	2022
4	FATF Mutual Evaluation	2022
5	Guidance on Proliferation Financing Risk Assessment and Mitigation	2021
6	FATF Objectives	2018-19
7	Guidance on Counter Proliferation Financing	2018
8	Concealment of Beneficial Ownership – joint report with the Egmont Group	2018
9	Combating Proliferation Financing Status Report	2010
10	FATF Typologies Report on Proliferation Financing	2008

Proliferation Financing National Risk Assessment Source Review: Other

Number	Source Link	Year
1	Australia	2022
2	France	2022
3	Hong Kong	2022
4	United States	2022
5	Australia	2022
6	Brazil	2021
7	Indonesia	2021
8	Malaysia	2021
9	Taiwan	2021
10	United Kingdom	2021
11	Mexico	2020

Proliferation Financing National Risk Assessment Source Review: Other publications

Number	Publication	Year
1	Council of the EU Press Release - Anti-money laundering: Council adopts package of rules	**2024**
2	Mexican Presidency's Priorities for 2024-2026	**2024**
3	The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges	2024
4	RUSI Public Dataset on DPRK	2024
5	OPCW Fact-Finding Mission on the use of toxic chemicals as weapons in the Syrian Arab Republic	2024
6	North Korean PF and Designated Non-Financial Business and Professions, and its Accompanying Annex, RUSI	2022
7	Asia/Pacific Group Yearly Typologies Report 2022	2022
8	Asia/Pasific Yearly Typologies Report 2021	2021
9	UAE Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction	2021
10	Black Gold: Exposing North Korea's Oil Procurement Networks, RUSI and C4ADS	2021
11	The Peddling Peril Index 2021/2022, Institute for Science and International Security	2021
12	North Korean Sanctions Evasion Techniques, RAND Corporation	2021
13	Gibraltar Counter Proliferation Financing Guidance Notes	2020
14	Proliferation Finance Survey, RUSI-ACAMS	2020
15	How does Global Trade and Receivables Finance Mitigate Against Proliferation Financing? ICC	2019
16	How does a global trade and receivables finance mitigate against proliferation finance, ICC	2019
17	Carnegie Endowment Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help	2018
18	C4ADS Mapping Overseas Forced Labour in North Korea's Proliferation Finance System	2018
19	Singapore Sound Practices to Counter Proliferation Financing	2018
20	The Financing of WMD Proliferation, Center for a New American Security	2018
21	Bahamas Guidance Note on Proliferation and Proliferation Financing	2018
22	Isle of Man Financial Sanctions Relating To Proliferation -Guidance	2018
23	The Financing of Nuclear and Other WMD Proliferation, Center for a New American Security	2018
24	C4ADS The Forex Effect - US Dollars, Overseas Networks, and Illicit North Korean Finance	2017
25	C4ADS Risky Business A System-Level Analysis of the North Korean Proliferation Financing System	2017
26	Study of Typologies of Financing of WMD Proliferation, King's College London	2017
27	Countering Proliferation Finance: An Introductory Guide for Financial Institutions, RUSI	2017
28	IAEA (various publications)	various
29	The Asia/Pacific Group on Money Laundering Yearly Typologies Reports (APG)	various
30	RUSI	various
31	Jersey Proliferation and Proliferation Financing of weapons of mass destruction	various
32	UAE Targeted Financial Sanctions Proliferation & Terrorism Financing	N/A

END