Jersey Financial Services Commission

Countering proliferation of weapons of mass destruction and its financing

Guidance on countering the financing of proliferation of weapons of mass destruction

Issued: April 2022

Glossary of Terms

Defined terms are indicated throughout this document as follows:

CPF	Counter the financing of proliferation of weapons of mass destruction
Diversion	Transactions that divert funds/resources away from their legitimately intended purpose to benefit Proliferators, directly or indirectly
DPRK	Democratic People's Republic of Korea (North Korea)
Dual use items	Items including, for example, software and technology which can be used for both civil and military purposes
EU	European Union
FATF	Financial Action Task Force
FATF Standards	The FATF Recommendations, the international anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT/CPF) standards, and the FATF Methodology to assess the effectiveness of AML/CFT/CPF systems
Financial services business	A business specified, or of a description specified, in Schedule 2 of the Proceeds of Crime (Jersey) Law 1999
Front company	A company that appears to undertake legitimate business but which, in reality, is serving to obscure illicit financial activity
IFC	International Finance Centre
The Minister	Minister for External Relations and Financial Services
Money laundering	Laundering the proceeds of crime
PF	Proliferation Financing (financing of Proliferation of weapons of mass destruction)
POCL	Proceeds of Crime (Jersey) Law 1999
Proliferation	Proliferation of weapons of mass destruction - 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 Dual use items used for illicit purposes), in contravention of national laws or, where applicable, international obligations
Proliferator	A State, natural or legal person, or a legal arrangement, undertaking Proliferation may, at times, be referred to as a Proliferator
Relevant financial institution	Defined in the Sanctions and Asset-Freezing (Jersey) Law 2019. Includes all Supervised Persons as well as persons (not being individuals) that are incorporated or constituted under the law of Jersey and that carries Financial services business in any part of the world

RUSI	Royal United Services Institute
SAFL	Sanctions and Asset-Freezing (Jersey) Law 2019
SAFO	Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021
Shell company	An inactive company used as a conduit for money that do not have a high level of capitalisation or which displays other Shell company indicators such as long periods of account dormancy followed by a surge of activity
Supervised Person	Defined in Article 1 of the Proceeds of Crime (Supervisory Bodies)(Jersey) Law 2008 and covers all of those persons that are required to comply with the Money Laundering (Jersey) Order 2008
Terrorist financing	The financing of terrorist acts, and of terrorists and terrorist organisations, regulated as: › Conduct which is an offence under any provision of Articles 15, 16 and 16A of the Terrorism (Jersey) Law 2002 › Conduct outside Jersey which, if occurring in Jersey, would be an offence under Articles 15, 16 and 16A of the Terrorism (Jersey) Law 2002 › Conduct which is an offence under any provision of Article 21 of the Terrorism (Jersey) Law 2002; and › Conduct which is an offence under any provision of Parts 3, 4 and 6 of the Sanctions and Asset-Freezing (Jersey) Law 2019
TFS	TFS, targeted financial sanctions, means both (i) asset-freezing and (ii) prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of those targets designated as being subject to sanctions
TFS-PF	Targeted financial sanctions relating to the prevention, suppression and disruption of Proliferation of weapons of mass destruction and proliferation financing
UK	United Kingdom
UN	United Nations
UNSC	Security Council of the United Nations as defined in the Sanctions and Asset-Freezing (Jersey) Law 2019
UNSCR	A resolution adopted by the UN Security Council under Article 41 of the Charter of the UN, as defined in Sanctions and Asset-Freezing (Jersey) Law 2019
WMD	Weapons of mass destruction, including, for example, automic explosive weapons, lethal biological and chemical weapons, radioactive material weapons and any weapons developed in the future which have comparative destructive effects

Table of Contents

Scope

This guidance has been produced by us in collaboration with the competent authority for financial sanctions, the Minister for External Relations and Financial Services (**the Minister**). Its aim is to provide insight and guidance on methods to be adopted by Industry to counter the financing of proliferation of weapons of mass destruction (**CPF**).

This guidance is general in nature and does not constitute, nor should it be construed as, legal advice. It should be read in conjunction with the practical guidance on sanctions on our website: https://www.jerseyfsc.org/industry/international-co-operation/sanctions/

Introduction

Why combatting the financing of Proliferation of weapons of mass destruction is important

The Financial Action Task Force (**FATF**) requires countries to implement United Nations Security Council Resolutions (**UNSCR**) concerning the prevention, suppression and disruption of proliferation of weapons of mass destruction (**WMD**) (**Proliferation**) and Proliferation financing (**PF**). UNSCRs require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council (**UNSC**) under Chapter VII of the Charter of the United Nations.

Jersey has zero tolerance for PF. Legislation governing the formation of Jersey legal entities and arrangements including, for example, companies, partnerships, and foundations, requires that they are formed for a lawful purpose. These provisions are applicable to all Jersey entities, theirs subsidiaries, affiliates or associates, directly or indirectly involved in activities that could pose a potential risk to the reputation of the Island.

Our Sound Business Practice Policy provides examples of some activities, that may expose Jersey to Proliferation and PF risks:

- Manufacture, maintenance, sale, supply, delivery, transfer, purchase, importation, exportation, transportation, financing or financial assistance, use of, provision of brokering services, training or technical assistance in respect of arms, weapons, ammunitions, countermeasures or any other military or defence equipment, goods, technology, and personnel
- Manufacture, marketing or sale of pharmaceutical goods or devices which are not licensed or have not received marketing authorisation in the jurisdiction where they are manufactured, marketed, sold or supplied
- Conduct of scientific research
- Exportation or importation of goods or technology, which would require an authorisation or licence under Jersey Dual use items legislation; **Dual Use items** including, for example, software and technology, which can be used for both civil and military purposes
- Mining, drilling or quarrying for natural resources
- Initial coin offerings, crypto exchanges or providing other services relating to cryptocurrencies
- The sale or facilitation of sale of citizenship/citizenship by investment (which includes the administration associated with citizenship and/or arranging for citizenship).

Proliferation networks continuously seek to exploit weaknesses in the global export control and international financial systems. Whilst there is currently no evidence to suggest that Supervised Persons in Jersey are knowingly facilitating illicit activities, it is the case that any International Financial Centre (**IFC**) is potentially exposed to PF risks.

CPF includes implementing relevant sanctions regimes as they refer to PF, including activity-based restrictions on access to the global financial system by **Proliferators**, A i.e. a State, natural or legal person, or a legal arrangement, undertaking Proliferation.

Understanding Proliferation and PF

What is Proliferation of WMD?

Proliferation is involvement in 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 Dual use items used for illicit purposes), in contravention of national laws or, where applicable, international obligations.

Jersey is not a manufacturer of weapons, nor a trade centre for Proliferation goods, however, all natural persons, and legal persons and arrangements located in Jersey, operating in or from within Jersey, or being incorporated or constituted under Jersey law, are required to comply with the relevant CPF legislation and related sanctions regimes.

Dual use items are items, including software and technology, which can be used for both civil and military purposes. A list providing examples is provided in **Annex A** – PF sensitive and export control goods**.**

Proliferation can take many forms, it includes legitimate technology, goods, software, services and expertise. For example, it may involve scientific research, transfer or export of sophisticated technology, such as in long range missiles; or it may involve a relatively unsophisticated dirty bomb, a device that combines conventional explosives with radioactive material.

What is PF?

While there is no internationally agreed definition for PF, it can be described as providing financial services and products for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. It involves the financing of trade in Proliferation sensitive goods, but could also include other financial support legal or natural persons or arrangements engaged in Proliferation.

In complex structures PF may not necessarily be directly connected to the physical flow of goods. For example, PF can include, although not be limited to, the following:

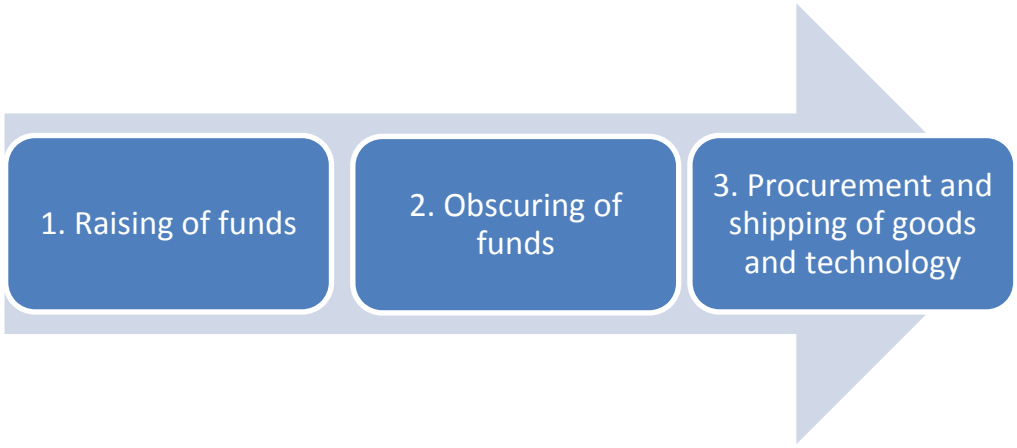
- Financial transfers
- Provision of loans
- Ship mortgages and registration fees
- Insurance and re-insurance services
- Credit lines for shipment of illicit sensitive goods
- Trust and corporate services
- Acting as an agent for, to, or on behalf of someone else
- Facilitation of any of the above.

In many cases PF activity has the sole aim of generating access to foreign currency and the international financial system. It may look like a legitimate trading transaction. For this reason, it is important to understand the full payment chain and consider how any trade may be used to enable illicit activity.

As an IFC, Jersey takes its obligations to ensure that legal arrangements are not abused for PF very seriously.

Stages of PF

The diagram below describes three stages of PF. The background arrow illustrates the gradual increase of the potential risk of abuse of international financial systems through each consecutive PF stage.



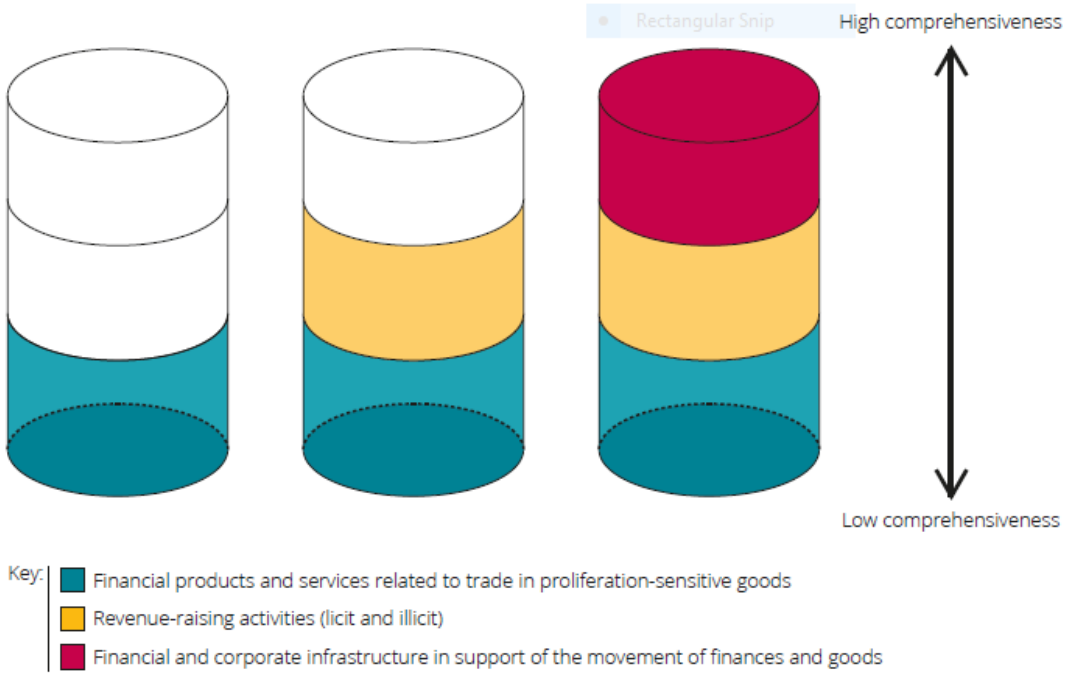
Source: Adapted from CNAS report on PF. J. Brewer (2018)

By way of example, the UNSC 1718 Sanctions Committee periodically provide Panel of Experts' reports focusing on analysis of PF stages process in the Democratic People's Republic of Korea (**DPRK**).

- Initially, financing can be sourced from both legitimate and illegitimate activities raising funds or obtaining foreign exchange, and may not necessarily involve laundering the proceeds of crime (**Money laundering**). Examples can include procuring or trading in Dual use items or goods subject to export control, or the trade in natural resources, illegal export of coal and sand, procurement of oil, smuggling of cash, gold, and other high-value goods, cyber-attacks and crypto raids, drug trafficking, export of weapons and arms etc.
- The more isolated the legal or natural persons or arrangements or State undertaking Proliferation becomes, for example due to imposed sanctions, the more sophisticated techniques it will use to obscure the source of funds to inject money into the international financial system. This is done, for example, via the use of opaque ownership structures or management, use of false documentation, middlemen, Front companies, i.e. companies that appear to undertake legitimate business but which, in reality, are serving to obscure illicit financial activity etc.
- Procurement and shipping of goods and technology is the final stage where the Proliferator pays for goods, materials, technology, and logistics needed for their WMD program. The final stage will inevitably involve international financial institutions processing the related transactions. At this stage PF links can be detected on the basis of various indicators, activity models and typologies.

PF typologies

The Royal United Services Institute (**RUSI**) has identified categories of direct and indirect PF activities.



Source: Adapted from RUSI's Guide to conduct a national PF risk assessment (2019)

The following are examples of financial products and services directly related to the trade in proliferation-sensitive goods.

- Use of trade finance products and services and clean payment services in procurement of Proliferation-sensitive goods.
- Use of:
    - Front companies, i.e. companies that appear to undertake legitimate business but which, in reality, serve to obscure illicit financial activity
    - Shell companies, i.e. inactive companies used as a conduit for money that do not have a high level of capitalisation or which displays other shell company indicators such as long periods of account dormancy followed by a surge of activity
    - Brokers and professional intermediaries

  to obtain trade finance products and services, or as parties to clean payments.
- Nationals or dual citizens of States that undertake Proliferation, or family members of such persons (regardless of citizenship), used as intermediaries in countries not of Proliferation concern, to facilitate procurement of goods and/or for payment of funds. Likely to involve use of personal banking products.
- Money transfer services used to conduct cash transfers related to procurement of goods.
- Use of professional intermediaries and firms to mask parties to transactions and end users.

- Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance.
- Use of financial routes that are indirect to the movement of sensitive goods, or to countries or institutions (such as universities or research institutes) which are not of Proliferation concern.
- Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. Often combined with use of Front companies with opaque ownership structures.

The following are examples of indirect revenue-raising techniques:

- Cybercrime, such as hacking accounts to obtain value, largely used by State actors.
- Use of banks and other financial institutions with foreign or local branches operating in countries of Proliferation concern or use of financial institutions with known links to Proliferating actors.
- Use of cryptocurrencies to avoid the formal financial system, and cybercrime to obtain illicit funds.
- Use of diplomats, consular officers or diplomatic or consular missions to build networks, including corporate networks, within a country. These networks then facilitate a range of revenue-raising activities as well as facilitating financial products or services related to trade in goods.
- Use of trade or other economic relations of countries with links or significant exposure to a country known for Proliferation. Often facilitated by a complex corporate network.
- Use of organised or transnational criminal networks, particularly their transport corridors and intermediaries in their networks.
- Use of vessels/ aircraft and shipping companies that do not attract Proliferation concern to obtain maritime or cargo insurance or other financial products, or using fraudulent documents relating to shipping, customs or payments.

In many cases PF activity has the sole aim of generating access to foreign currency and the international financial system. This can be through what appears to be a legitimate trading transaction. For this reason, it is important to understand the full payment chain and consider how any trade may be used to enable illicit activity.

Annex B – DPRK's use of the international financial system for Proliferation purposes illustrates a visual chart of how DPRK has used the international financial system for Proliferation purposes.

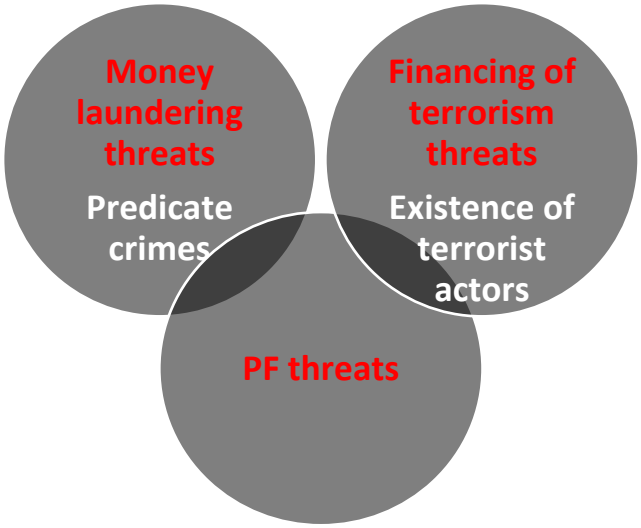
PF vs Money laundering and Terrorist financing

PF can be described as both a distinct financial crime risk and a sanctions risk. It may share certain characteristics with other forms of financial crime, such as Money laundering and/or Terrorist financing. See comparison table.

However, the nature and characteristics of PF risk are significantly different.

- PF threats are typically posed by Proliferation networks, created by those targeted by UNSCR designated sanctions to disguise their activities, including those acting on their behalf of, or at the direction of them. As a result, their financing needs and methods may not necessarily be the same as those of other criminal actors.
- Since PF networks may derive funds from both criminal activity and/or legitimately sourced funds, transactions related to PF may use the international financial system under the umbrella of legitimate business and may not exhibit the same characteristics as Money laundering and/or Terrorist financing.
- The number of customers or transactions related to Proliferation activities is likely to be smaller than those involved in other types of financial crime.

Predicate offences and criminal actors are relevant considerations for PF, but complex nature of PF means that the range of possible threats is broader than in considering Money laundering, or Terrorist financing, in isolation.



Source: Adapted from CNAS report (2018) and RUSI Paper (2017)

What are the difficulties faced with identifying and combatting PF?

PF transactions may look like normal commercial activity, structured to hide connections to the Proliferator or Proliferation activities. The ICC Policy Statement (2019) and CNAS Report (2019) list a number of difficulties associated with identifying PF, such as:

- A growing trend in the purchase and sale of elementary and replaceable components, as opposed to whole manufactured systems, making their identification increasingly problematic. In addition, identification of Dual use items and Proliferation sensitive commodities often requires specialist knowledge and expertise.

- PF networks tend to be complex. This, combined with the use of false documentation, may allow for Proliferation sensitive goods, the entities involved, the associated financial transactions and the ultimate end-user to avoid detection. Front companies, agents and other false end-users may be used to obscure the ultimate end-user.
- The risk of PF will be heightened in cases where the source of funds is legal, but the end-user of the goods involved is obscured, making identification of such activities challenging.
- Trade finance activities, often used for sanctions evasion, tend to have a fragmented nature, where multiple parties (in many cases with limited knowledge of one another) become involved in the PF activity.

Emerging threats in combatting PF

The CNAS Report (2020) outlined emerging threats in combatting PF:

- Cryptocurrencies offer Proliferation networks more ways to evade sanctions given that they are harder to trace and can be laundered multiple times. Many new technologies are built on distributed ledger technology, known as the "blockchain", which is a way of decentralising the collection of data. With distributed ledger technology, a record of transactions can be stored and verified through the consensus of a network's users, rather than through a central data-collection or settlement authority. There is evidence that DPRK seeks to use cryptocurrencies through fundraising, stockpiling and circumvention as part of its PF efforts.
- The advanced manufacturing techniques and chemical or biological innovations, such as three dimensional printing, synthetic biology, chemical synthesis, nano-biotechnology etc., could be reasonably inexpensive and obtainable for creating and maintaining a significant arsenal of weapons.

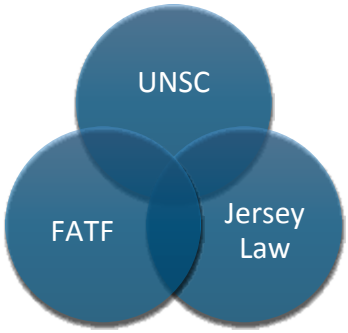
As a part of international efforts to combat PF, in 2021, the EU established a new Union regime for the control of exports, brokering, technical assistance, transit and transfer of Dual use items. It covers challenging categories of exporters, such as service providers, researchers, consultants, persons transmitting Dual use items electronically, especially scientists and academic and research institutions, involved in cutting edge technologies, who all need to be aware of PF risks.

Obligations to counter PF

Overview

Frameworks to combat PF rely on three interlinked sources of obligations:

- International legal obligations put in place by the UNSC
- FATF Recommendations
- Domestic legislation.



International Obligations – UNSCR

Though Jersey is not a UN member in its own right, the UK's membership of the UN extends to the Island. Therefore, in common with all UN members, Jersey has an obligation to implement the UNSCRs relevant to PF:

- UN Security Council Resolution 1540 (2004), requires countries to prohibit any non-state actor from financing the manufacture, acquisition, possession, development, transfer, or use of WMD. There are no current designations.
- UN Security Council Resolution 1718 (2006) and all successor resolutions concerning DPRK.
- UN Security Council Resolution 2231 (2015) endorsing the Joint Comprehensive Plan of Action on Iran, and replacing previous resolutions related to Iran.

International Obligations – FATF Standards

That FATF Standards establish international rules for the implementation of Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of WMD and PF **(TFS-PF).** These are prescribed in the FATF Recommendations, interpretative notes and methodology.

- **Recommendation 7** requires countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UNSC under Chapter VII of the Charter of the UN.
- **Recommendation 2** (revised in October 2020) calls on cooperation and coordination of the relevant authorities to combat Money laundering, Terrorist financing and PF.
- **Recommendation 1** (revised in October 2020) requires countries, financial institutions, designated non-financial businesses and professionals, virtual asset service providers, and non-profit organisations to identify and assess the risks of potential breaches, non-implementation or evasion of TFS-PF and to take action to mitigate them.
- **Recommendation 15** (revised in June 2021) requires to conduct a PF risk assessment and establish mitigation in respect of virtual asset activities and service providers.

The FATF Recommendations aim to ensure, via country applications, that private sector entities are made aware of the PF risks involved in their businesses and professions, and thereby understand that they must not support, or become part of, PF networks or schemes.

The FATF's Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to counter proliferation of weapons of mass destruction is a helpful resource. The paper aims to give non-binding guidance to facilitate both public and private sector stakeholders in understanding and implementing obligations. Additional

non-FATF required elements under relevant UNSCRs are also included to give stakeholders a more holistic perspective in CPF.

Domestic obligations

In addition to international obligations, there are offences under Jersey law relevant to the development, production, acquisition, retention, transfer etc. of nuclear, biological and chemical weapons, illustrated in the table below:

Legislation	Offence	Maximum penalty	WMD type
Crime and Security (Jersey) Law 2003	Article 2(1) – Use etc. of nuclear weapons	Imprisonment for life	Nuclear
Biological Weapons Act 1974 (Jersey) Order 1974	Article 1 - Restriction on development etc. of certain biological agents and toxins and of biological weapons	Imprisonment for life	Biological
Chemical Weapons Act 1996 (Jersey) Order 1998	Article 2(1) – Use etc. of chemical weapons	Imprisonment for life	Chemical
Sanctions and Asset-Freezing (Jersey) Law 2019	Part 3 – Dealing with and making funds, financial services or economic resources available for the benefits of designated person directly or indirectly	Imprisonment for a term of 7 years and to a fine	Vary with each sanctions regime
Nuclear Material (Offences) Act 1983 (Jersey) Order 1991	Sections 1 to 4, 6, 8 and the Schedule to the UK Nuclear Material (Offences) Act 1983 - use or possession of nuclear material etc.	Imprisonment for a term of 14 years	Nuclear material
Terrorism (Jersey) Law 2002	Article 15 – Use, possession or providing property or financial service for the purposes of terrorism Article 16 – Dealing with terrorist property	Imprisonment for a term of 14 years or to a fine, or both	All (within terrorism property)
Proceeds of Crime (Jersey) Law 1999	Article 30 – Dealing with criminal property Article 31 – Concealment etc. of criminal property	Imprisonment for a term of 14 years or to a fine, or both	All (within criminal property)

Legislation	Offence	Maximum penalty	WMD type
Money Laundering and Weapons Development (Directions) (Jersey) Law 2012	Article 14 – Failure to comply with directions given with regards to development, production or facilitation of nuclear, radiological, biological or chemical weapons, or their means of delivery	Imprisonment for a term of 7 years and to a fine	All

Jersey sanctions framework targeting PF

The FATF Standards require us to have an understanding of the risk of PF breaches, non-implementation or evasion of TFS-PF, as well as how to assess, and mitigate or manage these risks.

In Jersey, the the Minister is the competent authority for sanctions. The Ministry of External Relations coordinates the introduction of sanctions measures. Other sanctions, such as trade sanctions, arms embargos and other trade restrictions, are implemented by the Jersey Customs and Immigration Service (JCIS).

Jersey implements and enforces all relevant UN and UK sanctions regimes through the Sanctions and Asset-Freezing (Jersey) Law 2019 (**SAFL**), and the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021 (**SAFO)**.

Any changes to asset-freeze designations made by the UNSCRs and UK are effective immediately by virtue of the ambulatory provisions in Jersey's sanctions legislation. Failure to comply with sanctions legislation or to seek to circumvent its provisions is a criminal offence.

The Government of Jersey, to date, has not imposed any autonomous sanctions. Instead it adopts the UK OFSI Consolidated List and the UK Sanctions List as a comprehensive listing of sanctions designations applicable in Jersey.

	Financial sanctions	Trade sanctions, arms embargos and other trade restriction
Jersey legislation and sources	› SAFL / SAFO › Jersey sanctions regimes by country and category › Jersey sanctions regimes by person	› Customs and Excise (Import and Export Control) (Jersey) Order 2006 › Open General Export Licence 6 April 2021, including provision on Dual use items on GOV. JE website
Relevant UK legislation and sources	› Sanctions and Anti-Money Laundering Act 2018 › UK Financial Sanctions targets by regime on GOV. UK website	› Export Control Act 2002 › UK Guidance on Trade sanctions, arms embargoes, and other trade restrictions GOV.UK website › UK Guidance on Export control: military goods, software and technology on GOV.UK website
Common restrictive measures	› Asset freezes which restrict access to funds and economic resources › Restrictions on dealing with various financial markets › Restrictions to cease business of a specified type, e.g. with suspected links to terrorism	› Controls on the export and import of certain goods and technology, such as military goods and technology › Controls on the provision of certain assistance and services, such as financial services, related to controlled goods and technology

Financial sanctions	Trade sanctions, arms embargos and other trade restriction
› Directions to cease all business with certain sanctioned individuals or organisations	› Controls on other trade related activities, such as services relating to ships/vessels and aircraft

Sanctions compliance reporting obligations and process

Reporting obligations are set out in Article 32 of SAFL. The obligations apply to all sanctions regimes. The obligations include requirements for a "Relevant financial institution" to inform the the Minister if:

- It holds an account of a person; has entered into dealings or an agreement with a person or has been approached by or on behalf of a person, and
- It knows, or has reasonable cause to suspect, that the person is a designated person, or has committed an offence, and
- The information or other matter on which the knowledge or reasonable cause for suspicion is based came to it in the course of carrying on its business.

"Relevant financial institution" is defined in Article 1 of SAFL and means –

- a person (whether or not an individual) who carries on Financial services business, within the meaning of the Proceeds of Crime (Jersey) Law 1999, in or from within Jersey; or
- a person (not being an individual) that is incorporated or constituted under the law of Jersey and carries on such Financial services business in any part of the world.

If Supervised Persons know or have reasonable cause to suspect that they are in possession or control of, or are otherwise dealing with targeted assets of a UN designated person, the process to follow is:

- Freeze the assets
- Do not deal with or make them available to designated persons, or for the benefit of the designated person, unless there are exceptions, or a licence is in place
- Make a report to the the Minister at sanctions@gov.je using the Sanctions Compliance Reporting Form.
- These reporting obligations are in addition to the obligation to report suspicious activities (**SAR**) to the Jersey Financial Intelligence Unit, and to keep your JFSC supervisor informed of relevant matters in respect of your business.

Failure to meet with reporting obligations to the the Minister in respect of Sanctions is a criminal offence.

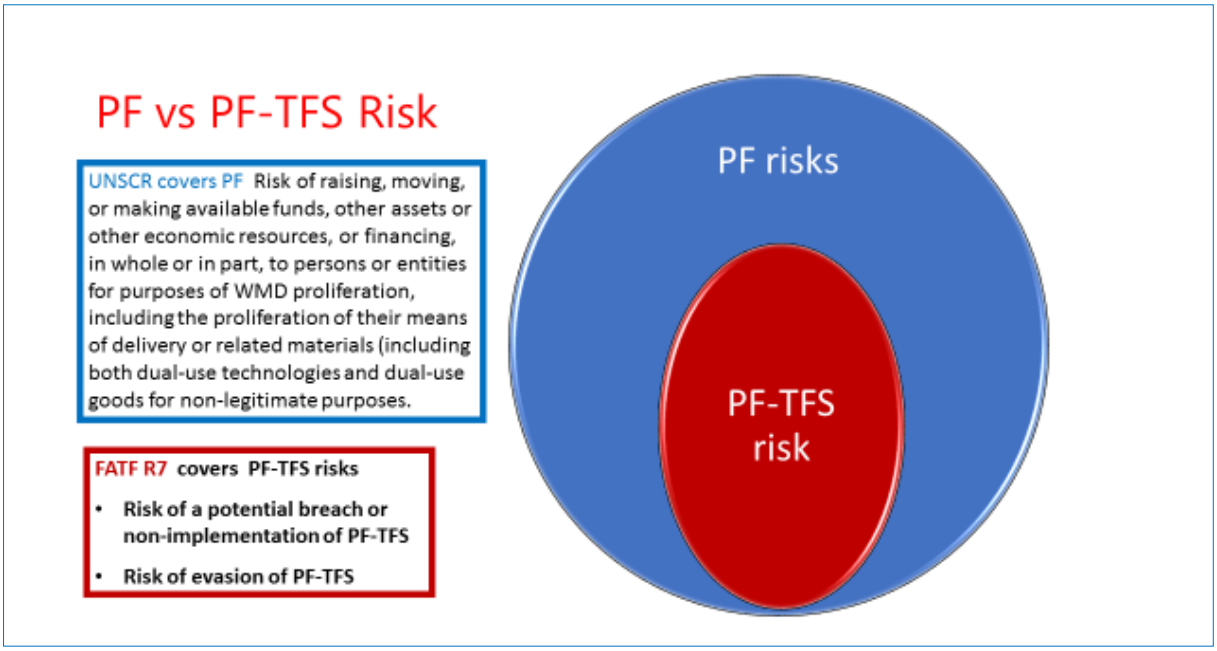
PF risk assessment and mitigation

In the context of FATF Recommendation 1, PF risk refers strictly and only to the potential breach, non-implementation or evasion of the TFS-PF obligations referred to in FATF Recommendation 7.

FATF Recommendation 7 sets out strict obligations to implement, without delay, TFS-PF related to two country specific regimes:

- The Democratic People's Republic of Korea (DPRK)
- Iran (Nuclear).

FATF uses a narrow definition of PF risk to access countries' compliance with this obligation as illustrated on the diagram below. It is the responsibility of Supervised Persons to understand these risks and adopt adequate policies and procedures to identify, assess, monitor, manage and mitigate them.



Rules-based approach

A rules-based approach provides for screening customers and their associates and relevant third parties against relevant designations lists. Since sanctions are tailor-made for specific risks and specific countries, they cannot serve as a model for developing a general risk-based approach to combat PF. These obligations are not risk-based, instead they are **mandatory in any risk scenario.**

The rules-based criteria to address TFS-PF risk may include a possible sanctions match (name match or other match, e.g. address, telephone number) with:

- A designated party, or
- A party owned or controlled by designated party, or
- A party acting on behalf or under the direction of designated party, or
- A record of export-control or related violations sanctions match.

Risk-based approach

Risk-based measures seek to reinforce and complement the full implementation of FATF Recommendation 7, under which Supervised Persons should identify, assess and understand their TFS-PF risks when dealing with their customers, and take appropriate mitigating action commensurate with the level of risks identified.

A risk-based approach requires wider screening of sources of PF, such as lists of designations under other sanctions regimes in other jurisdictions, customised to a Supervised Person's database, geographical links and other associations relevant to PF. For example, some of the entities and individuals, identified by the UNSC's Panel of Experts' reports on DPRK, may not have been sanctioned formally by the UN, but still maintain a significant involvement in PF.

Introducing measures should be proportionate to the overall Proliferation risk associated with the nature, types, and complexity of services provided by the Supervised Person, or its customer types,

geographical distribution of its customers and/or beneficial owners, and channels of distribution. For example, a business operating internationally or with an international client base will generally involve the assessment of a wider range of risks.

There are a number of non-governmental sources that can be consulted for advice on PF evasive patterns and potential exposure to PF risks, including detailed case studies. A list of examples of such sources can be found in **Annex C** – Sources for PF case studies**.**

The following section provides examples of risks factors which may be relevant to formulating a Proliferation focussed risk assessment within existing sanctions, or general compliance monitoring programmes.

PF risks categories

Country/geographic risk

Connections to certain countries may indicate a higher PF risk, for example:

- Commercial or business ties, or financial relationships (such as correspondent banking relationships) with a country that is subject to UN sanctions imposing WMD-related restrictions (DPRK and Iran, or countries in their close proximity)
- Commercial or business ties, or financial relationships (such as correspondent banking relationships) in countries with diplomatic, trade, or corporate links to States of Proliferation concern, or in their close proximity, for example, countries involved in Proliferation networks identified in the UNSC's Panel of Experts' reports
- Links with countries subject to other WMD Proliferation restrictions, for example, an "embargoed destination" or other Proliferation concern countries' lists identified in Schedules 1 to 4 of the UK's Export Control Order 2008
- Links with countries presenting on-going and substantial financial crime risks, for example countries with strategic trade controls deficiencies identified by the Peddling Peril Index (PPI)
- Other relevant factors could include countries with high levels of terrorist activities, corruption, civil unrest, organised crime related to arms dealing etc.

Customer risk

Categories of customers whose activities may indicate a higher PF risk could for example include:

- Those on national lists concerning WMD Proliferation
- A military or research body connected with a higher-risk jurisdiction of Proliferation concern
- Any customer or counterparty involved in the manufacture, supply, purchase, or sale of Dual use items, Proliferation-sensitive or military goods
- A customer who is a small trader/intermediary, who may be a dual-national of country of Proliferation concern
- A customer located in a major financial or trade centre
- Customers involved in the maritime industry, particularly those that own, operate, and/or provide services to ships operating in areas identified as posing a high risk for sanctions evasion

- A university or research institution with nuclear physics or related technical department with a history of violations of sanctions or export controls.

Product and services risk

The following may suggest higher PF risks:

- Delivery of services possibly subject to sanctions, e.g. correspondent banking services with institutions subject to UN DPRK sanctions
- Project financing of sensitive industries in jurisdictions of Proliferation concern
- Trade finance services, transactions, and insurance products involving jurisdictions of Proliferation concern (for example, direct loans or a general credit facility to facilitate export transactions; purchase of promissory notes or bills of exchange issued by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter; factoring - the purchase or discounting of a foreign account receivable for cash at a discount from the face value; provision of guarantees to or by financial institutions on behalf of exporters such as pre-shipment guarantees and performance guarantees; or provision of insurance against certain risks in the trading process)
- Transfer of Dual use items, Proliferation-sensitive goods and materials to a country of Diversion concern. **Diversion** refers to transactions that diverge funds/resources away from their legitimately intended purpose to benefit Proliferators, directly or indirectly
- Maritime insurance and re-insurance services.

In order to counter PF, a risk-based approach should be designed to emphasise the areas of greatest perceived vulnerability for a person or entity engaged in the breach, non-implementation, or evasion of TFS-PF.

As well as risk factors, mitigating factors should also be considered. For example, whether a customer is aware of Proliferation risks and has systems and processes in place to ensure its compliance with export control obligations, and can provide copies of valid export control licences.

Effective approach to PF risk mitigation

Supervised Persons should implement effective TFS-PF risk mitigation strategies to ensure that they are not directly or indirectly dealing with those subject to sanctions. The table below provides some examples.

Risks identified	Examples of vulnerabilities	Examples of mitigation measures
Risk of a potential breach or non-implementation of TFS-PF	› Weak customer on-boarding procedures › Inadequate on-going transaction monitoring and sanctions screening procedures and processes (e.g. use of out-of-date sanctions lists and lack of accuracy in matching names to those lists) › Non-existent or otherwise ineffective staff training › Ineffective risk management procedures	› Adequate and effective on-boarding processes and procedures for customers (including beneficial owners and controllers and their associates) › Enhanced customer due diligence procedures › Effective maintenance of customer data › Maintaining and managing Internal watch lists of customers/associated parties/ships/aircraft/entities/persons identified as potentially related to the TFS-PF designations

Risks identified	Examples of vulnerabilities	Examples of mitigation measures
	› Not having a healthy compliance culture (e.g. poor governance and risk management practices, highly action-orientated at the expense of compliance, lack of transparency and poor accountability) › Inadequate and ineffective internal controls (e.g. inadequate customer due diligence and record-keeping procedures and practices) › Lack of enhanced TFS-PF controls such as screening of direct and indirect third parties and associates, extended supply chain parties, third parties payees, Dual use items or other restricted items, in identified high risk scenarios with connections to jurisdictions known to have strong links to the enhanced risk states.	› Adequate controls to ensure effectiveness of procedures for sanctions screening to identify and mitigate potential sanctions evasion › Maintaining sound processes and internal controls, ensuring these are followed › Providing staff training to include PF risks, typologies, required risk mitigation measures, policies and procedures › Timely monitoring and incorporation of amendments to UN designations › Demonstrating awareness of entities and persons who are not designated, but who are known from reliable and independent third party sources to have connections to Proliferation activities.
Risk of evasion of financial sanctions	› Lack of understanding of the risks of potential sanctions evasion and what it may look like › Absence of tailored, risk-based measures to mitigate sanctions evasion › Absence of screening of customers' and their subsidiaries' undrelying assets, such as ships, aircrafts etc. › Outsourcing sanctions screening and reliance on Group policies and third parties providers without proper controls and testing of their functions	› Incorporation of, and continued review and update of, relevant sanctions evasion information into internal risk management policies and procedures › Tailored sanctions staff training › Supplementing reliance on list-based screening by enhanced customer due diligence measures to also capture indirect relationships and underlying assets which may be included on a sanctions list. › Understanding the overall structuring and rationale. › Maintaining documentation which clearly sets out who is responsible for the sceening systems within a Group and maintain access to that function

The FCA Financial Crime Guide provides some examples of good and poor practice of TFS-PF compliance, namely:

Examples of good practice	Examples of poor practice

Examples of good practice	Examples of poor practice
Screening information is contained within trade documents against applicable sanctions lists	Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively
Hits are investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made	Failure to screen trade documentation, failure to document decision-making
Shipping container numbers are validated on a risk-sensitive basis	Failure to screen against all relevant international sanctions lists
Potential sanctions matches are screened for at several key stages of a transaction	Failure to keep-up-to-date with the latest information regarding name changes for sanctioned entities, especially as the information may not be reflected immediately on relevant sanctions lists
Previous sanction alerts are analysed to identify situations where true hits are most likely to occur and the bank focuses its sanctions resources accordingly	Failure to record the rationale for decisions to discount false positives
New or amended information about a transaction is captured and screened	Failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin, as well as the main counterparties to a transaction
	Failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes
Ensuring staff are aware of Dual use item issues, common types of goods that have a dual use, and are capable of identifying red flags that suggest that Dual use items risk being supplied for illicit purposes	No clear Dual use items policy
Confirming with the exporter in higher risk situations whether a government licence is required for the transaction and seeking a copy of the licence where required	Failure to undertake further research where goods descriptions are unclear or vague
	Third party data sources are not used where possible to undertake checks on Dual use items

Risk indicators of the potential breach, non-implementation or evasion of TFS-PF

FATF PF risk indicators

In 2021, the FATF provided a non-exhaustive list of PF risk indicators related to a potential breach, non-implementation or evasion of TFS-PF. Having also taken into account other expert studies, the information in this section is based on PF typologies to provide greater understanding of wider PF risks.

Customer profile risk indicators

- During on-boarding, a customer provides vague or incomplete information about their proposed trading activities, appearing reluctant to provide additional information when further questions are raised.
- During initial or subsequent stages of the due diligence process, a customer, particularly a trade entity, its owners or senior managers, appear on sanctioned lists, or on a list of denied persons for the purposes of export control regimes, or in adverse news reports, e.g. alleging criminal activity, or on-going or past investigations or convictions.
- The customer is a person connected with a country of Proliferation or Diversion concern, e.g. through business or trade relations.
- The customer is a person dealing with Dual use items, or goods subject to export control goods, or complex equipment for which they lack technical background, or which is incongruent with their stated line of activity, or which otherwise does not appear to align with expectations.
- A customer engages in complex trade deals involving numerous third-party intermediaries, in lines of business that do not accord with their stated business profile as established during the on-boarding of the business.
- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest they are acting as if they were a money-remittance business or as a pay-through account. These accounts may involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons as to why this is. In some cases, the activity associated with originators appear to be entities who may be connected to a State-sponsored Proliferation programme (such as Shell companies operating near countries of Proliferation or Diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.
- A customer affiliated with a university or research institution is involved in the trading of Dual use items or goods subject to export control.
- A customer deals, directly or indirectly, with trade of sanctioned goods or under embargo, such as oil or other commodities, luxury goods, metals etc.

Account and transaction activity risk indicators

- The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of Proliferation or Diversion concern (e.g. DPRK and Iran).

- Account holders conduct transactions that involve items controlled under Dual use- or export control regimes, or the account holders have previously violated requirements under Dual use or export control regimes.
- Accounts or transactions involve possible companies with opaque ownership structures, Front companies or Shell companies.
- Demonstrating links between representatives of companies exchanging goods, e.g. the same owners or management, same physical address, IP address or telephone number, or which otherwise indicates their activities may be co-ordinated.
- An account holder conducts financial transactions in an indirect manner, or in a manner that otherwise does not appear to make business sense.
- Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards, or a weak export control regime (also relevant to correspondent banking services).
- A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals.
- Transactions are made on the basis of ledger arrangements that remove the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance their accounts.
- A customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.

Trade finance risk indicators

- Prior to the account approval, the customer requests letter of credit for a trade transaction for shipment of Dual use items or goods subject to export control.
- Lack of full information or inconsistencies are identified in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Transactions include wire instructions or payment details from, or due to, parties not identified on the original letter of credit or other documentation.

Maritime sector risk indicators

- A trade entity is registered at an address that may be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.
- The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination.
- The destination of a shipment is different from the importer's location.
- Inconsistencies are identified across contracts, invoices, or other trade documents, e.g.
  - contradictions between the name of the exporting entity and the name of the recipient of the payment

  - differing prices on invoices and underlying contracts
  - discrepancies between the quantity, quality, volume or value of the actual commodities and their descriptions, or which otherwise do not appear to correctly reflect what is to be anticipated.
- Shipment of goods have a low declared value in comparison with the shipping cost.
- Shipment of goods is incompatible with the technical level of the country to which it is being shipped, e.g. semi-conductor manufacturing equipment being shipped to a country that has no electronics industry.
- Shipment of goods is made in an indirect fashion that cannot be easily explained, including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping (flags of convenience practices), or using a small or old fleet.
- Shipment of goods is inconsistent with normal geographic trade patterns, e.g. the destination country does not normally export or import the goods listed in the trade transaction documents.
- Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement of export control laws.
- Payment for imported commodities is made by an entity other than the consignee of the commodities for no clear economic reasons, e.g. by a Shell company or Front company not involved in the trade transaction.

Other non-tangible Proliferation and PF sensitive risk indicators

- Research agreements with, or training at, universities and research centres abroad.
- Acquisition of foreign licenses or patents.
- Merging with/absorbing/acquiring foreign companies producing sensitive or export control goods.

Annex A – PF sensitive and export control goods

Example documents

Nuclear Suppliers Group (NSG) – Nuclear materials and technology, including Dual use items.

Missile Technology Control Regime (MTCR) – Technology for WMD delivery systems.

Wassenaar Arrangement – Conventional arms trade and Dual use items.

The Australia Group – Materials and technology needed for chemical and biological weapons.

Zangger Committee – Technology needed in production of fissile nuclear material.

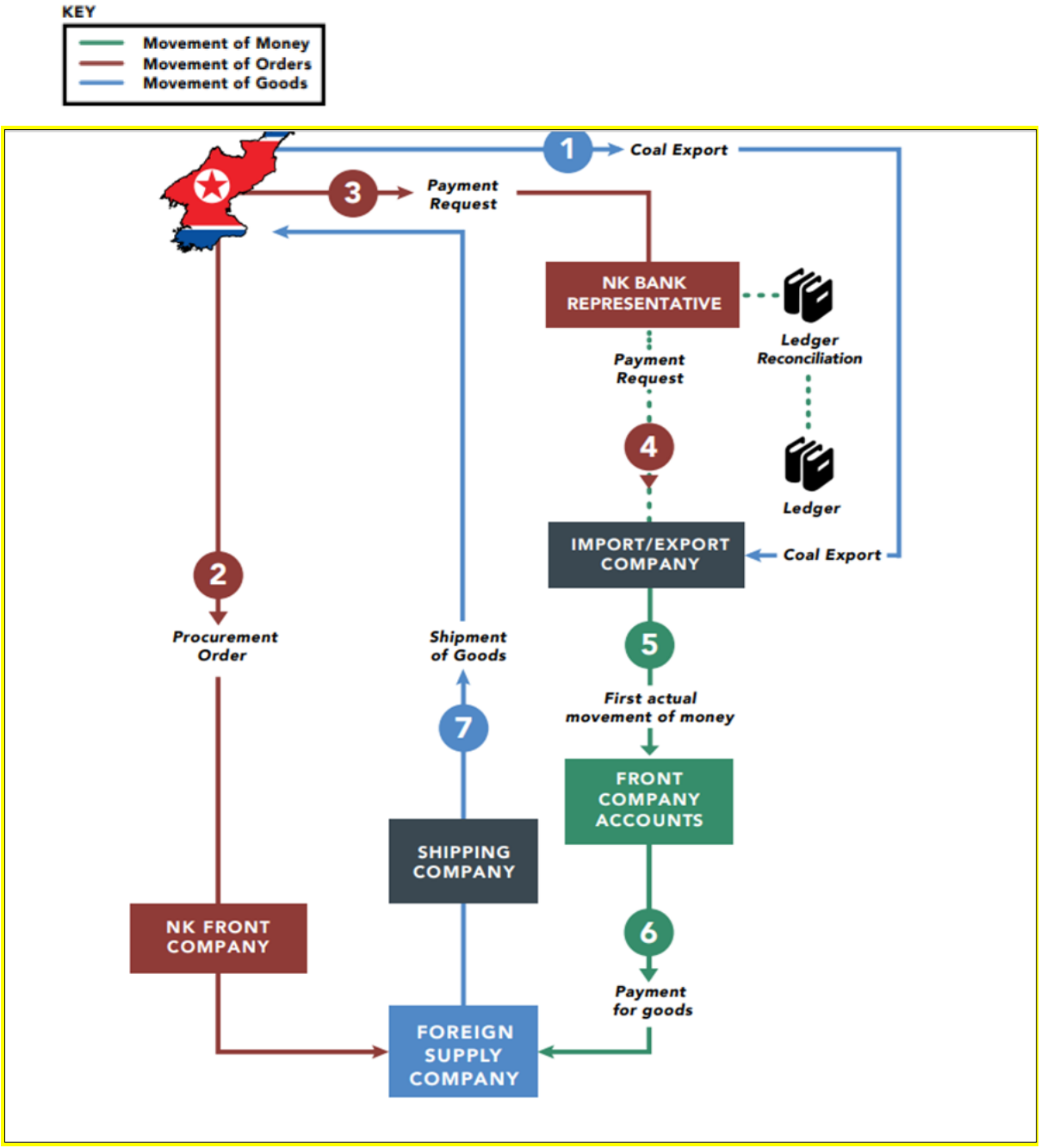
EU - List of all Dual use items and controlled items (Regulation (EU) 2021/821) and subsequent amendments.

UNSC (**DPRK Panel of Experts' reports** and **Iran designations List**)

UK lists of **Export control goods, Software and Technology**

Annex B – DPRK's use of the international financial system for Proliferation purposes

The diagram below illustrates an example of a DPRK trade based TFS-PF evasion scheme. These types of trade-based schemes allow the DPRK government to evade sanctions by directing payments for natural resource sales to its Front companies and Shell companies. The DPRK government use the laundered proceeds, through its Front companies and Shell companies, to access the international financial system to acquire technology for use in its WMD and ballistic missile programs. DPRK representatives also use these companies to establish bank accounts at local banks in foreign countries and take orders from sanctioned DPRK entities.



Source : FinCEN Advisory FIN-2017-A008

Annex C – Sources for PF case studies

Examples of sources for PF case studies:

International bodies:

- Annual Reports by the United Nations Panel of Experts established pursuant to resolution 1874 (DPRK). https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports
- FATF Typologies Report on Proliferation Financing, 18 June 2008. http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

Other sources:

- Project Alpha, Centre for Science and Security Studies at King's College, London. Comprehensive database of open-source PF case studies. https://acsss.info/
- James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey. Conducts research into non-proliferation and export controls. www.nonproliferation.org/
- 38 North, US-Korea Institute at the School of Advanced International Studies. Monitors nuclear and missile developments in DPRK through open-source materials. www.38north.org
- Stockholm International Peace Research Institute (SIPRI). Academic research on Dual use items and export control policies. www.sipri.org
- Royal United Services Institute (RUSI). Centre for Financial Crime and Security Studies. Projects: CPF Technical Assistance Programme, PF Risk Assessment, Project Sandstone. https://www.rusi.org
- Center for a New American Security (CNAS). Proliferation reports. https://www.cnas.org/
- Dr Tom Robinson, 'How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil' *Elliptic*, 21 May 2021 https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions#:~:text=Bypassing%20Sanctions%20%2D%20Through%20Bitcoin%20Mining&text=Iran%2Dbased%20miners%20are%20paid,financial%20institutions%20to%20be%20circumvented
- Sasha Erskine and Allison Owen, 'Compliance Harmony: How North Korean Cryptocurrency Abuse Is Expanding', RUSI, 14 July 2022 https://rusi.org/explore-our-research/publications/commentary/compliance-harmony-how-north-korean-cryptocurrency-abuse-expanding
- 'Iran makes first import order using cryptocurrency – report', *Reuters*, 9 August 2022 https://www.reuters.com/business/finance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09/
- Dr Daniel Salisbury, 'From Missions to Missiles: North Korea's Diplomats and Sanctions-Busting', RUSI, 14 November 2022, <https://static.rusi.org/343_EI_DPRK%20Diplomats.pdf
- Sasha Erskine, 'North Korean Proliferation Financing and Designated Non-Financial Businesses and Professions', RUSI, 5 January 2022 North Korean Proliferation Financing

and Designated Non-Financial Businesses and Professions | Royal United Services Institute (rusi.org)