# GUIDANCE ON COMBATTING PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND PROLIFERATION FINANCING

**20 December 2024**

ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

# TABLE OF CONTENTS

# A. INTRODUCTION

This Guidance Paper was prepared to provide guidelines to the regulated entities of Cyprus Securities and Exchange Commission (CySEC) for combatting the proliferation of weapons of mass destruction (WMD proliferation) and its financing. The Guidance Paper aims to promote awareness of the risks and vulnerabilities regarding WMD proliferation and proliferation financing, as well as the risks of non-compliance with domestic and international legal frameworks and the potential damages that could occur to regulated entities knowingly or unknowingly aiding proliferation financing.

The Guidance Paper provides some common definitions and a general understanding on WMD proliferation and Proliferation Financing (PF) and how it works. It also provides an overview of the domestic and international regulatory framework, together with international standards and obligations that are relevant to combatting PF risks. The identification, assessment, understanding and management of PF risks by the regulated entities is of vital importance. The Guidance Paper focuses also on PF indicators and red flags and the relevant risk management practices that the regulated entities should have in place to counter PF risks. The Guidance Paper also identifies types of Sanctions in relation to PF that may affect the regulated entities or their clients, maps out the characteristics of an effective PF risk assessment and provides recommended controls and mitigating measures to counter WMD proliferation and PF.

As a country whose financial services account for a large part of its GDP and those services are attributed to a large number of non-resident customers, the Republic of Cyprus must be vigilant to PF risks. Although no evidence currently exists that there are direct PF links between Cypriot entities and persons engaged in WMD proliferation activities, the exposure of the financial system when conducting international business and overseas financial transactions poses higher PF risks.

The information contained in this document is not supposed to be exhaustive, but rather to provide helpful considerations for CySEC's regulated entities on combatting WMD proliferation and PF. Each regulated entity is responsible for developing and implementing policies, procedures and controls to mitigate and manage their exposure to WMD proliferation and PF risks. The guidelines contained in this document are meant to be read in conjunction with relevant local and international standards and obligations, as mentioned below, and any other relevant guidance issued by CySEC on this topic.

# B. OVERVIEW

## What is proliferation and proliferation financing?

The FATF defines **proliferation of weapons of mass destruction** as *"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)"*. It includes technology, goods, software, services and expertise.

The FATF formed a working definition[1] for **Proliferation Financing (PF)** as *"The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations"*. The FATF adds that PF facilitates the movement and development of proliferation-sensitive items and can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction (WMD) are developed and deployed. Terrorism financing (TF) which supports terrorist organizations may also contribute to proliferation.

Proliferation financing takes place when a person makes available an asset, provides a financial service or conducts a financial transaction, and the person knows that, or is reckless as to whether the asset, financial service or financial transaction is intended, in whole or in part, to facilitate any of the proliferation activities specified above, regardless of whether the specified activity occurred or attempted.

[1] FATF, February 2010, FATF Report: Combating Proliferation Financing: A Status Report on Policy Development and Consultation, p.5

Proliferation financing is very broad and refers to more than simply the payment for goods. Proliferation financing includes any financial service provided in support of any part of the process of procurement and financing of nuclear, chemical and biological weapons, even if such financing is not directly connected to the physical flow of the goods. Financing can include financial transfers, mortgages, credit lines, insurance services, trust and corporate services and company formation. Thus, proliferation financing risk can be described as both a financial crime risk and a sanctions risk.

## What are the stages of proliferation financing?

The Centre for a New American Security ("CNAS") published a report[2] that contains information on the financial elements of proliferation of WMD. These are divided into three stages:

- **First Stage - Fund Raising**: During this stage, the proliferator raises funds for the WMD program through its own budget or funds raised by overseas networks or by criminal activity.

- **Second Stage - Disguising the funds**: During this stage, the proliferator transfers the funds into the international financial system. This stage poses the highest risks for credit and financial institutions, and generally for regulated entities with clients' business relationships which involves access to the financial systems. The techniques/methods used by proliferators to disguise the funds and avoid detection are similar with money laundering (ML), and includes, among others:
  - ✓ use of legal entities and legal arrangements (i.e. trusts) to conduct business activities and execute financial transactions in an international environment

[2] CNAS, Dr. Jonathan Brewer, January 2018, The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, p.4-5

- ✓ use of complex ownership structures to obscure the ownership and control of their assets and the origin of funds
- ✓ use of 'strawmen' which acts on behalf of, or at the direction of a proliferator
- ✓ use of jurisdictions that have been associated or are near sanctioned countries for these purposes (i.e. North Korea and Iran)
- ✓ use of convertible virtual currencies.

For countries subject to targeted financial sanctions (TFS) for proliferation of WMD, such as North Korea and Iran, this stage presents the greatest challenges.

- **Third Stage - Procurement of materials and technology and shipping**: During this stage, the proliferator uses the funds entered the international financial system to pay for goods, materials, technology, and logistics needed for purchasing or developing weapons, including transactions with brokers and trading companies. Throughout this stage, credit and financial institutions will be involved in processing the related transactions.

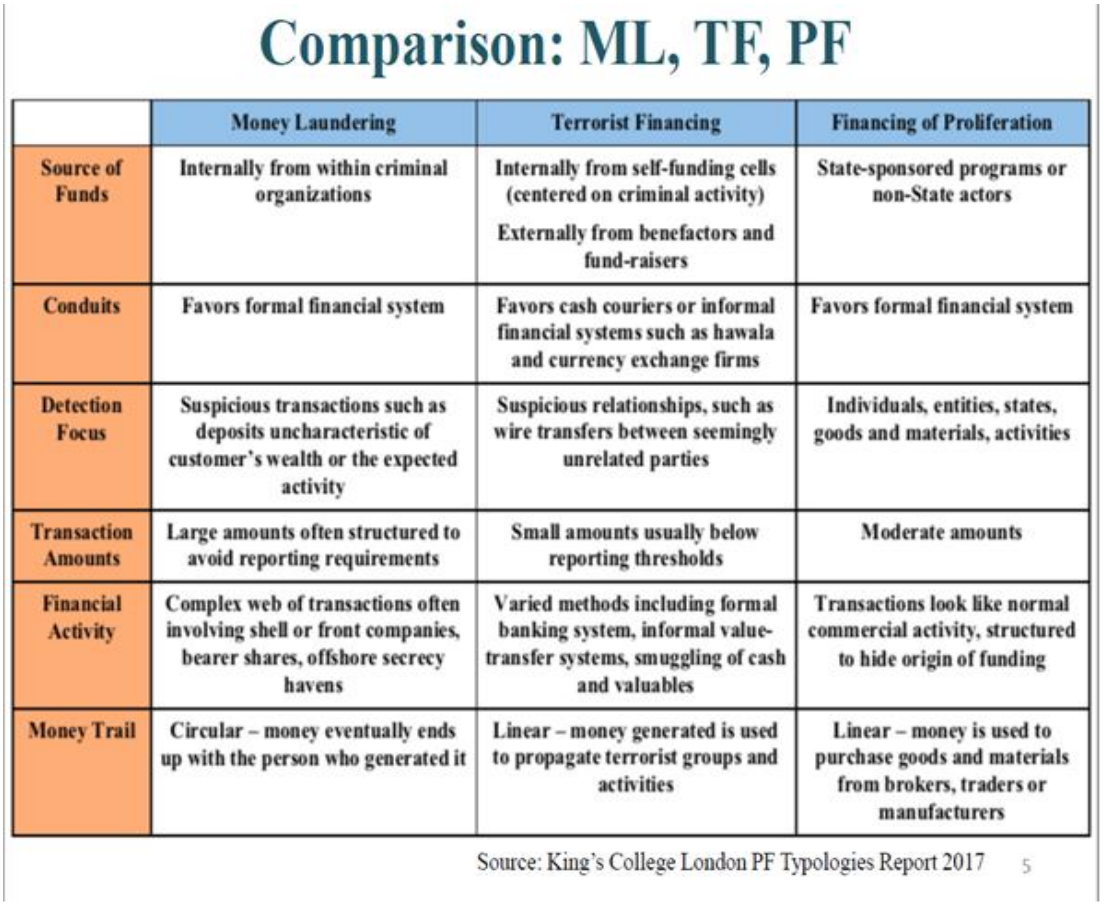
## Comparison between Money Laundering, Terrorism Financing and Proliferation Financing

Proliferation financing activities have differences and similar characteristics with ML/TF activities. While some risk indicators and control elements might overlap for ML, TF and PF, for example PF transactions may trigger ML risk indicators, PF has unique risk indicators and associated controls that regulated entities could implement. For example, given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or "red flags" for ML may be relevant in cases where the source of funds is illegal. **However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal, but the end-user or type of goods involved is intended to be obscured.** The structural differences and similarities between ML/TF and PF should therefore be considered when designing a compliance program for alerting on different ML/TF/PF risks indicators and sufficiently countering these risks.

Another example of differences between PF and ML/TF, is when the amount of a transaction is sometimes small (some materials used in the manufacture of WMD are not expensive), these transactions will not trigger ML suspicions during ongoing monitoring because these transactions are below a pre-determined threshold. In addition, PF networks are aware of ML triggers and could deliberately structure payments, transactions and corporate structures to avoid these triggers.

Figure 1 below provides a comparison of ML, TF and PF, and although, as pointed out above, they have similar characteristics, some differences exist that indicate the necessity for different considerations and approach on combatting PF.

**Figure 1**[3]



## Comparison: ML, TF, PF

| | Money Laundering | Terrorist Financing | Financing of Proliferation |
|---|---|---|---|
| Source of Funds | Internally from within criminal organizations | Internally from self-funding cells (centered on criminal activity)<br>Externally from benefactors and fund-raisers | State-sponsored programs or non-State actors |
| Conduits | Favors formal financial system | Favors cash couriers or informal financial systems such as hawala and currency exchange firms | Favors formal financial system |
| Detection Focus | Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity | Suspicious relationships, such as wire transfers between seemingly unrelated parties | Individuals, entities, states, goods and materials, activities |
| Transaction Amounts | Large amounts often structured to avoid reporting requirements | Small amounts usually below reporting thresholds | Moderate amounts |
| Financial Activity | Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens | Varied methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables | Transactions look like normal commercial activity, structured to hide origin of funding |
| Money Trail | Circular – money eventually ends up with the person who generated it | Linear – money generated is used to propagate terrorist groups and activities | Linear – money is used to purchase goods and materials from brokers, traders or manufacturers |

Source: King's College London PF Typologies Report 2017 5

[3] King's College London, Dr. Jonathan Brewer, October 2017, Study of Typologies of Financing of WMD Proliferation, p.35

## Challenges of detecting proliferation financing

Government authorities and regulated entities have to deal with many challenges when trying to detect PF and implement relevant PF controls, such as:

- The identification, assessment and countering of proliferation financing (CPF) can be difficult and complex. The networks of proliferators involved may be sophisticated and involve front and intermediary companies within complex structures that are operating in several different jurisdictions, the use of false documentation to obscure the end-use and end-user of the product/service, the use of several transshipment points before goods reach their target destination and the use of varying ways of accessing the financial system. It requires **specific training** to all relevant persons to **acquire the necessary knowledge and understanding** in detecting and countering PF.

- Although screening the lists of designated persons and entities known to be associated with proliferation (UN Sanctions/EU Restrictive Measures) is very important, **the reliance of regulated entities on screening transactions and customers on these lists for due diligence purposes might not always be effective**, as they do not cover the full extent of proliferation networks and activity. Proliferators are constantly engaging new persons or creating new entities in other jurisdictions to make it as difficult as possible to identify PF. Sometimes automatic software for KYC purposes, although necessary, cannot be effective. In many circumstances **manual checks on case-by-case basis might be needed.** Therefore, customer due diligence ('CDD') procedures should be adjusted to sufficiently address the PF component.

- Difficulties in identifying individuals and front companies which are potentially **acting on behalf** of the sanctioned entities/individuals ('Strawmen').

- A mistaken perception currently exists that WMD proliferation refers only to weapons and weapons components and not focusing on **dual-use goods and technology.** The goods and materials involved for the manufacturing of WMD are, for the most part, standard industrial or dual-use items (refer below for further information). Dual-use items, although subject to export controls, are very hard to identify, as these materials and components have a dual-use nature, where they can be used both for civil and military purposes. Technical expertise and knowledge are needed on dual-use items (goods or technology), as **it is very challenging to ascertain their intended use and ultimately whether their end use would be for legitimate or illicit purposes.**

- Proliferation financing can occur during usual business transactions, where the **source of funds is legitimate**, thus making it difficult to detect and counter it.

- For some types of regulated entities that are non-banks and are smaller in size and resources, there is **limited capacity for activity-based checks/analysis** i.e. limited information on transactions, insufficient CDD procedures on PF component, not sufficient technical expertise and knowledge on dual-use goods and technology, therefore there is a structural inability to detect relevant activities and transactions on WMD proliferation and PF.

- **Lack of coordination and information sharing between relevant actors** (credit and financial institutions, corporate service providers, import/export control authorities, Customs, Border Control, FIU and Law Enforcement). This **lack of transparency** and opaque processes on data-sharing (i.e. confidentiality rules) allow for WMD proliferation-sensitive goods and technology, the entities involved, the linked transactions and the ultimate end-user to avoid detection and disruption of proliferation networks, thus significantly increasing PF risk.

- This topic has not yet been prioritized and extensively researched by many jurisdictions, making it challenging to assess and identify through relevant

experience, the risks and typologies associated with proliferation financing. Therefore, in many countries, there is **limited guidance and targeted training** from relevant government authorities to promote awareness to their supervised entities on WMD proliferation and the risks and typologies associated with PF.

## How could WMD proliferation and its financing be combatted?

Countries could target WMD proliferation and its financing through **export controls** and **financial measures**.

Proliferating actors are known to exploit global trading practices by operating in countries with weak export controls, countries with large volume of international trades and free-trade zones where their activities are less likely to be detected. Export controls are the primary safeguard to counter WMD proliferation activities and should be focused on preventing illicit trade of proliferation-sensitive goods.

Financial measures that are targeting activities/transactions linked with WMD proliferation and its financing are supplemental to effective export controls. Proliferation networks will try using the international financial system to carry out transactions. Regulated entities should be alert to the possibility that any customer may be engaging or facilitating WMD proliferation and its financing. In order to combat WMD proliferation and its financing effectively, **the regulated entities should have awareness of the legal framework and their obligations (refer to section C below), conduct a PF risk assessment (refer to section D below) and implement risk mitigating measures and controls (refer to section E below), such as sanctions screening procedures and enhanced due diligence for customers and transactions linked with the supply chain of dual-use goods or WMD proliferation goods or trade finance, to address the findings of the PF risk assessment.**

## Dual-use items and export controls

Proliferation financing is usually linked with trading in dual-use goods, software and technology. **Dual-use goods, software and technology are items that can be used for both civilian and military applications, such as sensors, transistors, high-capacity batteries, lasers and other high-end electronics, as such they could be easily exploited by proliferators for their purposes.** These dual-use items could be components of a weapon or machines to manufacture a weapon that also have civil applications, for example, high-capacity batteries developed for consumer electronics that can be adapted for military use in portable equipment and vehicles or nickel aluminides can be used in the production of household glass containers but also for aircraft engine blade coating.

The EU Commission maintains and continuously updates a **control list of dual-use items** (refer to Regulation (EU) 2021/821 of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, and subsequent amendments to the list of dual-use items, such as the most recent Commission Delegated Regulation (EU) 2024/2547 of 5 September 2024), which every EU Member State should be monitoring accordingly. Many of these dual-use items are subject to exports control restrictions. Even if some items do not appear on lists of dual-use items, they still might be subject to scrutiny and monitoring if their intended use would end up for illicit proliferation purposes.

# C. DOMESTIC AND INTERNATIONAL LEGAL FRAMEWORK AND OBLIGATIONS

The legal framework for combatting proliferation of WMD and proliferation financing relies on the following international and domestic legal obligations, which impose requirements that should impact the risk management procedures and practices of all entities affected:

- The provisions of the United Nations Security Council Resolutions or Decisions ('UN Sanctions')
- The European Union Council's Decisions and Regulations ('EU Restrictive Measures')
- The Financial Action Task Force ('FATF') recommendations
- The domestic legislation, national requirements of each Supervisory authority from its respective regulated entities and the National Risk Assessment on PF (not yet conducted for Cyprus).

## The UN Security Council Resolutions

EU Member States are required to comply and implement in a mandatory way the United Nations Security Council Resolutions ('UNSCRs') relating to WMD proliferation and proliferation financing. These UNSCRs require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any designated person or entity.

The UN Security Council has adopted a two-tier approach, which includes both the implementation of broad provisions covering all "non-state actors", as well as targeting jurisdictions who have been specifically identified for WMD proliferation i.e. "state actors". Thus far, the UN Security Council has passed three UNSCRs relating to combatting WMD proliferation. Two resolutions are targeting specific jurisdictions, those are UNSCR

1718 for Democratic People's Republic of Korea ('DPRK') and UNSCR 2231 for Islamic Republic of Iran ('Iran'). These two countries are referred as "state actors" who are specifically targeted for proliferation of WMD. The third resolution is UNSCR 1540, which works independently (non-country specific) and covers "non-state actors", meaning any individual or entity which is not acting on behalf of any jurisdiction/state.

## ❖ UNSCR 1540 (2004)

UN Security Council Resolution 1540 (2004) are broad-based provisions **prohibiting the financing of proliferation-related activities by non-state actors** and are requiring countries to establish, develop, review and maintain appropriate controls on preventing the financing of activities related to the export and transshipment of items that would contribute to proliferation of WMD. UNSCR 1540 ultimately is seeking to prevent "non-state actors" from obtaining weapons of mass destruction. Non-state actors might include intergovernmental organizations, non-governmental organizations, global corporations, civil societies, terrorist organisations, religious actors, etc.

UNSCR 1540 establishes **obligations on countries** to:

1) Prohibit support to non-state actors seeking WMD, their means of delivery and related materials and components.
2) Adopt and enforce effective laws for prohibiting the proliferation of such items to non-state actors and prohibiting assisting or financing proliferation.
3) Take and enforce effective measures to control these items, in order to prevent their proliferation, as well as to control the provision of funds and services that contribute to proliferation.

## ❖ UNSCR 1718 (2006) on DPRK and UNSCR 2231 (2015) on Iran

The UN Security Council has imposed targeted financial sanctions on DPRK and Iran in relation to their activities on proliferation of WMD. These two countries are referred as

**state actors** and are specifically targeted for WMD proliferation. The sanctions regimes adopted fall under:

- UNSCR 1718 (2006), and all successor resolutions concerning the DPRK.
- UNSCR 2231 (2015), endorsing Joint Comprehensive Plan of Action on Iran and replacing previous resolutions to Iran.

The above-mentioned UNSCRs establish a series of obligations on UN member states relating to the DPRK and Iran. These obligations include the use of targeted financial sanctions against designated individuals and entities listed on both UNSCRs, as well as people acting on behalf, or at the direction of designated persons or entities, or entities owned/controlled by designated persons or entities. Each UNSCR contains specific measures related to DPRK and Iran and prohibitions against the provision of certain activities and services.

## EU Restrictive Measures

The EU has also adopted targeted Restrictive Measures against DPRK and Iran, namely:

- 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.
- Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010.

Furthermore, as discussed above, the EU Commission has published a list of dual-use items for exports control (refer to Regulation (EU) 2021/821 of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, and subsequent amendments to the list of dual-use items, such as the most recent Commission Delegated Regulation (EU) 2024/2547 of 5 September

2024), which every EU Member State should be monitoring accordingly. The EU controls the export, transit, brokering, technical assistance, transit and transfer of dual-use items so that it can contribute to international peace and security and prevent WMD proliferation (refer to the Dual-use export controls webpage).

## ❖ The EU export control regime

Regulation (EU) 2021/821 governs the EU export control regime, which includes:

- common export control rules, including a common set of assessment criteria and common types of authorisations (individual, global and general authorisations)
- a common EU list of dual-use items
- common provisions for end-use controls on non-listed items, which could be used for example in connection with a WMD programme or for human rights violations
- controls on brokering and technical assistance relating to dual-use items and their transit through the EU
- specific control measures and compliance to be introduced by exporters, such as record-keeping and registers, and
- provisions setting up a network of competent authorities supporting the exchange of information and the consistent implementation and enforcement of controls throughout the EU.

In certain cases, EU Member States may introduce additional controls on non-listed dual-use items because of public security or human rights considerations. Dual-use items may be traded freely within the EU, except for some particularly sensitive items, whose transfer within the EU remains subject to prior authorisation (refer to Annex IV of the Regulation (EU) 2021/821).

There are four types of dual-use items export authorisations in place in the EU export control regime:

- EU General Export Authorisations (EUGEAs), which allow exports of dual-use items to certain destinations under certain conditions (refer to Annex II of Regulation (EU) 2021/821).
- National General Export Authorisations (NGEAs), which are issued by EU Member States if they are consistent with existing EUGEAs and do not refer to items listed in Annex IIg of Regulation (EU) 2021/821.
- Global licenses, which can be granted by competent authorities to one exporter and may cover multiple items to multiple countries of destination or end users.
- Individual licenses, which can be granted by competent authorities to one exporter and cover exports of one or more dual-use items to one end-user or consignee in a third country.

## ❖ Russia's military aggression against Ukraine

Since the start of the war in Ukraine during February 2022 and the subsequent EU Restrictive Measures imposed against Russia and Belarus, the EU Commission have published general guidelines and **Frequently asked questions ('FAQs') on export-related restrictions** against Russia and Belarus for dual-use goods and advanced technologies (last updated on 26 July 2024). These FAQs focuses on the provisions of Council Regulation (EU) No 833/2014 and provides an updated Correlation table on the Goods listed in Annex VII of Council Regulation (EU) No 833/2014.

Additionally, the EU have published the **Economically Critical Goods List**, which comprised of mainly industrial goods subject to EU restrictive measures (trade sanctions under Council Regulation (EU) No 833/2014) for which anomalous trade flows via certain third countries to Russia have been detected. Furthermore, the EU and its international partners have published the **List of High Priority Battlefield Items**, which contains a number of prohibited dual-use goods and advanced technology items used in Russian military systems found on the battlefield in Ukraine or critical to the development, production or use of those Russian military systems. These lists may support due diligence

and compliance efforts by relevant parties for targeted and effective anti-circumvention actions. The EU Commission have also published **Frequently asked questions ('FAQs') on enhanced due diligence for operators manufacturing and/or trading with CHP items** (last updated on 11 December 2024).

## The FATF Recommendations

The FATF Recommendations (last updated November 2023) set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of WMD. The following Recommendations are setting out specific requirements for implementing procedures and controls for the prevention and suppression of proliferation and proliferation financing:

- **Recommendation 1** – Countries and private sector entities are required to identify, assess, understand and mitigate PF risks.

- **Recommendation 2** – Countries should ensure that policy-makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy making and operational levels, have effective mechanisms in place 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 financing of proliferation of WMD. The most important standard that is introduced is the necessity for domestic coordination and information sharing on PF between export control authorities and AML/CFT supervision authorities.

- **Recommendation 7** – Countries should **implement Targeted Financial Sanctions** ('TFS') to comply with UNSCRs relating to the prevention, suppression and disruption

of proliferation of weapons of mass destruction and its financing. Countries should **freeze without delay** the funds or other assets of, and ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated person or entity. Countries should have mechanisms in place for communicating designations to obliged entities immediately and provide guidance on their freezing obligations. Obliged entities should report on any actions taken and any assets frozen. Furthermore, countries should adopt measures for monitoring and ensuring compliance by obliged entities with the relevant laws or enforceable means governing the TFS-related obligations and failure to comply should be subject to civil, administrative or criminal sanctions.

- **Recommendation 15** – The FATF has responded to the threat of illicit proliferation of WMD by updating Recommendation 15 in June 2021 to include specific requirements and measures on the implementation of TFS related to proliferation by Virtual Asset Service Providers ('VASPs'). Countries are required to identify and assess the PF risks related to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for new and existing products.

The FATF Methodology (last updated August 2024), besides assessing technical compliance with the FATF Recommendations, it also focuses on the **effectiveness of AML/CFT systems.** A country must demonstrate that, in the context of the risks it is exposed to, it has an effective framework to protect the financial system from abuse. The assessment will look at 11 key areas, or Immediate Outcomes, to determine the level of effectiveness of a country's AML/CFT system.

**Immediate Outcome 1** is evaluating effectiveness of countries on the level of national cooperation and coordination on combating WMD proliferation and PF.

**Immediate Outcome 11** is targeted towards Proliferation financial sanctions: Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant United Nations Security Council Resolutions. One of the core issues to be considered in determining if Immediate Outcome 11 is being achieved is the extent that obliged entities within a country comply with and understand their obligations regarding targeted financial sanctions relating to financing of proliferation. FATF Methodology describes the characteristics of an effective system towards compliance to Immediate Outcome 11 as:

*"Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD."*

Following the Mutual Evaluation Report ('MER') of Cyprus by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism ('MONEYVAL'), as published in December 2019, Cyprus was rated as Largely Compliant for Recommendations 1, 2, 7 and 15 (re-rated as per the MONEYVAL's Follow-up Evaluation Report of December 2023[4]) and as having a Moderate level of Effectiveness for Immediate Outcome 11[5]. The Mutual Evaluation Report of Cyprus is providing Key Findings and Recommended Actions on Immediate Outcome 11[6], which includes, among others, the need to provide guidance on PF-related TFS to regulated entities.

[4] Third Enhanced Follow-up Report & Technical Compliance Re-Rating of Cyprus, MONEYVAL, December 2023, p.4
[5] Mutual Evaluation Report of Cyprus, December 2019, MONEYVAL, p.12
[6] Mutual Evaluation Report of Cyprus, December 2019, MONEYVAL, p.80-83

Considering lessons learned from the fourth-round results[7] of FATF mutual assessments conducted to countries and their respective MERs, compliance levels with Recommendation 7 and Immediate Outcome 11 are relatively low. Most countries are partially or non-compliant with Recommendation 7, as they have not yet developed the legal framework to implement, without delay, TFS related to PF. Countries are also experiencing shortfalls in identifying assets held by those acting on behalf of designated entities and communicating and enforcing clear policies related to listings/delisting/exemptions for covered private sector entities. This impacts effectiveness levels for Immediate Outcome 11, with 52% of FATF members and 82% of FATF-style regional body members rated either low or moderate. Private entities have varying degrees of awareness of their reporting obligations on PF. In more than two-thirds of countries, financial institutions demonstrate on average a medium-to-high understanding of their obligations regarding TFS for PF. However, designated non-financial businesses and professions have poor to unclear understanding in 70% of cases.

## Cyprus legal framework

The Republic of Cyprus, as a UN member and an EU Member State has an obligation to implement:

- Sanctions adopted by the relevant Security Council Resolution pursuant to Article 41 of Chapter VII of the Charter of the United Nations, which have direct and immediate application in the Republic of Cyprus. This is in accordance with Law 58(I) of 2016 which provides for the Implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and the Decisions and Regulations of the Council of the European Union (Restrictive Measures). In addition, the EU, and consequently the Republic of Cyprus, implement UN sanctions by

[7] FATF REPORT ON THE STATE OF EFFECTIVENESS AND COMPLIANCE WITH THE FATF STANDARDS, April 2022, p.46

incorporating them into EU law, through the adoption of relevant Decisions and Regulations within the framework of the Common Foreign and Security Policy.

- Restrictive measures adopted by the Council of the European Union, through the issuance of relevant Decisions (under Article 29 of the Treaty on European Union) and Regulations (under Article 215 of the Treaty on the Functioning of the EU), within the framework of the CFSP, which supersede national law. These are binding legal acts in their entirety for EU Member States and their citizens, requiring direct and immediate application to the integral legal order of EU Member States.

- Any other European legislation or legally binding international instrument related to Sanctions and Restrictive Measures.

As an EU Member State, Cyprus has the obligation to implement the Restrictive Measures of the Decisions/Regulations adopted by the EU Council. EU Restrictive measures are **directly enforceable** to Cyprus, without the need to transpose the relevant acts/provisions into national legislation. Other sanctions regimes are also relevant in Cyprus i.e. U.S. Sanctions, for example for US-dollar transactions taking place in Cyprus.

- The law that provides for the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions and the European Union Council's Decisions and Regulations in Cyprus is Law 58(I)/2016. In accordance with the said Law, the regulated entities are responsible to comply with the UN Sanctions and EU Restrictive Measures, such as:

  - Section 3(1) designates the competent authorities for securing the implementation of Sanctions/Restrictive Measures in Cyprus, and these are defined in accordance with the provisions of section 59 of the Prevention and Suppression of Money Laundering Activities Laws of 2007, as amended.

- Section 4 provides for strict penalties for non-compliance (including the possibility of imprisonment and criminal prosecution).
- Section 6 provides for the transmission of data/information to the Police, in case a competent authority, ascertains that a person does any act in violation of Sanctions and Restrictive Measures.

➢ CySEC's Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing of 2020, as amended **('CySEC's AML/CFT Directive')**, and specifically paragraph 36 on the detention of actions that are in breach of Sanctions/Restrictive Measures, serve as secondary legislation for compliance with Sanctions and Restrictive Measures.

**Paragraph 36 of CySEC's AML Directive provides for the detention of actions that are in breach of Sanctions/Restrictive Measures.** The regulated entities have the obligation to design and implement measures and procedures for the detection of actions that are in breach or may potentially be in breach of the provisions of Sanctions/Restrictive Measures. The regulated entities shall record in their Risk Management and Procedures Manual regarding money laundering and terrorist financing the measures and procedures for the detection of actions that are in breach or may potentially be in breach of the provisions of Sanctions/Restrictive Measures.

CySEC is providing **relevant guidance** to its regulated entities for the implementation of the provisions of the UN Sanctions and EU Restrictive Measures through the section 'Sanctions/Restrictive Measures' on CySEC's website, such us information on existing legal framework, useful links, updated guidelines and FAQs from relevant competent authorities, notifications on new or amending designations of sanctioned persons and entities as the result of UN Resolutions or EU Decisions/Regulations, notifications on any national and international announcement, etc. CySEC is also issuing **Circulars** to inform its regulated entities when important developments occurred on

Sanctions/Restrictive Measures, such as Circulars C474, C489, C494, C501, C556, C570, C622 and C635.

CySEC has also published a **practical guide** on the implementation of Sanctions and Restrictive Measures to support its regulated entities. The said guide provides, amongst others, for the characteristics and legal framework of Sanctions and Restrictive Measures, general considerations and examples and best practices for understanding and implementing Sanctions and Restrictive Measures, an analysis of the EU Restrictive Measures against Russia and relevant obligations of the regulated entities, guidance for the prevention of sanctions evasion and guidance for the elements of an effective Sanctions Compliance Program.

- Furthermore, the **Combating of Terrorism and Victims' Protection Law of 2019,** as amended (Law 75(I)/2019, only in Greek) deals with a number of issues, including the definition of terrorism felonies, the responsibilities of legal persons, responsibility of entities obliged under the AML/CFT Law to confiscate property belonging or controlled by persons engaged in terrorism and the responsibility of supervisory authorities for ensuring that regulated entities abide with the provisions of this law.

- The Cyprus Legal framework also consists of **the Import and Export of Controlled Items and the Conduct of Controlled Activities Law of 2011**, as amended, (Law 1(I)/2011, only in Greek). The said Law, as well as the Regulations and Decrees issued based on it, regulates the licencing of imports and exports of controlled items, such as dual-use goods, arms and military equipment, and the conduct of controlled activities, with the aim of promoting the objectives of the EU's Common Foreign and Security Policy, the promotion of the foreign policy of the Republic of Cyprus and/or the fight against organized crime and international terrorism. Further information is available from an announcement of the Ministry of Energy, Commerce and Industry on Law 1(I)/2011 (including issued separate Regulations based on the Law on dual-use goods, arms and military equipment).

- Breaching the provisions of any of the Laws referred above constitute a serious offence, which may trigger significant penalties/damages, such as:

  - **Criminal penalties:** Law 58(I)/2016 provides for strict penalties for non-compliance with Sanctions/Restrictive Measures. If a natural person is found guilty of an offence, they may be subject to imprisonment not exceeding 2 years or a pecuniary penalty not exceeding €100,000 or both. In the case of a legal person, it may be subject to a pecuniary penalty not exceeding €300,000. Criminal prosecution may be carried out with the approval of the Attorney General.
  - **Administrative penalties:** For implementing Law 58(I)/2016, the competent authorities may also take administrative measures in accordance with the provisions of Section 59(6) of the AML/CFT Law. These includes the possibility of fines up to €5.000.000 and/or suspension, or withdrawal, of the regulated entity's license.
  - **Reputational damages:** The consequences of reputational damage are very high and possible losses will certainly be higher than any administrative penalty imposed, if the name of a regulated entity is linked or associated with a sanctioned person who has committed sanctions-related violations.

- CySEC has added the section "Terrorism Financing (TF)/Proliferation Financing (PF)" on CySEC's website to provide **useful information and publications on TF/PF** to its regulated entities, as well as relevant notifications, when available. Through Circular C647, CySEC urges the regulated entities to continuously monitor, inter alia, the said section on CySEC's website, including notifications for useful information and publications on TF/PF, ensuring their full compliance with their relevant legal obligations for preventing TF and PF.

# D. RISK ASSESSMENT

The financing of proliferation refers to 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). An **understanding of the risks of WMD proliferation and its financing** will have a positive contribution to the understanding of risks of breach, non-implementation or evasion of PF-related sanctions and will assist in implementing effective preventive measures and controls.

According to FATF guidance[8], PF risk can be seen as a function of three factors: **threat, vulnerability, and consequence**. A PF risk assessment should account for these elements:

- **Threat** refers to designated persons and entities that have previously caused or with the potential to evade, breach or exploit a failure to implement PF-related TFS in the past, present or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities. It can be an actual or a potential threat.
- **Vulnerability** refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF-related TFS. Vulnerabilities may include weaknesses of the country's national counter proliferation financing regime e.g. insufficient laws and regulations, weak supervision and enforcement framework and unavailability of beneficial ownership information. Vulnerabilities also features in the private sector, either for a particular sector, a financial product or type of service that make them attractive for a person or entity engaged in the breach, non-implementation or evasion of PF-related TFS.

[8] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.9-10

- **Consequence** refers to the outcome where funds or assets are made available to designated persons, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit weapon systems (or their means of delivery), or where frozen assets of designated persons would be used without authorisation. A breach, non-implementation or evasion of PF-related TFS may also cause reputational damages and punitive measures by the relevant authorities. Ultimately, the consequence of PF i.e. the threat of use or the use of a WMD, is more severe than any other financial crimes, and is more similar to the potential loss of life associated with the consequences of TF.

A PF risk assessment should also account for inherent and residual risks associated with PF[9]. **Inherent risk** refers to the natural level of risk, prior to introducing any **control measures (relevant policies and procedures)** to mitigate or reduce the likelihood of a person exploiting that risk. Understanding inherent risk is important and beneficial as it can facilitate the corresponding understanding and assessment of whether the control measures are effective, and in the case where no control measures are to be introduced, the impact of such risk to the country or to a firm. For a country, inherent risk may refer to various factors, for example close links with designated persons under PF-related TFS regimes, or the level of production of dual-use goods or goods subject to export controls in the country, trade patterns of such products, as well as weak legal framework aimed at the implementation of relevant UNSCRs for countering PF. **For a private sector firm, it may refer to the nature, types, and complexity of services provided by the specific firm, or its customer types, geographical distribution of its customers and/or beneficial owners, and channels of distribution.**

**Residual risk** refers to the level of risk, which remains after the risk mitigation process. An understanding of residual risk allows private sector firms to determine if they are effectively managing PF risks within their business operations and clientele. A high degree of residual risk may suggest that control measures are inadequate and that a firm should take remedial

[9] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.8-9

actions to address that risk. An example of residual risk is that regulated entities may not identify sanctioned persons and entities even after introducing enhanced screening measures.

## Identification and analysis of threats and vulnerabilities

In terms of **scope**, a PF risk assessment may likely be more targeted than an ML/TF risk assessment, due to the scope of the risks assessed to be narrower than that of ML/TF. A PF risk assessment may follow though the same six key stages as an ML/TF risk assessment, which are: (1) preliminary scoping; (2) planning and organisation; (3) identification of threats and vulnerabilities; (4) analysis; (5) evaluation and follow-up; and (6) update[10].

The FATF states that a good foundation for PF risk assessments is to **identify the major PF threats and vulnerabilities**. Starting with the threats, these includes identifying key sectors, products or services that have been exploited (e.g. financial instruments that might enable proliferation, the maritime and shipping industry, payments in cryptocurrencies, complex structures to obscure the identity of the beneficial owner and the actual business activities, etc.), types and activities that designated persons engaged in, and the challenges on identifying and freezing the assets of designated persons[11]. **Potential information sources** could include CDD information collected, transaction records involving the sale of dual-use goods or goods subject to export control, national PF risk assessments and relevant PF guidance from national supervisors[12].

After identifying the threats, the next step is to identify major PF vulnerabilities. Similar to identifying ML/TF vulnerabilities, PF vulnerabilities could be based on a number of factors, such as **structural, sectoral, product or service, customers and transactions.** The vulnerabilities identified through a comprehensive assessment is inherently linked to a

[10] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.10-11
[11] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.13, par.28
[12] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.16, par.31

country's context and identified threats, and the results will be different from country to country, as well as from sector to sector, and may not be applicable to all countries and private sector entities in the same degree.

The FATF divides vulnerabilities into structural, sectoral, product or service, customers and transactions[13]:

- **Structural vulnerabilities** refer to weaknesses in the national regime to counter PF that makes the country or the private sector entity (including its business and products) attractive to designated persons. Some non-exhaustive examples may include countries:
  - having weak governance, weak law enforcement, weak export controls and/or regulatory regimes and/or weak knowledge of PF risks across agencies.
  - having weak AML/CFT/PF regimes, as identified on FATF Countries Reports during FATF Mutual Evaluations.
  - lacking a legislative framework and national priorities to counter PF.
  - being subject to sanctions, embargoes or other measures imposed by the UN.
  - having significant levels of organised crime, corruption or other criminal activities.
  - having loose market entry, company formation and beneficial ownership requirements and poor internal identification and verification controls on customer and beneficial ownership information.
  - being an international or regional financial, trading, shipping or company formation services center or transit country for smuggling.
  - lacking a culture of inter-agency co-operation among public authorities and a culture of compliance among the private sectors.

- **Sectoral vulnerabilities** refer to weaknesses in the contextual features of a particular sector, such as:

[13] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.21-29

- low level of awareness of PF risks.
- low level of understanding of TFS requirements.
- weak culture of compliance within a sector.
- complexity and movement of funds within each sector.
- High-risk sectors with greater exposure to PF risks are the Trust and Company Service Providers (TCSPs), dealers in precious metals and stones, Virtual/Crypto Assets Service Providers (VASPs or CASPs) and the maritime sector.

### ❖ TCSPs sector:

UN Reports on North Korea and Iran (e.g. UNSCR 2231 (2015)[14], UNSCR 2270 (2016)[15]) noted that **both countries frequently use front companies, shell companies, joint ventures and complex, opaque ownership structures for the purpose of violating measures imposed in relevant UNSCRs.** UNSCR 2270 (2016) also directs the UNSC 1718 Committee to identify individuals and entities engaging in such practices and designate them to be subject to relevant targeted financial sanctions for North Korea.

Furthermore, typologies identified by the UNSCR 1718 (2016)[16] Panel of Experts indicated that designated persons, and persons and entities acting on their behalf, have quickly adapted to Sanctions and developed complex schemes to make it difficult to detect their illicit activities. An investigation in 2019 found that at least five front companies had been established by designated persons and those acting on their behalf to hide their beneficial ownership of various cross-border (US-Dollar-denominated) financial transactions involving two different jurisdictions in Asia, and different front companies were used per transaction. In another investigation, shell and front companies were set up for transferring funds to designated persons

[14] UN Resolution 2231 (2015) on Iran Nuclear Issue
[15] UN Resolution 2270 (2016) on Democratic People's Republic of Korea ("the DPRK")
[16] UN Security Council Committee established pursuant to resolution 1718 (2006) (Resolutions S/2019/691; S/2020/151; S/2020/840)

and entities and the companies were subsequently closed when the UNSCR 1718 Panel of Experts started enquiries about these companies.

❖ **VASPs sector:**

UNSCR 1718 (2016) Panel of Experts also observed that there is a widespread and increasingly sophisticated use of cyber means by the DPRK to steal funds from financial institutions and VASPs across the world, all while evading financial sanctions. Large-scale attacks against VASPs allows the DPRK to generate income that is often harder to trace and subject to less regulation.

Some of the activities identified by the UNSCR 1718 include, amongst others, the theft of crypto-assets (through attacks on both exchanges and users) and the mining of cryptocurrencies through crypto-jacking (i.e. the introduction of malware to computers to turn those systems into cryptocurrency miners for the benefit of DPRK hackers), as well as through the use of its own computer networks to generate funds. To obfuscate these activities, a digital version of layering was used, which created thousands of transactions in real time through one-time use crypto wallets. Transacting in some virtual asset arrangements allows largely instantaneous and nearly irreversible cross-border transfers of funds. Stolen crypto-assets were converted to anonymity-enhanced crypto-assets through other VASPs, often in a complex series of hundreds of transactions with the aim of converting and cashing out all the stolen crypto-assets into fiat currency.

➢ **Private Sector vulnerabilities (product or service, customers and transactions)** refer to weaknesses that are specific to each firm according to its business products or services, customers and transactions, such as:

- the nature, scale and diversity of the firm's business.
- the geographical footprint of the firm's business, including the jurisdictions the firm is operating are major financial or transshipment centers, a firm's business is

connected to a manufacturing sector that produces dual-use goods or subject to export controls, proximity to countries linked with WMD proliferation or countries with trade or corporate networks near or within sanctioned jurisdictions.

- target markets and customer profiles, such as the number of high-risk customers and number of customers with cross-border activities.
- volume and size of transactions.
- Products or services that are complex in nature, have a cross-border reach (e.g. via the distribution channels), are easily accessible to international customers, attract a diverse customer base or offered by multiple subsidiaries or branches.

**Sources of information**[17] for a PF risk assessment could be drawn from:

- ✓ Domestic and international PF typologies
- ✓ National and Supranational risk assessments, focus on the PF component
- ✓ Sectoral reports published by competent authorities
- ✓ PF Risk reports of other jurisdictions (especially those close to Iran and North Korea)
- ✓ Supervisory reports on cases involving breaches, non-implementation, or evasion of PF-related TFS
- ✓ FATF and MONEYVAL countries evaluation reports
- ✓ FATF reports on PF risks indicators/factors
- ✓ Information obtained from on-boarding, ongoing CDD processes and transactions monitoring and screening
- ✓ Internal audit and regulatory findings

After identifying the threats and vulnerabilities relevant to the firm and its business, these needs to be analysed for the identified PF risks. According to the FATF[18], at the **analysis stage**, a relative value or importance should be assigned to each of these PF risks and prioritise between identified risks. This involves a consideration of the potential likelihood

[17] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.29, par.41
[18] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.29-30, par.42-43

and consequence of the materialisation of specific PF risks. **Likelihood** is the possibility that a PF risk may materialised and the **consequence** is the possible impact of the materialization of this specific PF risk. The analysis stage provides the knowledge to the firm to **prioritise between identified PF risks** with high value of likelihood and/or consequence and **design appropriate mitigating measures**.

## Examples of Risk Factors

The **ultimate goal** of conducting a PF risk assessment is to ensure full implementation of PF-related TFS requirements, effectively preventing a breach, non-implementation or evasion of PF-related TFS. PF risk assessment is not necessarily separated from an ML/TF risk assessment. **Regulated entities could employ a PF risk component within their overall risk assessment process.** Those with greater exposure to certain risks, after identifying their threats and vulnerabilities, such as having an international client base, would be expected to account for PF risks within their risk-based approach.

The nature and extent of a PF risk assessment should be appropriate and proportionate to the nature and size of each regulated entity's business activities and customers. **A regulated entity should assess its exposure to PF risks by analysing the countries involved in the provision of its services, the types of customers it has and their business activities, the nature of the products/services offered and the delivery channels of these products/services.** The following non-exhaustive **examples of risk factors** are relevant in formulating a PF risk assessment:

- **Country/Geographic Risk Factors:** The most notable risk factor in terms of geography will be to identify close links with sanctioned countries for WMD proliferation i.e. North Korea and Iran. The Proliferation Financing Index[19] provides useful considerations. Other possible country risk factors might be:

[19] Institute for Science and International Security, September 2021, PPI 2021/2022

- Countries with strategic deficiencies to counter ML, TF and PF (FATF "black and grey" lists) or EU Commission's list of high-risk third countries.
- Countries with weak export controls.
- Countries that are known strategic allies of North Korea and/or Iran.
- Countries that have geographic proximity with countries linked to WMD proliferation.
- Countries that are major transshipment centers or have many registered vessels under its flag.
- Countries that manufacture large quantities of dual-use goods or goods subject to export controls.
- Countries with high levels of organised crime linked to arms dealing.

➢ **Customer Risk Factors:** Some customers' business activities might indicate higher PF risks, such as:

- Business activities with third parties known to be connected to high-risk jurisdictions for WMD proliferation.
- When the customer is involved in the supply chain of dual-use or proliferation-related goods.
- When the customer's UBOs and/or directors are residents in countries that have geographic proximity with countries linked to WMD proliferation.
- When the customer is part of a complex corporate structure or has nominee shareholders.
- Business activities are cash intensive.

➢ **Product/Service or Delivery Channels Risk Factors:** Some products or services and their means of delivery might indicate higher PF risks, such as:

- Dual-use goods or goods subject to export controls or proliferation-related goods.
- Services are used by destinations close to countries linked to WMD proliferation or North Korea or Iran.
- Trade finance services and transactions.

- The customer is financed by financial institutions in higher risk jurisdictions for PF purposes.
- Products/services or transactions that favor anonymity e.g. non-face-to-face business relationships.
- Payment received from unknown or unassociated third parties.
- New products/services and new delivery mechanisms, such as the use of new or developing technologies for new products/services.

## PF Risks in the context of crypto-assets and CASPs operations

The rise of crypto-assets has transformed the financial landscape, offering innovative opportunities for transactions and investments. However, this evolution also brings challenges, particularly regarding the potential for proliferation financing and related illicit activities. Advances in technology and the use of crypto-assets for payments have characteristics and certain features that may be attractive to terrorists and proliferators[20]. Although compliance practices within crypto-assets have improved and expanded in recent years, funds are increasingly being raised and transferred through crypto-assets for PF purposes[21].

The FATF recommendations, particularly those relating to virtual assets and VASPs, provide a comprehensive framework for combating PF. FATF's key aspects include risk-based approach, customer due diligence, reporting obligations for suspicious activities and international cooperation. In addition to the FATF guidance, several organizations and regulatory bodies have issued recent guidance and useful information related to combating PF in connection with crypto-assets[22].

[20] For more information please refer to CySEC's Circular C580 - Guidance on identifying, assessing and understanding Terrorist Financing risks in the context of Crypto Assets activities
[21] Kayla Izenman, *Counterproliferation Financing for Virtual Asset Service Providers - Guidance Paper 2021*, Royal United Services Institute for Defence and Security Studies
[22] U.S. Department of Treasury, 2024 National Proliferation Financing Risk Assessment, UNICRI, CBRN Proliferation Financing: A perspective from Southeast Asia

To identify and mitigate the risks posed by proliferating countries looking to take advantage of the system for their own benefit, a risk-based strategy is needed. For the better identification of customers, sectors and transaction types that might be more vulnerable to PF activity, regular and documented internal risk assessments are necessary, accompanied with controls for the mitigation of PF risks identified.

Regulated entities can benefit from automated blockchain analysis tools that provide, among others, wallet screening (before and after the transaction) and the ability to identify and flag addresses and wallets related to PF. Such tools are essential components for crypto-assets related operations (par. 2.2.2.4 of the Policy Statement PS-01-2021) and should be used in combination with other more "traditional" automated AML/CFT tools for customers screening and due diligence. Regulated entities can also consider media screening and consult typology reports from blockchain analytics companies and cybersecurity firms.

Moreover, it is crucial for regulated entities to prioritize cybersecurity due to the widespread cyber-attacks of crypto-assets by illicit actors, including for PF purposes. This involves staff training, in addition to hiring cybersecurity experts to deploy necessary security measures. Training employees on cybersecurity procedures is crucial in order to defend against hackers representing proliferation actors. Special attention should also be paid to the use of mixers and privacy coins by hackers, as both of them exacerbate PF risk.

Therefore, regulated entities are expected to adhere to the guidance provided, including FATF Recommendations, to strengthen their defenses against the misuse of their services and contribute to global efforts to prevent PF activities. It is imperative that VASPs or CASPs remain vigilant and proactive in adapting to the evolving threat landscape, ensuring the integrity of their operations while promoting the legitimate use of virtual assets.

## PF Risk Indicators/Red Flags

**A PF risk indicator or red flag suggests the likelihood of the occurrence of unusual or suspicious activity for PF purposes.** The existence of a single standalone indicator in relation to a customer or a transaction may not alone warrant suspicion or clear indication of PF, but it could prompt further monitoring and examination, as appropriate. The occurrence of several PF risk indicators (especially from multiple categories) could also require deeper investigation. PF risk indicators are dependent on the business lines, products or services that a regulated entity offers, its customers and the adequacy of the regulated entity in human and technological resources. **PF risk indicators or red flags are relevant to all regulated entities, regardless of their size of business operations and customers.** Some PF risk indicators require cross-comparison of various data (e.g. other financial transactions, Customs data and open market prices) held in external sources.

The FATF (2008[23], 2018[24], 2021[25]) and other independent experts (e.g. CNAS[26]) have published several reports on PF typologies/red flags, intended to assist government authorities and financial institutions to mitigate PF risks. Some of these risk indicators/red flags are similar to those for ML or TF. **The below list of PF risk indicators or red flags aim to assist in raising awareness of situations where there may be potential PF, enhanced understanding of the PF risks and provides a basis for controls and procedures that could be implemented to detect PF:**

### ❖ Customer Profile Risk Indicators

- During on-boarding, a customer provides vague or incomplete information about their proposed trading activities. Customer is reluctant to provide additional information about their activities when asked.

[23] FATF, June 2008, FATF Typologies Report on Proliferation Financing, p.54
[24] FATF, February 2018, FATF GUIDANCE ON COUNTER PROLIFERATION FINANCING, p.32-34
[25] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.17-21
[26] CNAS, Dr. Jonathan Brewer, January 2018, The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, p.7-8

- A customer, particularly a trade entity, or its UBOs and directors, appear in Sanctions Lists or in negative media news for e.g. ongoing or past investigations or convictions for ML schemes, fraud or other criminal activities.
- A customer is a person or entity physically located or connected (e.g. through business or trade relations) with a known country for WMD proliferation (i.e. Iran and North Korea) or a country of diversion concern (e.g. China, Hong Kong, Turkey).
- A customer had previous dealings with designated persons or entities for WMD proliferation and PF.
- The CDD information of a customer or a counterparty of the customer has similarities to information of designated persons or entities for WMD proliferation and PF, for example names, addresses, telephone numbers, UBOs, directors, etc.
- A customer or a counterparty of the customer is, directly or indirectly, involved in the supply, sale, delivery or purchase of dual-use or proliferation-sensitive goods, particularly to higher risk jurisdictions.
- A customer is a person or entity dealing with dual-use goods or goods subject to export controls for which lacks the technical background to do so or which is inconsistent with their risk profile or anticipated activities.
- A customer engages in complex trade deals involving numerous third-party intermediaries in business lines that do not agree with the stated business activities in the Economic Profile or the historical pattern of trade activities.
- A customer, particularly a trade entity, is purchasing or selling goods under unclear circumstances, for example the end-use and end-user of the goods is not identified, incomplete information about importers/exporters and shipping companies, irregularities between contracts and pricing (e.g. undervalued shipment or overvalued delivery costs without justification), payments are executed by an unrelated party with the customer, etc.
- A customer provides trade documentation with unclear or misleading or over-technical description of goods or the evidence suggests that the trade documentation or other customer representations (e.g. relating to shipping, Customs or payment) are fake or fraudulent.

- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money-remittance business or a pay-through account. These accounts involve rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons.
- A customer associated with a university or a research institution is involved in the trading of dual-use goods or goods subject to export controls.

## ❖ Account and Transactions Risk Indicators

- A transaction or activity is, directly or indirectly, connected with the supply, sale, delivery or purchase of dual-use or proliferation-sensitive goods, particularly to higher risk jurisdictions.
- A transaction involves parties physically located or connected (e.g. through business or trade relations) with a known country for WMD proliferation (i.e. Iran and North Korea) or a country of diversion concern (e.g. China, Hong Kong, Turkey).
- The originator or beneficiary of a transaction is a person or entity ordinarily resident of or domiciled in a known country for WMD proliferation (i.e. Iran and North Korea) or a country of diversion concern (e.g. China, Hong Kong, Turkey).
- Customers conduct transactions that have previously violated requirements under dual-use goods or export controls regimes.
- Accounts or transactions involve companies with opaque or complex ownership structures with front companies or shell companies or unnecessary intermediaries.
- Demonstrating links between representatives of companies exchanging goods, i.e. same owners or management, same physical address, same IP address or telephone number or their activities may be co-ordinated.
- Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCRs obligations and FATF Standards and/or weak AML/CFT controls and/or weak export controls regime.
- A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions. For financial institutions, the transactions

are visible through sudden inflows of cash to the account followed by cash withdrawals.

- Transactions are made on the basis of "ledger" arrangements that prevent the need for frequent international financial transactions and avoid scrutinising. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf (related parties).
- Transactions or payments to parties not identified or to parties located in a third country other than the beneficiary's known location.
- The transaction structure (whether for shipping route, financing arrangement or documentation) appears unnecessarily complex or irrational.
- The fragmented nature of the trade cycle and the involvement of different financial institutions in a single transaction.
- Transactions involving correspondent banks or financial institutions with known AML/CFT deficiencies or located in high-risk jurisdictions for PF purposes or have history for facilitating payments for high-risk jurisdictions for PF.
- Involvement of a small trading, brokering or intermediary company, that is often carrying out business inconsistent with their normal business activities.
- A customer uses a personal account to purchase industrial items that are under export controls that are not normally associated with the regular business activities.

## ❖ Country or Geographical Risk Indicators

- Countries with geographic proximity to known countries for WMD proliferation (i.e. Iran and North Korea) or a country of diversion concern (e.g. China, Hong Kong, Turkey).
- Countries that are known trade or strategic allies of North Korea and Iran.
- Countries with weak implementation of relevant UNSCRs obligations.
- Countries with strategic deficiencies to counter ML, TF and PF, for example those identified by the FATF as non-cooperative jurisdictions (FATF "black and grey" lists) or EU Commission's list of high-risk third countries.

- Use of jurisdictions with laxed regulations for beneficial ownership requirements, usually where there is no public register for companies' information.
- Countries with high levels of organised crime or known to provide funding or other support to terrorists/proliferators.
- Countries that manufactures large quantities of dual-use goods or goods subject to export controls.
- Transactions which involve individuals, companies or shipment routes located in countries with weak export controls laws or weak enforcement of export controls.
- Orders for goods is placed by persons in third countries other than the country of the end-use of the products.
- Shipment of goods is inconsistent with normal geographic trade patterns or expected business activities e.g. the destination country does not normally export or import the goods listed in the trade documents.
- Shipment of technical goods that is incompatible with the technological level of the country to which it is being shipped, for example semiconductor manufacturing equipment is being shipped to a country with no electronics industry.
- Transshipment of goods through several countries for no apparent reason.
- Payments or transfers made to importers, exporters, agents or brokers that export to countries and ports near the border of sanctioned countries. For example, shipments of prohibited goods to North Korea are often marked as destined to Dangdong, China or other nearby ports.

## ❖ Maritime or Shipping Sector Risk Indicators

- A trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes.
- The person or entity preparing a shipment have listed a freight forwarding or shipping entity as the final destination of goods.
- 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 exporter and the name of the payment recipient; differing prices on invoices and underlying contracts; discrepancies between the quantity, quality, volume or value of the actual commodities and their descriptions.
- Shipment of goods have a low declared value in contradiction with the shipping cost.
- Shipment of highly technical goods that is incompatible with the technological level of the country to which it is being shipped, for example semiconductor manufacturing equipment is being shipped to a country with no electronics industry.
- Shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping or using a small or old fleet.
- Shipment of goods is routed through a country with weak implementation of relevant UNSCRs obligations and/or FATF Standards or weak export controls.
- Payment for imported commodities is made by an unrelated entity with no clear economic reasons e.g. by a shell or front company not involved in the transaction.
- Quantities are just below certain reporting thresholds of the jurisdictions involved.

## ❖ Trade Finance Risk Indicators

- Prior to account approval, the customer requests letter of credit for trade transaction for shipment of dual-use goods or goods subject to export controls.
- Lack of full information or inconsistences 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.
- Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.

# E. RISK MITIGATION AND CONTROLS

All regulated entities should consider **calibrating and enhancing their policies, controls, and procedures to effectively manage and mitigate identified PF risks from the PF risk assessment (refer to section D above).** Appropriate and proportionate resources (both human and technological) should be allocated to the implementation of mitigating measures based on the findings of the PF risk assessment. Regulated entities should develop robust standards and procedures to mitigate their exposure to PF risks, for example by providing targeted training to compliance personnel, having adequate risk management systems and procedures in place, senior management oversight in CDD procedures, clear reporting requirements for PF purposes and efficient and effective screening systems.

## Recommended controls and mitigating measures

The nature of risk mitigating measures and controls to counter PF will depend on the source and degree of the risks identified. According to FATF Recommendations[27], these could include:

- **Improved onboarding processes and ongoing monitoring for customers** (including their beneficial owners). For example:
  - **Specific PF-related questions** could be added to the customers' onboarding questionnaire for due diligence purposes and re-visited during the review of the business relationship. Any business activities of the customer that are associated with the supply chain of WMD proliferation or with goods subject to export controls or with proliferation-sensitive goods or trade finance should be identified at the establishment of the business relationship. Other PF-related

[27] FATF, June 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation, p.37-42, par.64-82

questions could help identify the international activity and relations of the customer that would help ascertain geographical PF risk factors.

- **Transactions screening (collecting and assessing information on the purpose and nature of transactions)** must account for both parties (payer and payee), including screening for related and unrelated companies and their beneficial owners, directors, authorized signatories, suppliers and buyers, shipping industry companies, transshipment countries and companies, end users, Customs codes for exporting goods, etc. Transactions that have incomplete information (e.g. unclear description of goods, missing final destination and end-use of goods and/or missing third party information) should be flagged for further assessment.
- Screening procedures should **account for all relevant international sanctions lists** and documented properly, irrespective of a true match or not. Screening procedures should **timely account for updates of all relevant international Sanctions lists.**
- **Understanding the customers' business activities and transactions** is vital. Customers' Economic Profiles should contain not only current, accurate and complete CDD information, but also comprehensive information on the business activities (products or services, countries operating or trading with, important counterparties, delivery channels) to be able to assess and compare actual and expected transactions for PF purposes.
- **Activity-based screening as opposed to list-based screening.** Sanctioned persons will try to hide their identity behind complex corporate structures and business associates, making it essential to fully understand customers' business operations, rather than just identifying the customers' beneficial owners, to manage and mitigate PF risks. The names of sanctioned persons and entities will rarely appear in financial transactions, therefore activity-based screening is more effective for countering PF. Screening should account for export controls regimes lists and dual-use items lists.

- **Enhanced customer due diligence procedures and controls**, especially for customers involved with trading in dual-use goods or goods subject to export controls. For example, a regulated entity could obtain additional information and supporting evidence to:
  - **Verify the customers' business operations and understand their nature**.
  - **Assess the intended use of the regulated entity's services**.
  - **Scrutinise intended or performed transactions that seem inconsistent with expected activity**, especially payments for dual-use goods, payments being made to importers/exporters and shipping companies, payments for goods that are being shipped to countries near sanctioned countries. This could be undertaken by reviewing contracts, pricing, vessels information, transshipment companies and countries, existence of dual-use goods, Customs codes for exporting goods, existence of a valid license from official sources or similar proof in higher risk situations of exporting or importing goods, trade embargoes, etc.
  - An **automated transactions monitoring system** could be utilised where there is a high volume of transactions. **Transactions in high-risk situations should be screened against Sanctions Lists, export controls lists and dual-use items lists.**
  - **Ascertain the end-user and end-use of a product or service.**
  - **Verify the source of funds and source of wealth of the customer and its beneficial owners.**

- Effective maintenance of CDD information (**effective record keeping**).
- Regular controls to ensure **effectiveness of sanctions screening systems and procedures**. The EBA has recently issued a set of guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures[28], which includes, amongst others, guidance on how to put in place an effective screening system to reliably identify sanctioned persons, including

[28] EBA, November 2024, Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures

considerations on defining the set of data to be screened, calibration, reliance on third parties, management and analysis of alerts, etc.

- Understanding the **exposure of customers and related geographical activities and services** to PF risks i.e. proximity of activities to sanctioned countries.
- **Leveraging the existing compliance programmes** (including internal controls) to identify potential sanctions evasion and illicit trade finance.
- **Written policies and procedures for internal and external reporting**, if transactions connected to PF are identified.
- **Training** for relevant compliance personnel on identifying and countering PF.

## Reporting requirements

In cases where a regulated entity identifies a transaction that involves the buying/selling of dual-use goods, trade documentation obtained must be screened against the EU List of dual-use goods for identification of possible matches. If there is a true match, additional due diligence measures must be performed to ascertain if the goods are subject to export controls, depending on their final destination and end-use.

In cases of business relationships with designated persons, the regulated entities must take all mandatory actions/measures such as freezing assets and prohibiting access to funds for these designated persons, where applicable, in accordance with the provisions of EU Restrictive Measures and UN Sanctions. Relevant guidance was provided through Circulars C489, C556 and C570 and continuously through CySEC's website.

In cases where a regulated entity identifies suspicious customer transactions or potential activity for PF purposes, after a thorough assessment is conducted, these suspicions must be immediately submitted to the Unit for Combating Money Laundering in Cyprus (MOKAS) through a Suspicious Activity Report (SAR) or a Suspicious Transaction Report (STR), depending on the circumstances.

## Non-compliance with PF requirements

Failure to comply with PF requirements, in addition to causing reputational damage for both the regulated entity and its jurisdiction, could trigger administrative and/or criminal proceedings that may result in penalties for non-compliance and/or criminal prosecution and/or imprisonment, in accordance with the legal framework in Cyprus, the EU Restrictive Measures and UN Sanctions.

# F. USEFUL LINKS

## EU Restrictive Measures

- EU Sanctions Map
- Consolidated List of Sanctions
- Consolidated FAQs on the implementation of Council Regulation No 833/2014 and 269/2014
- Council of the European Union
- Official Journal of the European Union
- Common Foreign and Security Policy (CFSP)

## UN Sanctions

- General Information
- Consolidated List of Sanctions
- United Nations Security Council Resolutions

## Other

- Cyprus Financial Intelligence Unit (MOKAS)
- Cyprus Police
- Customs & Excise Department
- Cyprus Port Authority
- Ministry of Energy, Commerce and Industry (Trade Department)
- Ministry of Foreign Affairs
- Ministry of Finance
- Central Bank of Cyprus
- Institute of Certified Public Accountants Cyprus
- Cyprus Bar Association

- Committee of Experts on the Evaluation of AML/CFT Measures (MONEYVAL)
- Europol / Eurojust
- Financial Action Task Force (FATF)
- Proliferation Financing Index
- Office of Foreign Assets Control (OFAC)
- Financial Crimes Enforcement Network (FinCEN)