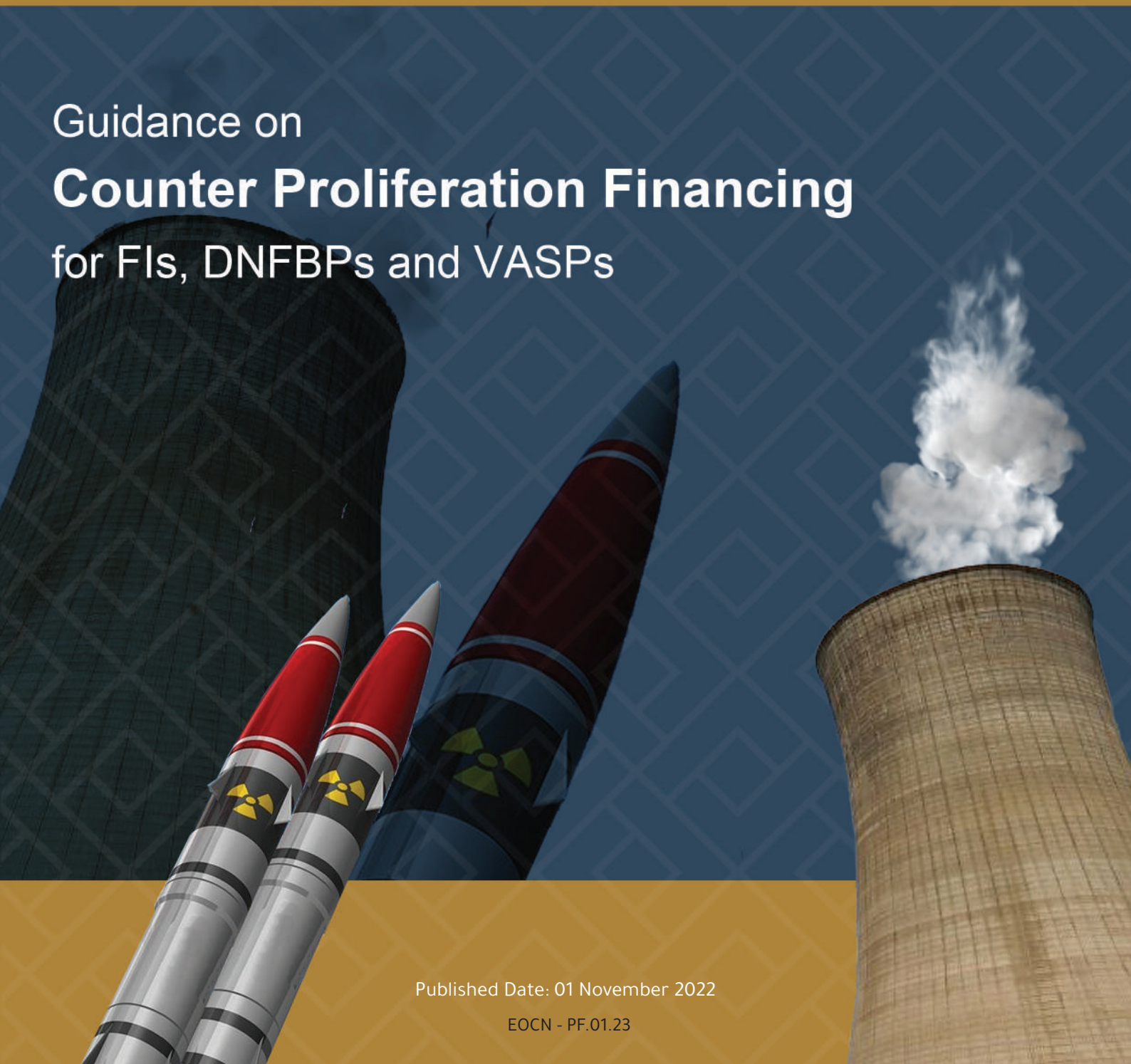
المكتب التنفيذي للرقابة وحظر الانتشار

EXECUTIVE OFFICE FOR CONTROL & NON-PROLIFERATION

United Arab Emirates

Guidance on
Counter Proliferation Financing
for FIs, DNFBPs and VASPs



Published Date: 01 November 2022

EOCN - PF.01.23

Contents

Acronyms

CDD	Customer Due Diligence
DNFBPs	Designated non-financial businesses and professions
EDD	Enhanced Due Diligence
Executive Office or EOCN	Executive Office For Control & Non-Proliferation
FATF	Financial Action Task Force
FANR	Federal Authority for Nuclear Regulation
FCA	Federal Customs Authority
FIs	Financial Institutions
PF	Proliferation Financing
STR/SAR	Suspicious Transaction Report / Suspicious Activity Report
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UAE	United Arab Emirates
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
VASPs	Virtual Assets Service Providers
WMD	Weapons of Mass Destruction

Introduction

Framework

1. This Guidance is produced by the Executive Office For Control & Non-Proliferation (EOCN).
2. This Guidance is supplementary to the Guidance on Targeted Financial Sanctions for Financial Institutions (FIs), Designated Non-Financial Business and Professions (DNFBPs) and Virtual Assets Service Providers (VASPs).
3. The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and has primary responsibility for the maintenance of international peace and security. The Security Council sanctions regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counterterrorism. These regimes include measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.
4. The Financial Action Task Force (FATF), an inter-governmental body responsible for setting international standards on anti-money laundering (AML) and countering the financing of terrorism (CFT) and proliferation (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards, requires the implementation of targeted financial sanctions (TFS) to comply with the UN Security Council Resolutions (UNSCRs) relating to the prevention and suppression of Terrorism, Terrorism Financing (TF), and Proliferation Financing (PF).
5. The United Arab Emirates (UAE), as a member of the UN, is committed to implementing UNSCRs, including those related to the UN's sanctions regimes. Consequently, through the Cabinet Decision No. 74 of 2020, the UAE is implementing relevant UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, in particular relating to TFS.
6. The UAE framework sets relevant federal laws and executive regulations in relation to Counter-Proliferation and its Financing. These are set in Section 3 of this guidance.

Purpose and Scope

7. The guidance explains the definitions of Proliferation Financing, Stages of Proliferation Financing and the UAE AML/CFT legal framework.
8. This Guidance on Counter Proliferation Financing for FIs, DNFBPs and VASPs is issued to raise the awareness of the private sector against the threats, risks and vulnerabilities of PF and to identify, assess, understand and mitigate the PF risks in line with the FATF Standard.
9. The Guidance provides list of red flags to assist FIs, DNFBPs and VASPs in identifying and uncovering PF sanctions evasion activities.

1. Definition of Proliferation and Proliferation Financing

The threat posed by weapons of mass destruction (WMD) and their associated delivery systems is a distinct but related concept from the financing of such activity. Although the FATF has not presented official definitions of "proliferation" and "proliferation financing", the FATF's 2021 Guidance on Proliferation Financing Risk Assessment and Mitigation offers the following working definitions:

- **WMD Proliferation** refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both Dual-Use technologies and Dual-Use goods used for non-legitimate purposes).

- **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)[1].

The definitions above provide broader descriptions of proliferation and PF than the scope of this Guidance. FIs, DNFBPs, and VASPs in the UAE are required to assess and mitigate "proliferation financing risk" as defined more narrowly in the FATF's Recommendation 1:

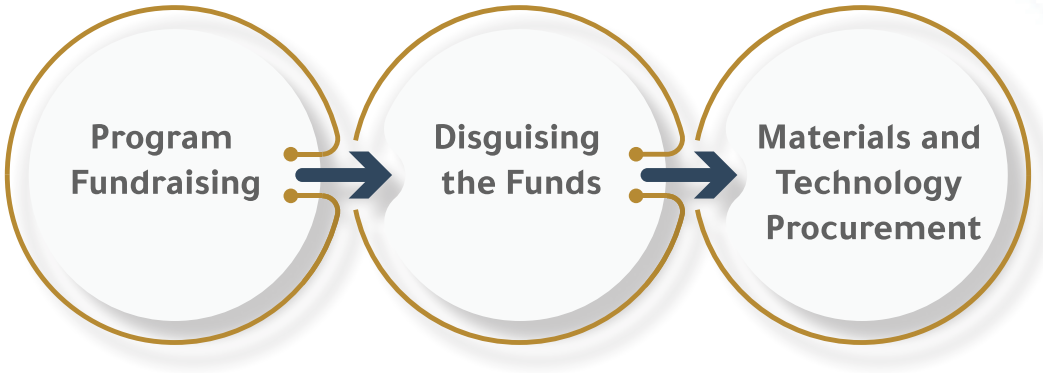
- **Proliferation Financing Risk** refers to the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in FATF Recommendation 7, namely those pursuant to UNSCRs relating to the prevention, suppression, and disruption of proliferation of WMD and its financing[2].

However, a broader understanding of the risk of WMD proliferation and its underlying financing is important as it assists institutions in developing their understanding of the risk of the breach, non-implementation or evasion of TFS related to proliferation (i.e., the narrowly-defined proliferation financing risks required to be assessed and mitigated).

1- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, June 2021, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf, p. 8.
2- FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Updated October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 10.

2. Stages of Proliferation Financing

PF can be understood as taking place over three stages: [3]



Stage 1: Program Fundraising: A proliferating country raises financial resources for in-country costs. The funding sources may derive from the proliferating country's budget, profits from an overseas commercial enterprise network, and/or proceeds from an overseas criminal activity network.

As an example of program fundraising, the UN Panel of Experts has found that North Korea/ DPRK has exported prohibited commodities (such as coal, iron and steel products, and copper) to generate revenue[4]. International observers believe that the DPRK's sales of natural resources are part of elaborate trade-based payment schemes to support its WMD and conventional weapons program development[5].

Stage 2: Disguising the Funds: The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes. A proliferating country may use means that range from the simpler to the more complex, including using normal correspondent banking channels or an intricate network of procurement agents and front companies. During this stage, states that are subject to comprehensive sanctions will seek to circumvent such sanctions, often using methods on the more sophisticated end of the spectrum to disguise the funds. Both Iran and the DPRK have been found to use front companies, shell companies, and complex, opaque ownership structures to evade and circumvent TFS.[6]

3- Dr. Jonathan Brewer, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation, Center for a New American Security (CNAS), January 2018, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-ProliferationFinance-Finalb.pdf?mtime=20180202155127&focal=none, pp. 4-6.
4 - United Nations (2018), Final report of the Panel of Experts submitted pursuant to resolution 2345 (2017), S/2018/171, www.undocs.org/S/2018/171, p. 15.
5 - U.S. Financial Crimes Enforcement Network (FinCEN), "Advisory on North Korea's Use of the International Financial System," November 2, 2017, https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf.
6- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, June 2021, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf, p. 25.

Stage 3: Materials and Technology Procurement: The proliferating state or its agents use the disguised resources for procurement of materials and technology within the international financial system. This stage also includes the payments for shipping and transport of materials and technology.

A past UN Panel of Experts report observed that Iran used various procurement methods, including using front companies for prohibited procurement, as well as using its petrochemical sector to obscure the end use of items procured for its nuclear program[7].

3. UAE's Framework on Counter-Proliferation and its Financing

This Guidance builds upon the provisions of the following laws and regulations, which together comprise the UAE's legal and regulatory framework for counter-proliferation and its financing:

Federal Law No. 13 of 2007 established the UAE's framework of export controls to prevent the unrestricted exportation of goods, information, and technology of strategic value, including certain dual-purpose military-civilian goods and technologies. Under this framework and pursuant to Cabinet Resolution 3/99 of 2009, the Committee for Goods and Material Subjected to Import and Export Controls is charged with overseeing the UAE's import/export governance and licensing regime and implementing policies, regulations, and amendments to Federal Law No. 13 to further improve its effectiveness and enforceability.

7- United Nations (2014), Final report of the Panel of Experts established pursuant to resolution 1929 (2010), S/2014/394, https://undocs.org/S/2014/394, pp. 22-24.

UAE Control List

Cabinet Resolution No. (50) of 2020 contains the list of strategic and Dual-Use goods controlled under UAE law (UAE Control List). The UAE Control List implements internationally agreed Dual-Use goods subject to import and export control, including the Missile Technology Control Regime (MTCR), Nuclear Suppliers Group (NSG), the Wassenaar Arrangement (WA), the Australia Group (AG), the Chemical Weapons Convention (CWC), and the Organization for the Prohibition of Chemical Weapons (OPCW).

The UAE Control List is composed of 12 categories based on the technology used. Each category includes a technical description of the items and their control parameters. A summary of the categories can be seen in the table below:

Category	Type / mandate	Example of controlled items used in WMD programs
0	Nuclear Materials	Nuclear Reactor - Pressure Tubes - Zirconium Metal Tubes - Steam generators
1	Special Materials	Protective and detection equipment - Body armour and components - High-density lead glass
2	Material Processing	Bearing systems - Milling Machines - Robotics - Vibration test systems - Motion simulators
3	Electronics	Microcomputers - Microcircuits - Microwave Amplifiers - Oscillator - High-speed pulse generators
4	Computers	Electronic Computers - Hybird Computers - Analouge Computers
5	Telecommunications	Telecommunication systems - Electronically steerable antennae - Interception & Jamming equipment
6	Sensors	Acuoustic systems - Optical sensors - Scanning cameras - Imaging cameras - Optical equipment
7	Navigations & Avionics	Accelerometers - Gyros - Inertial measurement equipment - Global Navigation Satellite Systems
8	Marine	Submersible Vehicles and surface vessels - Pumpjet propulsion - Noise reduction systems
9	Aerospace & Propulsion	Gas Turbine Engines - Marine gas turbine engines - Liquid rocket propulsion - Ramjet - Scramjet
10	Chemical List (OPCW)	Chemical Weapons Chemical Lists
11	National Controlled Commodities	Armoured components and technologies

In addition, the EOCN provides a list of Dual-Use chemicals that fall under the UAE Control List on its website[8]. The list can be searched by filtering Harmonized System Codes (HS Code), CAS Registry Numbers (CAS Number), Export Control Classification Numbers (ECCN), Chemical Names, and Synonym Names.

The Executive Office for Control & Non-Proliferation

The Executive Office for Control & Non-Proliferation also acts as the UAE's central authority to ensure the implementation of TFS, and serves as the licensing authority responsible for reviewing applications and granting permits for the import, export, re-export, and transit of Dual-Use controlled goods, information, and technology from, to, or through the UAE. The permits issued by the Executive Office are based on three main criteria:

1. **Technical specifications:** This criterion looks at the item's description and technical specifications. Most items are considered Dual-Use and are therefore controlled for import/export only when they meet certain specification requirements or thresholds. These specifications are further detailed in the UAE Control List.

8- https\\www.uaeiec.gov.ae\ar-ae\control-list-good

2. **End-use of the Dual-Use item:** This criterion looks at the end use of the Dual-Use item. In other words, it looks at the question of "what will the item be used for?". Since Dual-Use items have both civil and military applications, it is important to identify whether the item being imported/exported is intended for civil use or in a WMD program.

3. **End-user of the Dual-Use item:** This criterion looks at the end user of the Dual-Use item. It looks at the question of "who is the ultimate user of the item?". In many cases, freight forwarders and shipping companies apply for permits on behalf of importers/exporters; hence, it is important to identify the end-user of the items to ensure that they are not users of proliferation concern.

In addition, The Executive Office for Control & Non-Proliferation coordinates closely with supervisory authorities to ensure a sound understanding of proliferation and PF risks faced by the private sector and compliance with TFS and other PF obligations and expectations.

The Federal Authority for Nuclear Regulation

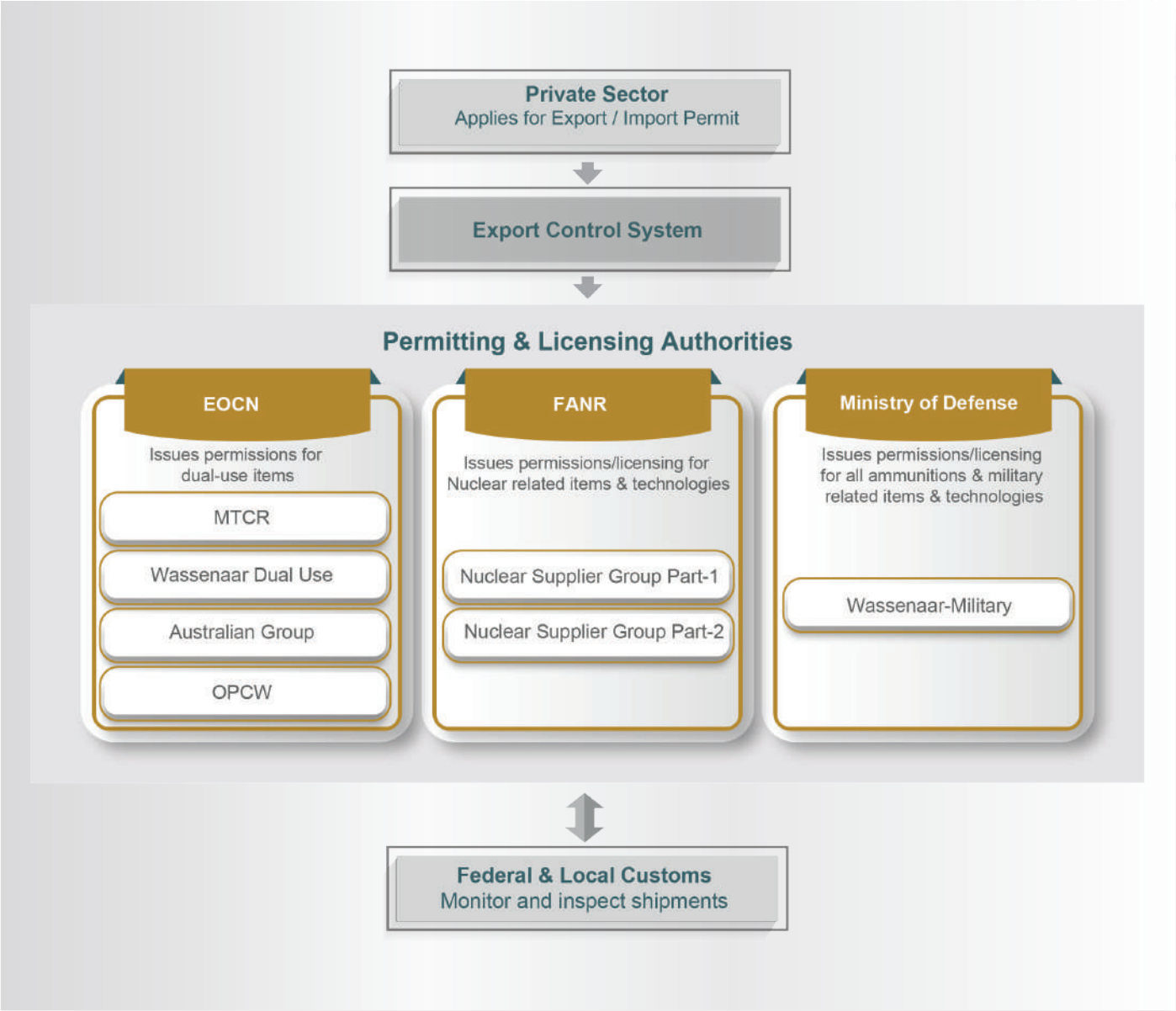
The Federal Authority for Nuclear Regulation (FANR) is the regulatory authority responsible for overseeing the nuclear industry's compliance with Federal Law No. 6 of 2009 Concerning the Peaceful Uses of Nuclear Energy. FANR regulates the design, construction, operation, and decommissioning of nuclear energy facilities in the UAE and regulates the use of radioactive materials and radiation sources for medical, scientific, and other purposes. In coordination with the EOCN, FANR is responsible for reviewing and granting permits for the import, export, and transit of nuclear materials and technology.

The Federal Authority for Identity, Citizenship, Customs and Ports Security

Finally, the Federal Customs Authority (FCA) was established in 2002 and is charged with implementing the UAE's unified customs law and executing the UAE's obligations under the Gulf Cooperation Council's customs union. The FCA develops and oversees the implementation of national customs policies concerning the import of banned or restricted items into the UAE, including but not limited to goods subject to local or international prohibitions or restrictions.

Interagency Mechanism

The Executive Office regulates the import and export of strategic and Dual-Use goods. For nuclear-related goods, the FANR is responsible for regulating the licensing of businesses operating in the nuclear sector, as well as issuing permits to import and export nuclear materials and technologies. Both the Executive Office and the FANR work closely together with the FCA to inspect and seize shipments that relate to proliferation and violate the export control laws of the UAE. The image below illustrates the UAE export control framework:



4. Understanding and Assessing PF Risks

Understanding and assessing PF risks is a critical starting point for FIs, DNFBPs, and VASPs to develop their associated preventive and mitigating measures. A rigorous approach, promoted by the FATF, is to assess risk as a function of three factors: threat, vulnerability, and consequence[9].

The subsections below contain guidance for regulated entities in the UAE to understand potential PF threats, vulnerabilities, and consequences, and subsequently incorporate PF risk into their institutional risk assessments.

9- FATF, National Money Laundering and Terrorist Financing Risk Assessment, February 2013, https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf, p. 7; and FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, pp. 8 and 29.

PF Threats

Threat refers to designated persons and entities that have previously caused or have the potential to evade, breach, or exploit a failure to implement TFS related to proliferation 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[10].

The first step for an institution to understand its PF risk is to compile a list of major known or suspected threats; key sectors, products, or services that have been exploited; types and activities that designated individuals/entities have engaged in; and the primary reasons why designated persons and entities have not been deprived of their assets or identified[11]. Institutions should consider not just their direct exposure to known PF threats, but also their potential exposure to otherwise legal activities that may be exploited by PF threat actors.

To assist in identifying PF threats, private sector entities are advised to consult databases containing customer due diligence (CDD) information collected during the onboarding and ongoing due diligence processes (including beneficial ownership information for legal persons and arrangements) and, if applicable, transaction records involving the sale of Dual-Use goods or goods subject to export control[12].

Key proliferation and PF threats include foreign state and non-state actors attempting to exploit a country's financial sector and transportation infrastructure to clandestinely finance, procure, ship, or trans-ship goods for use in WMD proliferation. State actors attempting to develop or acquire WMDs and their means of delivery and related materials constitute a significant threat, but non-state actors also pose proliferation and PF threats. Private sector entities should be particularly aware of the following major threats:

- **State actors**. North Korea/DPRK and Iran have created international networks of front and shell companies and use sophisticated methods to conceal their PF activity and evade international TFS levied against them. Other states with existing or developing WMD capabilities pose a more limited threat. Common typologies that have been used by DPRK[13] and Iran include:

    1. Use of extensive overseas networks of procurement agents and front companies, including officials who operate from diplomatic missions or trade offices, as well as third country nationals and foreign companies, to procure dual-use and controlled items.

    2. Mislabelling dual-use goods in export documentation by falsely declaring the items being shipped as general-purpose goods.

    3. Concealing the end user of a shipment by using freight forwarding companies and front companies established in foreign countries (often within close proximity to the proliferating state) as the receivers of the shipped goods.

10- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 9.
11- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 13.
12- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 16.
13- US DOS, DOT, & DOC Joint Advisory "North Korea Ballistic Missile Procurement Advisory".

4. Sale of natural resources (such as coal by the DPRK and petroleum products by Iran) to generate revenue in order to fund nuclear and ballistic weapons program.

- **Non-state actors**. Terrorist groups have at least stated an intent to pursue nuclear weapons and radiological materials. The United Nations calls the prospect of non-state actors, including terrorist groups, accessing and using WMD a "serious threat to international peace and security[14]."

The absence of direct links to these countries or hostile non-state actors does not mean that a transaction or customer is necessarily low risk. Proliferators have developed capabilities to disguise their involvement and the nature of the activity underlying a transaction or business relationship Every FI, DNFBP, and VASP faces a certain amount of risk and should assess the extent and type of PF threats that it faces given its customer base, product and service offerings, and geographic footprint.

PF Vulnerabilities

Vulnerability refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation, or evasion of TFS related to proliferation. Vulnerabilities may include features of 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 TFS related to proliferation[15].

After formulating a list of PF threats, FIs, DNFBPs, and VASPs should next compile a list of their major PF vulnerabilities. These vulnerabilities may be based on various factors, such as their business structure or sector, products or services, customers, and transactions[16]:

- **Structural vulnerabilities** could include the nature, scale, and geographical footprint of the entity's business; its customer base's characteristics; and the volume and size of transactions flowing through the entity[17].
- **Sectoral vulnerabilities** are weaknesses in a sector that make it attractive for designated persons and entities to attempt to abuse it to circumvent TFS related to proliferation[18]. Each entity performing this analysis should consider the sector it belongs to, as well as the sectors of its customers. Select examples of sectoral vulnerabilities include the following:
  - The **banking or money or value transfer sectors** are vulnerable to exploitation because proliferators need access to the international financial system to carry out the stages of PF described above (especially stages 2 and 3). Hawala and other similar service providers are particularly vulnerable to abuse. The UN Panel of Experts presented an example of hawala transactions being used by an Iranian company to purchase goods worth several million euros from a company outside of Iran[19]. Although the Panel of Experts could not confirm that prohibited PF activities related to Iran occurred through the hawaladar sector, their report noted that the use of hawala channels to finance procurement was a risk that UN member states should take into account.

14- United Nations Office of Counter-Terrorism, "Chemical biological, radiological and nuclear terrorism," https://www.un.org/counterterrorism/cct/chemical-biological-radiological-and-nuclear-terrorism.
15- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, pp. 9-10.
16- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 21.
17- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 22.
18- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 23.
19- United Nations (2014), Final report of the Panel of Experts established pursuant to resolution 1929 (2010), S/2014/394, https://undocs.org/S/2014/394, pp. 26-28.

- **Trust and company service providers (including lawyers, notaries, and other legal professionals and accountants providing these services)** may be abused for the formation of front and shell companies that enable the disguising of designated persons or entities involved in transactions. In the broader **DNFBP sector**, another vulnerability is the generally lower level of awareness and understanding of PF risk.

- **VASPs (and FIs that provide services to VASPs)** are vulnerable to misuse because of the nature of virtual assets transactions—the potential for anonymity, the ability to transact across borders, and the enablement of rapid settlement. Virtual assets have been used in program fundraising (Stage 1 of PF), and there is evidence that North Korea/DPRK has conducted attacks on FIs and virtual asset exchanges to steal funds[20]. Virtual assets are also vulnerable to being used to evade TFS in Stage 2 of PF, as observed in cases involving North Korea/DPRK laundering illicit proceeds using virtual assets[21].

- **Product or service-specific vulnerabilities** could include whether a product or service provided by the FI, DNFBP, or VASP is complex, enables cross-border transactions, appeals to a diverse customer base, or is provided by multiple subsidiaries or branches[22]. Examples of products and services that are higher risk for PF include correspondent banking services and trade finance products.

- **Customer and transaction vulnerabilities** could include exposure to customers that are higher risk for PF (e.g., due to their engagement in cross-border transactions, especially those involving legal persons and arrangements) and exposure to transactions exhibiting PF-related red flags (e.g., due to geographies involved)[23]. Section 7 of this Guidance contains a list of red flags for possible PF activities.

To assist in identifying PF vulnerabilities, private sector entities should review international reports of PF typologies, relevant sectoral reports published by UAE authorities, and publicly available court cases about evasion of TFS. Entities should also examine their CDD records, transaction monitoring and screening records, and internal audit and supervisory/regulatory findings.

PF Consequences

Consequence refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical, or biological weapon systems

20- United Nations Security Council, Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019) (S/2019/691), August 30, 2019, https://undocs.org/S/2019/691.
21- Ibid.
22- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 26.
23- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 29.

(or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for PF. A consequence may also include reputational damage. The ultimate consequence of PF is the use or threat of use of a WMD[24].

To help prioritize between identified risks, FIs, DNFBPs, and VASPs should consider the potential likelihood and consequences of the materialisation of specific PF risks.

Incorporating PF Risk into the Institution's Risk Assessment

FIs, DNFBPs, and VASPs in the UAE should incorporate their analysis of PF risks into a written risk assessment, in order to document their understanding and analysis of PF risk as a foundation of the risk-based approach. For most entities, it will be appropriate to incorporate their PF risk analysis into the same risk assessment performed for other financial crimes (including money laundering and TFS). However, private sector entities may decide to conduct a PF-specific risk assessment. The approach should be commensurate with an entity's nature, size of its business, and level of exposure to PF risks.

Using the threat/vulnerability/consequence construct described above, FIs, DNFBPs, and VASPs should evaluate their PF risks. Their risk assessments should generally include the following categories: 1) Geographic risk, 2) Customer risk, and 3) Product and service risk, in accordance with Article (4) of Cabinet Decision No. (10) Of 2019 Concerning The Implementing Regulation Of Decree Law No. (20) Of 2018 On Anti- Money Laundering And Combating The Financing Of Terrorism And Illegal Organisations.

- **Geographic Risk:** The private sector entity should identify and assess the jurisdictions where it has headquarters and branches, as well as where it conducts business and has target markets.

  Countries that are known or suspected to have developed illicit WMD programs are a major source of PF risk. Currently, North Korea/DPRK and Iran are states subject to TFS imposed because of their efforts to develop illicit WMD programs and capabilities. These states present a key global threat for WMD proliferation and PF.

  However, geographic risk is not restricted to proliferating countries themselves. Countries and terrorist groups rely on transnational connections to carry out financing and procurement activities. For instance, both North Korea/DPRK and Iran have built programs leveraging global procurement networks to source goods, exploiting other jurisdictions to route the money in a way that is difficult for even the most sophisticated FIs to uncover. North Korea/DPRK relies on extensive corporate networks hosted in neighbouring countries, particularly those serving as regional trading and financial hubs. Proliferators may aim procurement efforts at countries with weak export control laws, and they may choose to have sensitive or Dual-Use goods delivered initially to trans-shipment hubs rather than directly to their home countries.

24- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 10.

- **Customer Risk:** Private sector entities should evaluate their customer base to identify sources of PF risk. Customer risk may emanate from the following dimensions:
  - Designated persons and entities: FIs, DNFBPs, and VASPs are prohibited from offering financial services to UN-designated individuals and entities.
  - Entities owned or controlled by designated persons: As part of the CDD process, FIs, DNFBPs, and VASPs must identify the individuals who own or control their legal entity customers and screen the names of these individuals against TFS lists. Even if FIs, DNFBPs, and VASPs are legally allowed to accept as a customer a company that is partly owned by a sanctioned person.The regulated entity must be aware that such a company may also be involved in proliferation activity and poses elevated risks.
  - Customer business type or activities: Legitimate customers in industries that produce sensitive or Dual-Use goods, or companies or institutions involved in advanced research can pose PF risk. Shipping companies, particularly those serving high-risk regions, may also present risks.
  - Customer geographic factors: The assessment of the institution's customer base should examine customers' locations of headquarters, countries of incorporation, and locations of operations (for entities); and customers' locations and nationalities (for individuals). Higher risk countries for PF include not just those jurisdictions that are directly involved in illicit PF and proliferation activities, but also those jurisdictions that have been identified in international reports as being locations of transnational procurement and financing networks.

- **Product and Service Risk**: Private sector entities should assess their product and service offerings for indicators of PF risk. Entities should assess the risk that their products and services may be used in any of the three PF stages: to obtain funding for WMD program activities; to enable the disguising of funds to distance the funds from a designated party; or to obtain Dual-Use goods or proliferation-sensitive goods or services[24]. Examples of products and services posing elevated PF risk include the following:
  - Trade finance transactions: Although documentary trade finance provides the involved FIs with data points that enable closer surveillance of a transaction (such as vessels involved, goods traded, etc.), trade finance still poses elevated PF risk because of the complexity of trade finance instruments and the potential involvement of controlled goods or technology.
  - Cross-border wires: Cross-border wires may not contain information about the purpose of a transaction, making it extremely difficult for the FIs involved to identify red flags for PF risk.

25- K2 Integrity, Dedicated Online Financial Integrity Network (DOLFIN), "Proliferation Finance: Risks."

- Correspondent banking services: Correspondent banking may present PF risks, particularly if the respondent bank is subject to lax PF regulatory standards. The PF risk appetite and due diligence standards of some banks often do not match those of international FIs. Correspondent banking may also expose an institution to higher-risk countries and underlying customers in a transaction.
- Products and services related to virtual assets: The virtual asset sector, and related products and services, are an emerging area of PF risk. This sector's importance for PF efforts is growing as proliferation actors increasingly face difficulties accessing the traditional financial system, so they are turning toward alternative methods for moving funds.

5. Preventive and Mitigating Measures for PF Risks

FIs, DNFBPs, and VASPs in the UAE are required take appropriate steps to manage and mitigate PF risks that they identify in their institutional risk assessment. AML/CFT policies and procedures must cover proliferation and PF and reflect CPF guidance and warnings issued by the EOCN, supervisory authorities, the FATF, and other relevant international best practices.

Enhanced Due Diligence for Customers and Transactions

FIs, DNFBPs, and VASPs should conduct enhanced due diligence (EDD) on all customers and transactions that are assessed as high-risk for PF.

A key objective of customer EDD is to collect information regarding the customer's expected behaviour, and to identify the expected end users of any strategic goods or Dual-Use goods and the customer's expected exposure to high-risk jurisdictions, including trans-shipment hubs. Another objective of the customer EDD is to mitigate the PF risk of a designated person concealing their identity or ownership of an entity. Potential customer EDD measures include, but are not limited to, the following:

- Obtaining additional information on the customer and the intended nature of the business relationship, and updating more frequently the identification data of the customer and beneficial owner;
- Obtain additional information on the customer's source of funds and wealth.
- Requiring customers to provide a list of main suppliers and customers, and conducting basic due diligence and public records searches on these entities;
- Reviewing the customer's customer acceptance policy, TFS policy, and any policies related to export controls, and requiring the customer to make changes if these policies are not sufficient;

- Obtaining senior management's approval to commence or continue the business relationship; Conducting enhanced monitoring of the business relationship by increasing the timing and number of controls applied.

Private sector entities should also apply EDD to transactions found to involve any proliferation-sensitive goods or services, regardless of whether the customer is itself in a high-risk category. As with customer onboarding, entities should seek to identify the end users of any strategic goods or Dual-Use goods. Private sector entities may request that the customer provide a valid export permit or a reference to the export control requirements in the relevant jurisdiction showing that the exported goods do not require a license.

Correspondent Banking Relationships

As explained above, banking services present elevated product and service risk for PF. It is important to note that correspondent banking enables international financial connectivity and global trade, and effective risk assessment and mitigation measures can facilitate financial security in correspondent transactions. However, FIs should ensure that their risk-rating and EDD processes for respondent banks consider, assess, and manage PF risk. Not all respondent banks present uniform risks, so FIs should evaluate the strength of potential respondents' internal controls, their geographic footprint, and characteristics of their underlying customer base. Additionally, FIs should perform ongoing due diligence on correspondent banking relationships, including periodic reviews of respondents' CDD information.

Insurance Products

Insurers, insurance brokers, insurance agents, and others operating in the insurance sector face PF risks, such as when providing insurance services for vessels. Companies providing vessel insurance are required to screen the vessel name, in addition to other relevant parties (for example, the vessel owner and operator), when providing an initial policy, as well as during insurance policy renewals, as vessels, or their owners or operators, may have been added to a relevant sanctions list in the time since the initial insurance policy was created[26]. Where PF risks relating to the insurance of vessels are identified, the insurer or insurance sector operator may mitigate these risks by requiring the vessel's owner to sign a warrant or other agreement that it complies with all UN and UAE TFS, and that it will not provide services to designated individuals or entities. Insurance companies should be aware of the PF risk that designated persons or those acting on their behalf may seek insurance cover for their vessels for the purpose of providing an appearance of legitimacy to their underlying, insured activities.

26- United Kingdom HM Treasury, National risk assessment of proliferation financing, September 2021, p. 15.

Shell and Front Companies

Although shell companies often serve a legitimate economic purpose, shell and front companies have been abused by designated individuals and entities seeking to obscure their involvement in transactions and evade TFS. Layers and networks of shell and front companies can make it extremely difficult for the private sector and authorities to track the flow of illicit funds around the globe. This PF risk demands that FIs, DNFBPs, and VASPs perform effective customer due diligence, and EDD when relevant, to fully identify their customers (including their customers' beneficial owners). Private sector entities should also monitor for the presence of shell companies in transactions, particularly companies from high-risk jurisdictions. When DNFBPs are engaging in corporate formation, they should be cognizant of the risk that proliferators may attempt to engage their services to create shell and front companies for the singular purpose of circumventing or evading TFS. DNFBPs should implement measures to understand the true nature of their customers' business and ownership and control structures[27].

Trade Finance and Dual-Use Goods

Trade finance instruments may be exploited by proliferators attempting to use cross-border trade of goods and commodities to evade TFS. FIs have more insights into trade finance transactions compared to cross-border wires (i.e., "open account" transactions) due to the extensive information in underlying documents, such as letters of credit, bills of lading, contracts, and invoices showing the quantity and price of goods traded[27]. Nonetheless, FIs should monitor trade finance transactions for PF risk indicators, including document discrepancies, under- or over-priced goods, involvement of sanctioned parties or vessels, and involvement of Dual-Use goods.

Dual-Use goods is defined as goods that may have both civilian and military uses. These items are generally controlled by governments via export controls, which prevent the export of certain items depending on the end user and end use of the item absent governmental permission. FIs, DNFBPs, and VASPs should be aware that Dual-Use goods are frequently controlled for export and should attempt to identify Dual-Use goods in transactions and provide enhanced scrutiny to such transactions. FIs should screen the UAE Control List (Cabinet Resolution No. 50 of 2020) in trade-based transactions that may involve Dual-Use goods. The import or export of Dual-Use goods require a permit from the relevant authorities.

27- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 42.
28- FATF, Guidance on Proliferation Financing Risk Assessment and Mitigation, p. 27.

Trade documentation such as bills of lading or letters of credit often do not include the level of detail needed to ascertain whether goods are controlled for export[29]. Nevertheless, private sector entities may be able to detect certain export-related red flags present in transactions. If there is a reasonable suspicion that the goods involved in the transaction could be used in the development, production, or use of products related to WMD, the customer should be required to provide more information about the product, including technical specifications, as well as the end use and end user of the product.

Training and Education for Staff

One challenge many private sector institutions face in identifying PF activities is that the typologies often resemble other types of financial crimes (such as trade-based money laundering) but have significant divergences that can make traditional preventive measures ineffective, for example, the involvement of goods or materials that are difficult to identify as proliferation-sensitive. Moreover, proliferators go to great lengths to conceal their behaviour and the sources and destinations of funds, and they have developed sophisticated TFS evasion techniques.

This situation requires FIs, DNBFPs, and VASPs to ensure that all staff are educated on the basic principles of WMD proliferation and PF and that staff with critical positions in the compliance and audit functions related to higher-risk products and services, such as trade finance, receive additional training about PF typologies and red flags. A list of red flags for possible PF activities is presented in Section 7 of this Guidance. In addition, the Executive Office have issued a Typologies paper that constitutes specific PF typologies[30] .

29- Wolfsberg Group, International Chamber of Commerce, and Bankers Association for Finance and Trade, "Trade Finance Principles" (2019 amendment), https://www.wolfsberg-principles.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf, p. 21.
30- Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction. https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=2bed11bf-4a94-4a16-a9f3-87db9f4e69f6

6. Process for Transactions Involving Dual-Use Goods

While conducting transactions (specifically trade-based), FIs, DNFBPs and VASPs may come across transactions that involve the import or export of Dual-Use items that are export controlled. In such instances, below are the additional due diligence steps that should be taken:

Step 1: Screen trade-based documentation (such as Bill of Lading, Bill of Sales, Sales & Purchase Agreements, etc.) for alerts against the UAE Control List to be able to identify items that may be export controlled.

Step 2: If an alert is identified, the next step is to request more information from the client. This includes requesting technical specifications (e.g. catalog, manual, etc.) of the item, as well as information on the end-use and end-user of the item.

Step 3: There are two possible scenarios following the review of the item's specifications:

Scenario 1: **You have verified that the item is controlled.**

- Ensure client has a valid permit issued by the EOCN before processing the transaction.

Scenario 2: **You are unable to verify whether the item is controlled.**

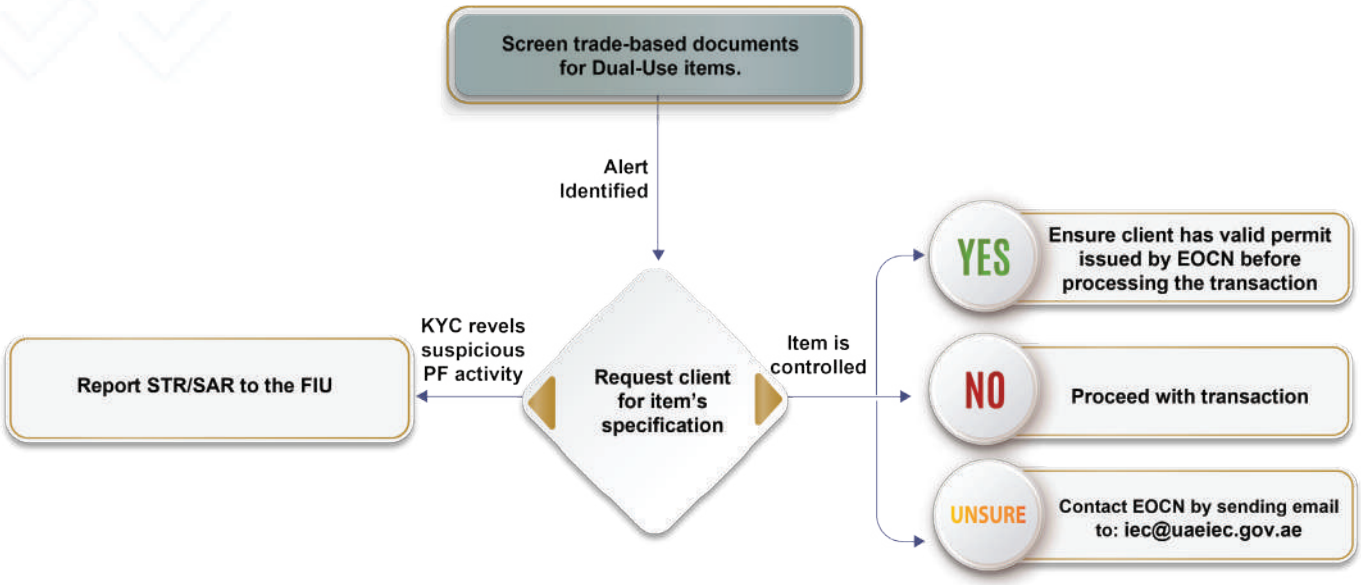
1. Contact the technical support team at the EOCN by sending email to iec@uaeiec.gov.ae.
2. Attach the technical specifications (e.g., catalog) of the item in the email.
3. The EOCN support team will provide a response to your query:

- If the item is controlled, ensure the client has a valid permit issued by the EOCN before processing the transaction.
- If the item is not controlled, you may proceed with the transaction.

While conducting the due diligence checks, FIs, DNFBPs and VASPs may come across suspicious proliferation financing red flags. In such cases, FIs, DNFBPs and VASPs should report suspicious PF activities to the UAE Financial Intelligence Unit (FIU). See Section 9 below for more details.

Important: Trading in Dual-Use goods merely is not considered a suspicious activity if the parties involved have obtained the proper permits, and there is no presence of any PF related red flags following the due diligence checks.

The diagram below provides a process map for dealing with transactions involving Dual-Use goods:



How to Use the List – Example

- Your client is attempting a transaction to export goods. While screening trade-based documentation, an item described as a **(semi-conductor)** has been identified without detailed description on the specifications of the item. Client should be requested to submit technical specifications of the item to determine whether it is controlled or not.
- While not all types of semi-conductors are controlled, semiconductors with certain specifications may fall under controlled dual-use items. As an example, semiconductors can be used in both refrigerators (civilian) and missile guidance systems (military).
- A screening alert appears on a controlled item listed on the UAE Control List. The item is listed as a (Solid-state power **semiconductor** switches, diodes, or 'modules') in the UAE Control List, which is controlled if it meets certain specifications.
- Following review of the item's specifications, you are unable to verify whether the item is controlled. In this case, you should follow the process detailed under **Scenario Two** above.
- In addition, the due diligence checks have identified the following red flags:
    - o The export of semi-conductors is not in line with the regular business activity of the client
    - o The client is reluctant to provide an export permit issued by the EOCN, and;
    - o The shipment is being exported to a country of proliferation concern.

    In this case, you should consider reporting an STR/SAR to the FIU.

7. Good v Bad Practices on TFS - PF Compliance

	Good Practices	Bad Practices
Screening	Information on goods / items contained in trade documents is used to screen against the UAE Control List	Information contained in trade documentation is not screened against sanctions lists and the UAE Control List
Staff Expertise	Staff in trade-based roles have a common understanding of dual-use goods and can identify related red flags	Staff dealing with trade-related sanctions queries are not qualified and experienced to perform the role effectively
Reporting	Raising STRs/SARs when encountering suspicious activities indicative of PF and sanctions evasion	Lack of reporting suspicious PF and sanctions evasion activities
Trade-Based CDD	Confirm with exporters (in higher risk situations) whether a government license is required for the item and seek a copy	No requests are made to verify license requirements for trading in dual-use items
UBO CDD	UBOs are diligently screened to identify links between clients acting as front companies and individuals / entities sanctioned for PF	UBOs are not properly screened, leading to failure in identifying links between front company clients and sanctioned PF parties.

8. TFS / PF International Obligations

UN Security Council Resolutions

The UNSC imposes global and country-specific prohibitions related to PF under Chapter VII of the UN Charter applicable to UN Member States, including the UAE.

Global approach under UNSCR 1540 (2004) and its successor resolutions: UNSCR 1540 constitutes the overarching global requirement related to PF. It focuses on activities and is not a state-specific sanctions resolution. There are no requirements, for example, to freeze assets of named individuals or entities. UNSCR 1540 requires that UN Member States implement legislation to prohibit non-state actors (including terrorists) from financing the manufacture, acquisition, possession, development, transport, transfer, or use of WMDs, and to control the provision of funds and financing for export and trans-shipment of WMDs and related materials.

Country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their (future) successor resolutions: In addition to the global prohibitions embedded in UNSCR 1540, the UNSC has imposed sanctions resolutions to target the WMD-proliferation activity of specific Member States, namely, the DPRK and Iran, under UNSCR 1718 (2006) and UNSCR 2231 (2015). These resolutions, among other requirements, require Member States 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 the UNSC.

Regarding DPRK-related sanctions, the scope and nature of DPRK-related sanctions have been expanded in response to the country's repeated violations of UN resolutions[31]. Sanctions against the DPRK, managed by the UN Security Council's 1718 Committee, combine targeted financial sanctions, activity-based sanctions, and sectoral sanctions. The UNSC has issued nine subsequent sanctions resolutions. Pre-2016 measures were narrowly targeted toward prohibiting conduct connected to weapons proliferation, enforced through targeted financial sanctions and a luxury goods ban. Since 2016, measures have included significant increases in the scope and nature of prohibitions, including a variety of sectoral and activity-based measures in addition to targeted financial sanctions.

31- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 4.

Regarding Iran-related sanctions, UNSCR 2231 (2015) and the implementation of the Joint Comprehensive Plan of Action (JCPOA) terminated prior resolutions relating to Iran and PF, including UNSCRs 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010). However, UNSCR 2231 (2015) has retained targeted financial sanctions against certain designated individuals and entities under these resolutions and implemented new specific restrictions[32]In sum, targeted financial sanctions related to PF under UNSCR 1718 (2006) and UNSCR 2231 (2015) form the basis for FATF Recommendation 7 and its Interpretive Note, and Immediate Outcome 11, discussed below[33].

FATF Recommendation 7 and Immediate Outcome 11

The FATF Standards outline measures to facilitate implementation of the relevant UNSCRs related to PF, adopted under Chapter VII of the UN Charter. These measures—FATF Recommendation 7 and its Interpretive Note, and Immediate Outcome 11—are currently applicable to two country-specific regimes: the DPRK and Iran. The UAE complies with these requirements, which are reflected in the laws and regulations that comprise the UAE's CPF legal and regulatory framework and are implemented under the central oversight of the EOCN in coordination with supervisory authorities, law enforcement, and other UAE agencies.

FATF Recommendation 7 and its Interpretive Note: FATF Recommendation 7 states that countries are required to implement TFS imposed under UNSCRs related to the "prevention, suppression and disruption of proliferation of WMD and its financing[34]." TFS related to PF are applicable to persons and entities designated by either the UNSC, or a relevant committee of the UNSC. The specific designation and listing criteria are the following[35]:

- Persons or entities engaging in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;
- Persons or entities acting on behalf of or at the direction of designated persons or entities;
- Entities owned or controlled by designated persons or entities; and
- Persons or entities assisting designated persons or entities in evading sanctions, or violating resolution provisions.

32- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 4.
33- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 4.
34- FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Updated October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 13.
35- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 6.

In accordance with FATF Recommendation 7, countries are required to immediately freeze funds and other financial assets and economic resources that are in their territories or under their jurisdiction that are owned or controlled, directly or indirectly, by the persons/entities mentioned above[35]. Countries are likewise responsible to ensure that no funds or other assets and economic resources are made available to such persons and entities, except in specific situations, and under conditions specified in the UNSCRs[37].

The Interpretive Note to Recommendation 7 provides further information with specific requirements for countries to effectively implement targeted financial sanctions related to PF. The requirements that are relevant to FIs, DNFBPs, and VASPs are the following:

- Freezing and prohibiting dealing in funds or other assets of designated persons and entities: The Interpretive Note to Recommendation 7 instructs countries to "require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities[38]." In this capacity, countries should apply measures for preventing prohibited payments, preserving the "rights of innocent third parties," cooperating with international counterparts, and preventing asset flight to ensure effective compliance[39].
- Post-freezing reporting and investigation: The Interpretive Note to Recommendation 7 also recommends that countries require FIs and DNFBPs to report to competent authorities "any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions, and ensure that such information is effectively utilized by competent authorities[40]."

FATF Immediate Outcome 11: FATF Immediate Outcome 11 requires that "Persons and entities involved in the proliferation of WMDs are prevented from raising, moving and using funds, consistent with the relevant UNSCRs." An effective system in relation to Immediate Outcome 11 ensures that "Persons and entities designated by the UNSCRs on proliferation of WMD are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation[41]."

36- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 6.
37- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, p. 6.
38- FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Updated October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 54.
39- FATF, Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, pp. 9-10.
40- FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Updated October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 54.
41- FATF, Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, Updated November 2020, https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf , pp. 126-27.

To that end, countries must demonstrate that they fully and accurately implement targeted financial sanctions "without delay." In addition, countries must have measures for monitoring and ensuring compliance by FIs and DNFBPs, specifically through "adequate co-operation and co-ordination between the relevant authorities" with policies and measures that prevent sanctions evasion and combat PF[41]."

FATF Immediate Outcome 11: FATF Immediate Outcome 11 requires that "Persons and entities involved in the proliferation of WMDs are prevented from raising, moving and using funds, consistent with the relevant UNSCRs." An effective system in relation to Immediate Outcome 11 ensures that "Persons and entities designated by the UNSCRs on proliferation of WMD are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation[40]." To that end, countries must demonstrate that they fully and accurately implement targeted financial sanctions "without delay." In addition, countries must have measures for monitoring and ensuring compliance by FIs and DNFBPs, specifically through "adequate co-operation and co-ordination between the relevant authorities" with policies and measures that prevent sanctions evasion and combat PF[42]."

9. Sanction Evasion and Red Flags for Possible PF Activities

FIs, DNFBPs, and VASPs are required to file a suspicious transaction report (STR) or suspicious activity report (SAR) to the UAE Financial Intelligence Unit (FIU) when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. STR/SAR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. STR/SAR filings are essential to assisting law enforcement authorities in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

The following red-flags are specific to proliferation financing cases related to the UAE and other regional countries which can help the FIs, DNFBPs and VASPs to detect the suspicious transaction and report STRs to the FIU:

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector.

42- FATF, Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, Updated November 2020, https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf , pp. 126-27.

- Dealings with sanctioned goods or Dual-Use goods.
- Identifying documents (e.g. bill of lading, sales puchase agreement, etc.) that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
  - For companies, they are importing high-end technology devices which is not in accordance with their trade license.
  - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide humanitarian aid.
- Complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.

Appendix A reflects comprehensive red flag indicators to help financial institutions detect activities related to proliferation or PF.

For guidance on how to report confirmed or potential matches, FIs, DNFBPs, and VASPs should refer to the "Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs" issued by the EOCN.

Appendix A

Global standards-setters have identified the following "red flag" indicators to help financial institutions detect activities related to proliferation or PF. Such "red flag" indicators suggest the likelihood of the occurrence of unusual or suspicious activity, including possible PF activities, terrorist financing, and evasion of TFS. The evasion of TFS is an attempt to avoid the prohibitions and restrictions of TFS, using tactics such as renaming, using intermediaries, creating front companies, and using alternative financial networks. The existence of a single standalone indicator may not on its own warrant suspicion of a TFS evasion attempt or PF, nor will a single indicator necessarily provide a clear indication of such activity, but could prompt further monitoring and examination, including the application of customer or transactional EDD, as appropriate.

a. Customer Profile Risk Indicators

- During onboarding, a customer provides vague or incomplete information about their proposed trading activities. The customer is reluctant to provide additional information about their activities when queried.
- During subsequent stages of due diligence, a customer, particularly a trade entity, or its owners or senior managers, appears in sanctioned lists or negative news, e.g., relating to past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes.
- The customer is a person connected with a country of proliferation or diversion concern, e.g., through business or trade relations, as identified through the national risk assessment process or by relevant national CPF authorities.
- The customer is a person dealing with Dual-Use goods, goods subject to export control goods, or complex equipment for which he/she lacks technical background, or that is incongruent with their stated line of activity.
- 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 established at onboarding.
- 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 a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the originators appear to be entities who may be connected with 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 goods or goods subject to export control.
- Customer activity does not match the customer's business profile, or end-user information does not match the end-user's business profile.
- A new customer requests a letter of credit transaction while awaiting approval of new account.

b. Account and Transaction Activity Risk Indicators

- A transaction involves person or entity in foreign country of proliferation concern.
- A transaction involves person or entity in foreign country of diversion concern.
- A transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Wire transfer activity shows unusual patterns or has no business or apparent lawful purpose.
- 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.
- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g., companies do not have a high level of capitalisation or displays other shell company indicators. Countries or the private sector may identify more indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity.
- Business or compliance personnel identify links between representatives of companies exchanging goods, e.g., the same owners or management, physical address, IP address, or telephone number, or activities that appear to be co-ordinated.
- The account holder conducts financial transactions in a circuitous manner.
- A transaction or account activity involves an originator or beneficiary that 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).
- The 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 obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies that maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance these accounts.
- The 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.
- 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.

c. Maritime Sector Risk Indicators

- An order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- 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, 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; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.
- A shipment of goods has a low declared value vis-à-vis the shipping cost.
- A shipment of goods is incompatible with the technical level of the country to which it is being shipped, e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- A 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.

- A 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 trade transaction documents.
- A shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, weak 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 with no clear economic reasons, e.g., by a shell or front company not involved in the trade transaction.

d. Trade Finance Risk Indicators

- A trade finance transaction involves a shipment route (if available) through a country with weak export control laws or weak enforcement of export control laws.
- A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- A transaction involves a shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import good involved?).
- Based on the documentation obtained in the transaction, the declared value of the shipment is obviously under-valued vis-à-vis the shipping cost.
- Prior to account approval, the customer requests a letter of credit for a trade transaction to ship Dual-Use goods or goods subject to export control.
- Lack of full information or inconsistences are identified in trade documents and financial flows, such as names, companies, addresses, final destination, etc.
- Identifying documents seem to be forged or counterfeited.
- Identifying documents seem to be tampered or modified documents with no apparent explanation, especially those related to international trade.
- Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

Document Version Update

Date: 01 November 2022

Section	Update
Section 3	• Additional information on UAE Control List • Added criteria for issuance of EOCN permits
Section 4	Added typologies used by PF state actors
New Section (Section 6)	Process for Transactions Involving Dual-Use Goods
New Section (Section 7)	Good v Bad Practices on TFS – PF Compliance
Sections 8 and 9	Renumbered sections (previously 6 and 7)