Combating Proliferation Financing & Sanctions Evasion

Aim of the session

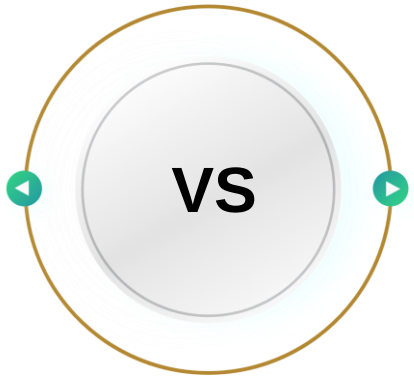
Raise awareness and provide insights into:

- Definition of WMD proliferation and proliferation financing.
- Stages of proliferation financing.
- UAE’s framework on counter-proliferation and its financing.
- Understanding, assessing, and mitigating PF risks.
- PF red flags, case studies, and reporting suspicious PF activities.
- Good and bad practices to combatting proliferation financing.

Definition of WMD Proliferation vs Proliferation Financing

WMD Proliferation
(The **Act**)

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).



Proliferation Financing
(The **Financing** of the Act)

Proliferation Financing 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).

Stages of Proliferation Financing

PF can be understood as taking place over three stages:

Stage 1

Program Fundraising

A proliferating country **raises financial resources** for in-country costs. The funding sources may derive from:

- Country's budget.
- Profits from an overseas commercial enterprise network.
- Proceeds from an overseas criminal activity network.

Stage 2

Disguising the Funds

The proliferating state **moves assets** into the international financial system, often involving a foreign exchange transaction, for trade purposes.

Examples include:

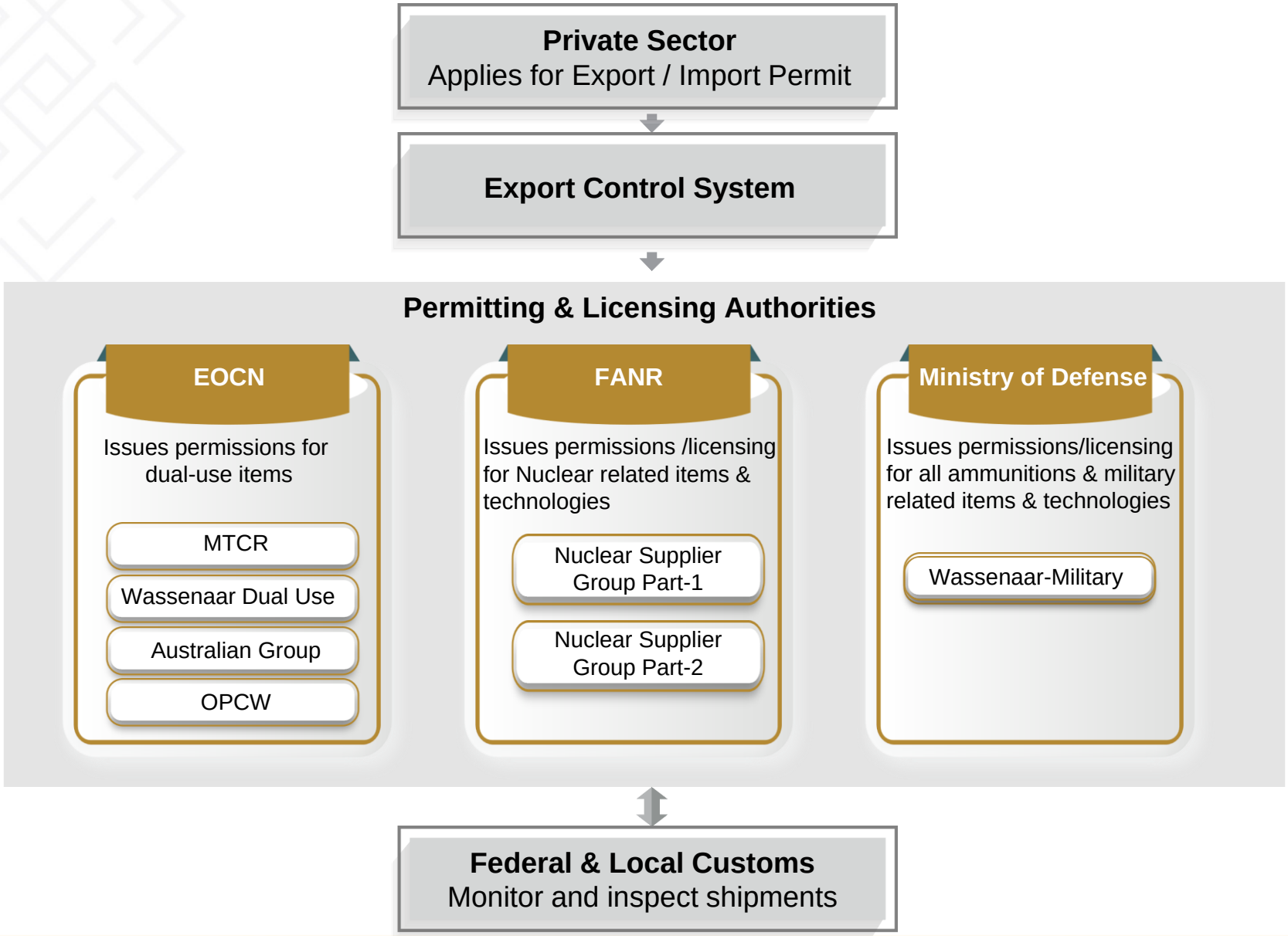
- Use of correspondent banking channels.
- Use of procurement agents.
- Use of front and shell companies.

Stage 3

Materials 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.

UAE Counter Proliferation and CPF Framework



What is a Dual-Use item?

Definition:

- Dual-use items are goods, software and technology that can be used for both civilian and military applications.

Example:

Signal Analyser

Metal Powder

Accelerometer

Pressure Transducer

Servo

Graphite and Ceramic Materials

How Dual-Use items can be used?

Medical Equipment

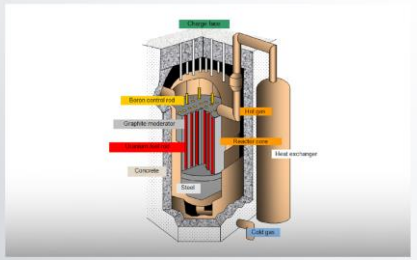
Servo

Missile Technology

Pencil

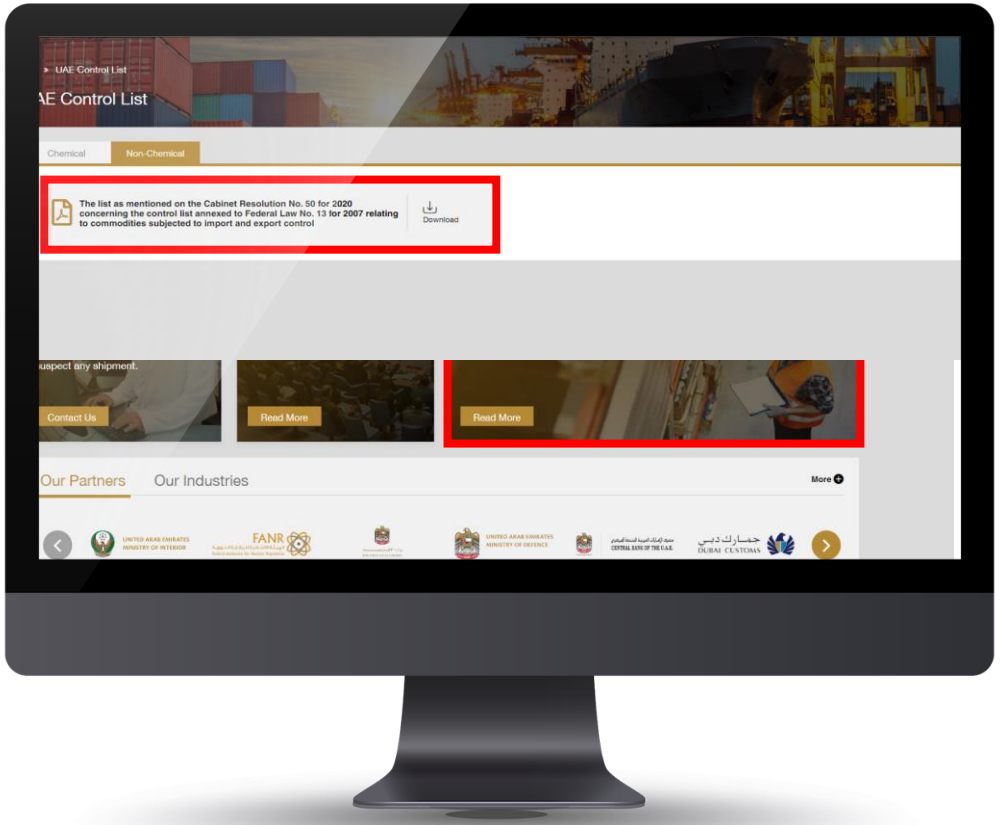
Graphite and Ceramic Materials

Nuclear Reactor



UAE Control List

The UAE Control List implements internationally agreed dual-use goods subject to import and export control and can be found in Cabinet Decision No. 50 of 2020. The list can be accessed through the EOCN website at https://www.uaeiec.gov.ae/en-us/control-list-good



UAE Control List Categories

The UAE Control List is composed of 11 categories based on the technology used. Each category includes a technical description of the items and their control parameters.

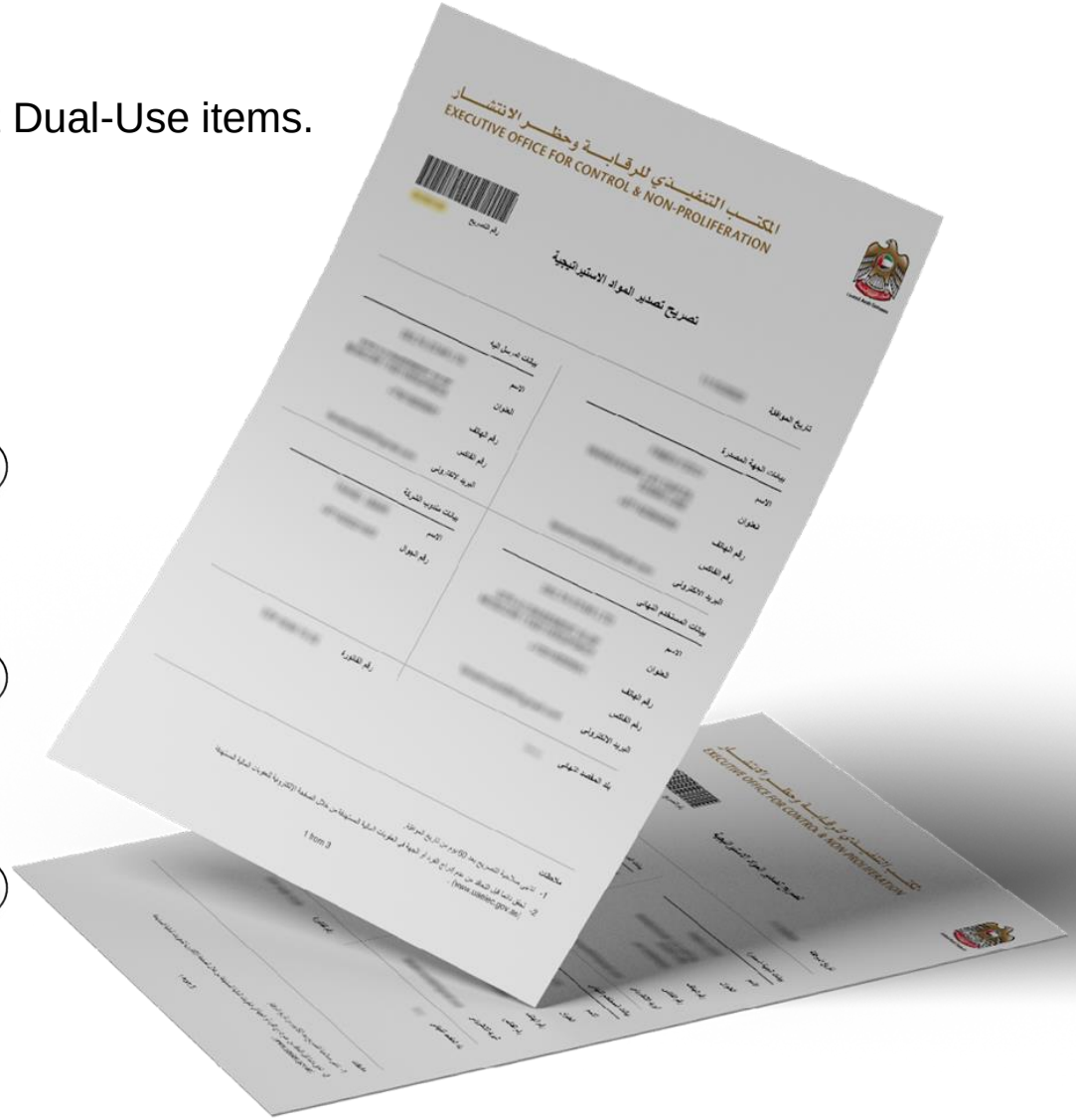
Category	Type / mandate	Example of controlled items used in WMD programs
0	**Nuclear Materials**	Nuclear Reactor - Pressure Tubes - Zirconium Metal Tubes - Steam generators
1	**Special Materials**	Protective and detection equipment - Body armour and components - High-density lead glass
2	**Material Processing**	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

EOCN Dual-Use Permits

The EOCN issues permits to companies that import/export Dual-Use items.

The permits are issued based on three main criteria:

1. Technical description and specifications of the Dual-Use item.
2. End-use of the Dual-Use item.
3. End-user of the Dual-Use item.

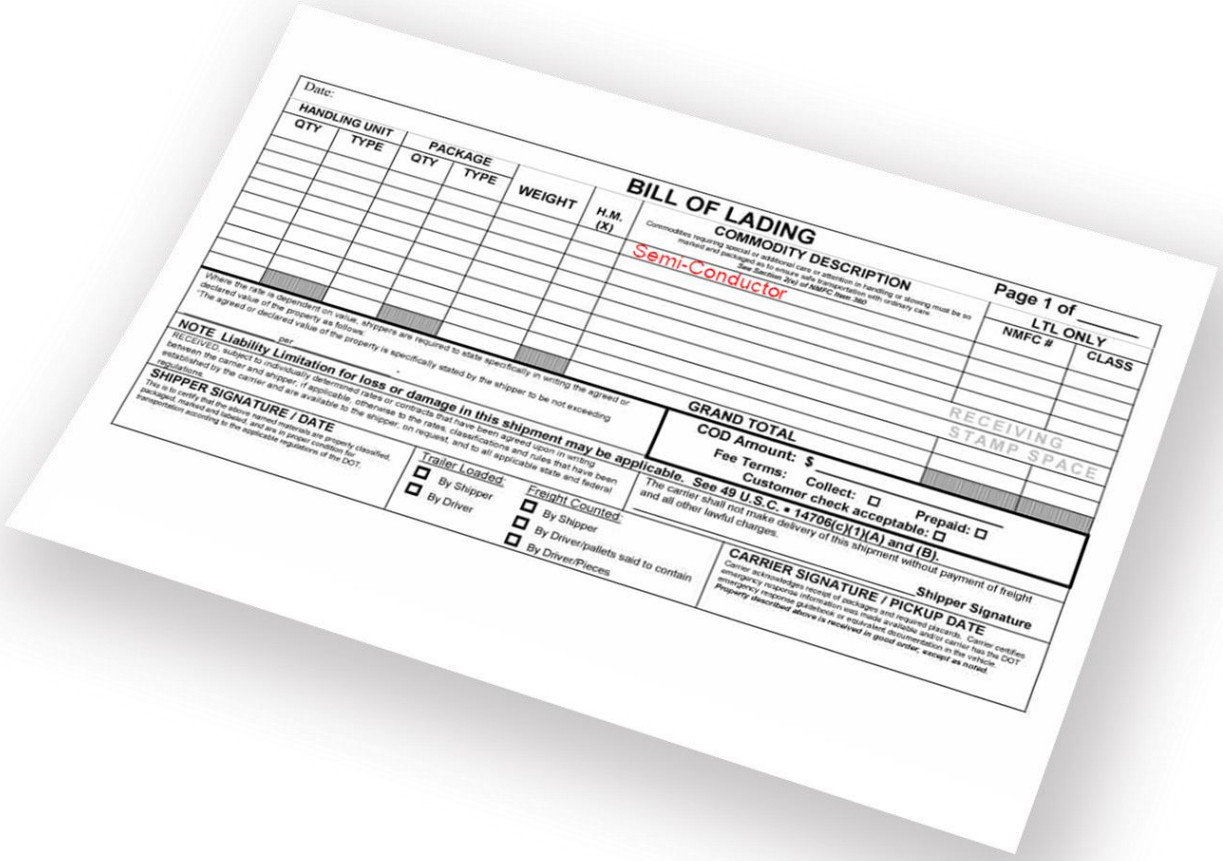


How to use the list – Example

Example:

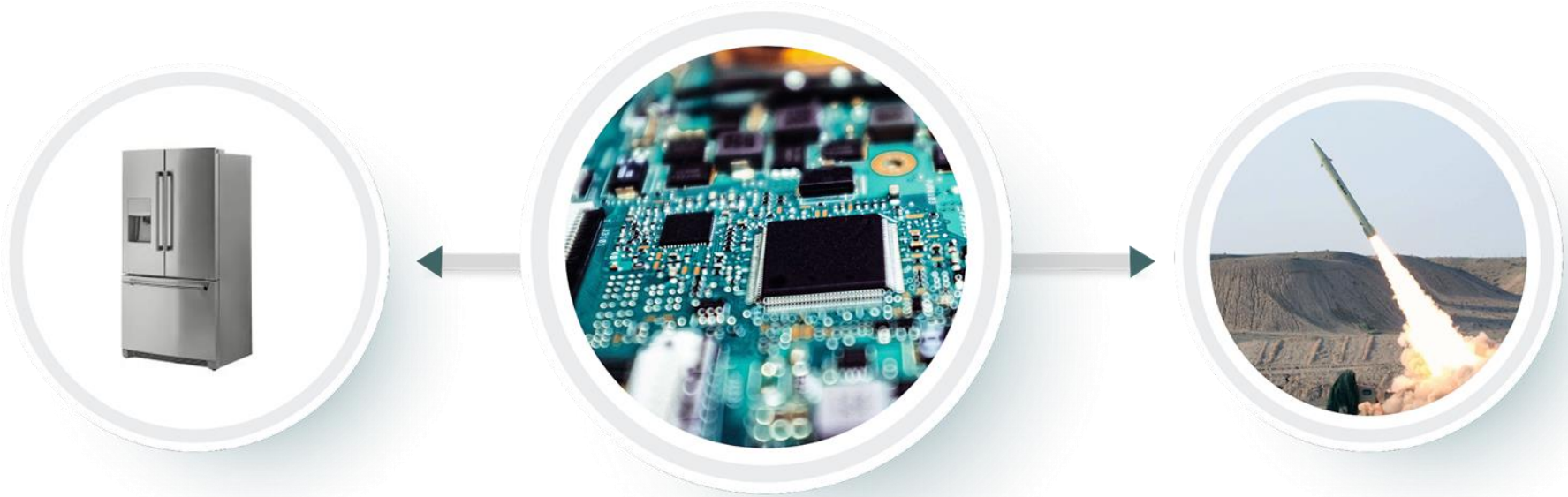
- Your client is attempting a transaction to export goods. While screening trade-based documentation, an item described as a (semi-conductor) has been identified without detailed description on the specifications of the item.

- Client should be requested to submit technical specifications of the item to determine whether it is controlled or not.



How to use the list – Example (cont'd)

- Semiconductors can be used in both **refrigerators (civilian)** and **missile guidance systems (military)**.
- While not all types of semi-conductors are controlled, semiconductors with certain specifications may fall under controlled dual-use items.



How to use the list – Example (cont'd)

- 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'), which is controlled if it meets certain specifications.

UNITED ARAB EMIRATES
THE CABINET

الإمارات العربية المتحدة
مجلس الوزراء

Annex **الملحق**

Schedule of strategic goods attached to Federal Law No. (13) of 2007 regarding subject to import and export control

جدول السلع الاستراتيجية الملحق بالقانون الاتحادي رقم (13) لسنة 2007 بشأن السلع الخاضعة لرقابة الاستيراد والتصدير

This Schedule 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) or other related systems.

يُطبق هذا الجدول الضوابط المتفق عليها دولياً فيما يتعلق بالسلع ذات الاستخدام المزدوج والخاضعة لرقابة الاستيراد والتصدير بما في ذلك نظام مراقبة تكنولوجيا الصواريخ (MTCR) ومجموعة موردي المواد النووية (NSG) واتفاق واسنار (WA) ومجموعة أستراليا (AG) واتفاقية الأسلحة الكيميائية (CWC) ومنظمة حظر الأسلحة الكيميائية (OPCW) أو أي أنظمة أخرى ذات علاقة.

h. Solid-state power semiconductor switches, diodes, or 'modules', having all of the following:

1. Rated for a maximum operating junction temperature greater than 488 K (215 °C);

2. Repetitive peak off-state voltage (blocking voltage) exceeding 300 V; and

3. Continuous current greater than 1 A.

Note 1: Repetitive peak off-state voltage in 3A001.h. includes drain to source voltage, collector to emitter voltage, repetitive peak reverse voltage and peak repetitive off-state blocking voltage.

Note 2: 3A001.h. includes:

— Junction Field Effect Transistors (JFETs)

— Vertical Junction Field Effect Transistors (VJFETs)

120

How to use the list – Example (cont'd)

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.

How to use the list – Example (cont'd)

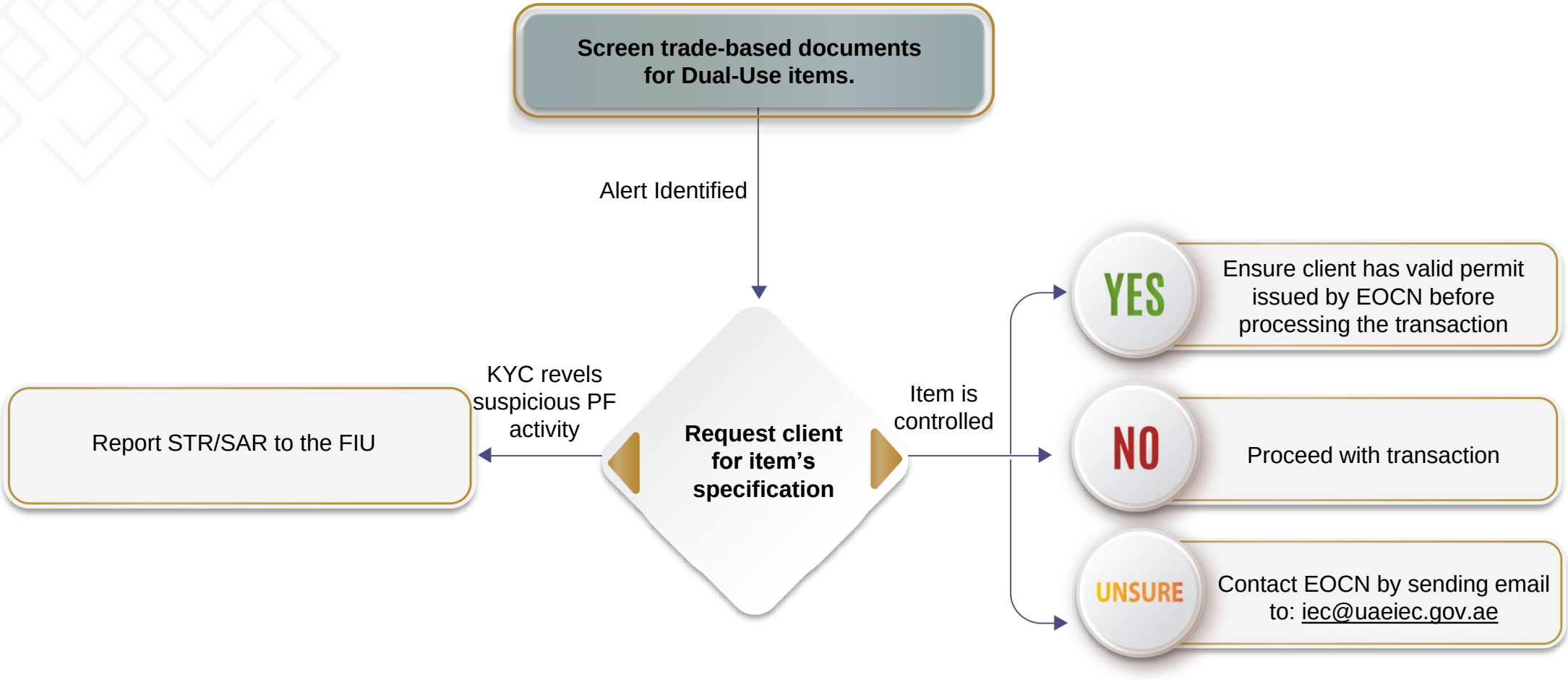
If you come across suspicious activity while conducting the client's KYC, such as:

1. The export of semi-conductors is **not in line with the regular business activity** of the client
2. The client is **reluctant to provide an export permit** issued by the EOCN, and;
3. The shipment is being **exported to a country of proliferation concern.**

In this case, you should consider reporting an STR/SAR to the FIU using the below red flags:

- PF – A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.
- PF – Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.

Process for Transactions with Dual-Use items



Understanding and Assessing PF Risks

Definition of Proliferation Financing Risk (as per FATF)

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.

Risk is a function of three factors

Threats

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.

Vulnerabilities

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.

Consequences

refers to the **outcome** where funds or assets are made available to designated persons and entities.

PF Threats

Key proliferation financing 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

North Korea/DPRK (UNSCR 1718) and **Iran (UNSCR 2231)** 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.

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".

Sanctions Evasion Methods used by PF Threats

Commonly used typologies by the DPRK &Iran to evade sanctions

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.

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.

Source : US DOS, DOT, & DOC Joint Advisory “North Korea Ballistic Missile Procurement Advisory”

PF Vulnerabilities

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.

Types of Vulnerabilities

Structural

- Nature, scale, and geographical footprint of the entity's business.
- Customer base's characteristics.
- Volume and size of transactions flowing through the entity.

Sectoral

- Banking or money and value transfer services.
- Trust and company service providers.
- Virtual Asset Service Providers (VASPs).

Product or Service-Specific

- Product or service is complex, enables cross-border transactions, appeals to a diverse customer base, or is provided by multiple subsidiaries or branches.
- E.G: correspondent banking, trade finance, etc.

Customer or Transaction

- Exposure to customers or transactions that are higher risk for PF.

Preventive and Mitigating Measures for PF Risk

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.

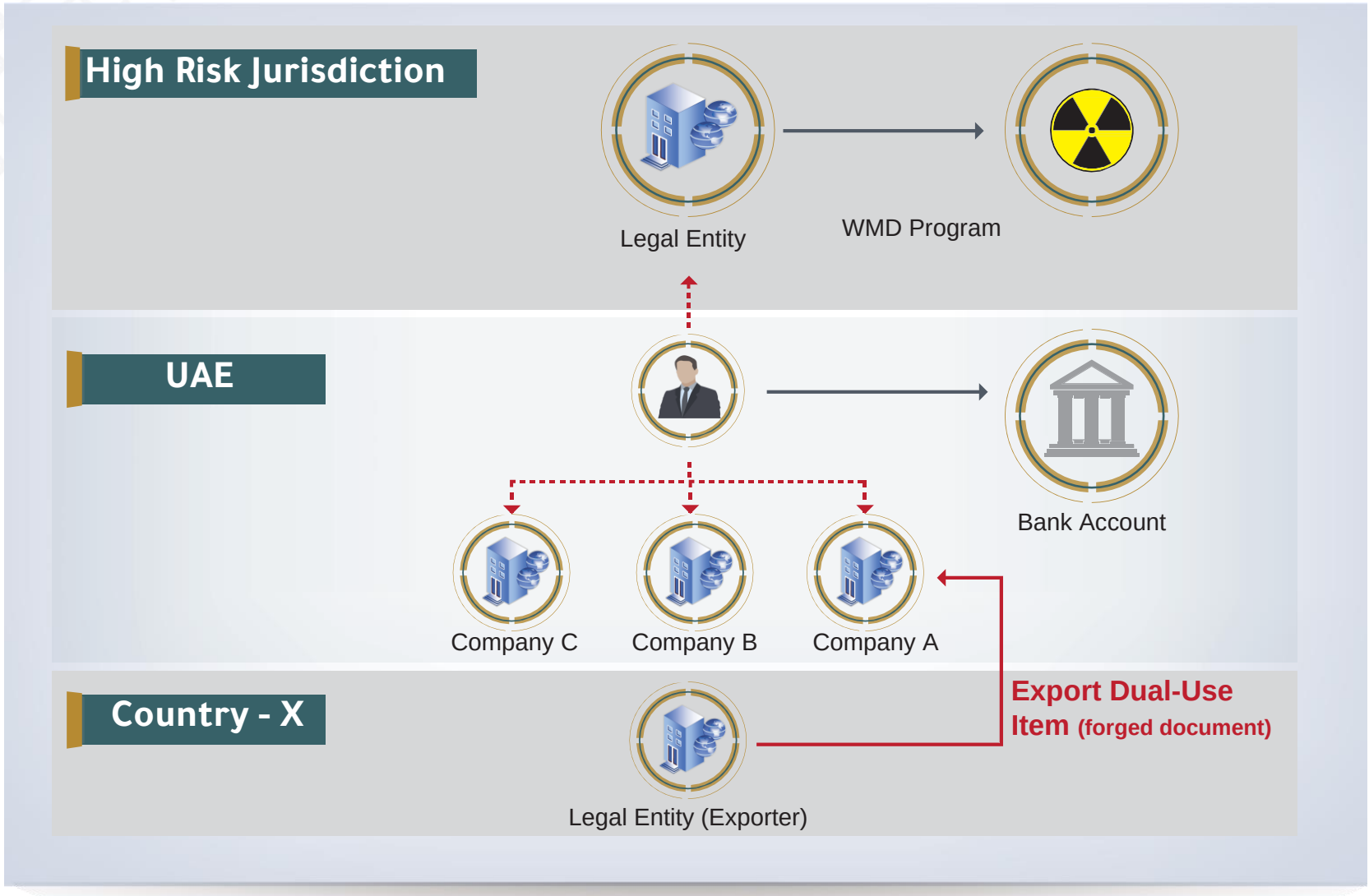
PF Sanctions Evasion and Risk Indicators

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.

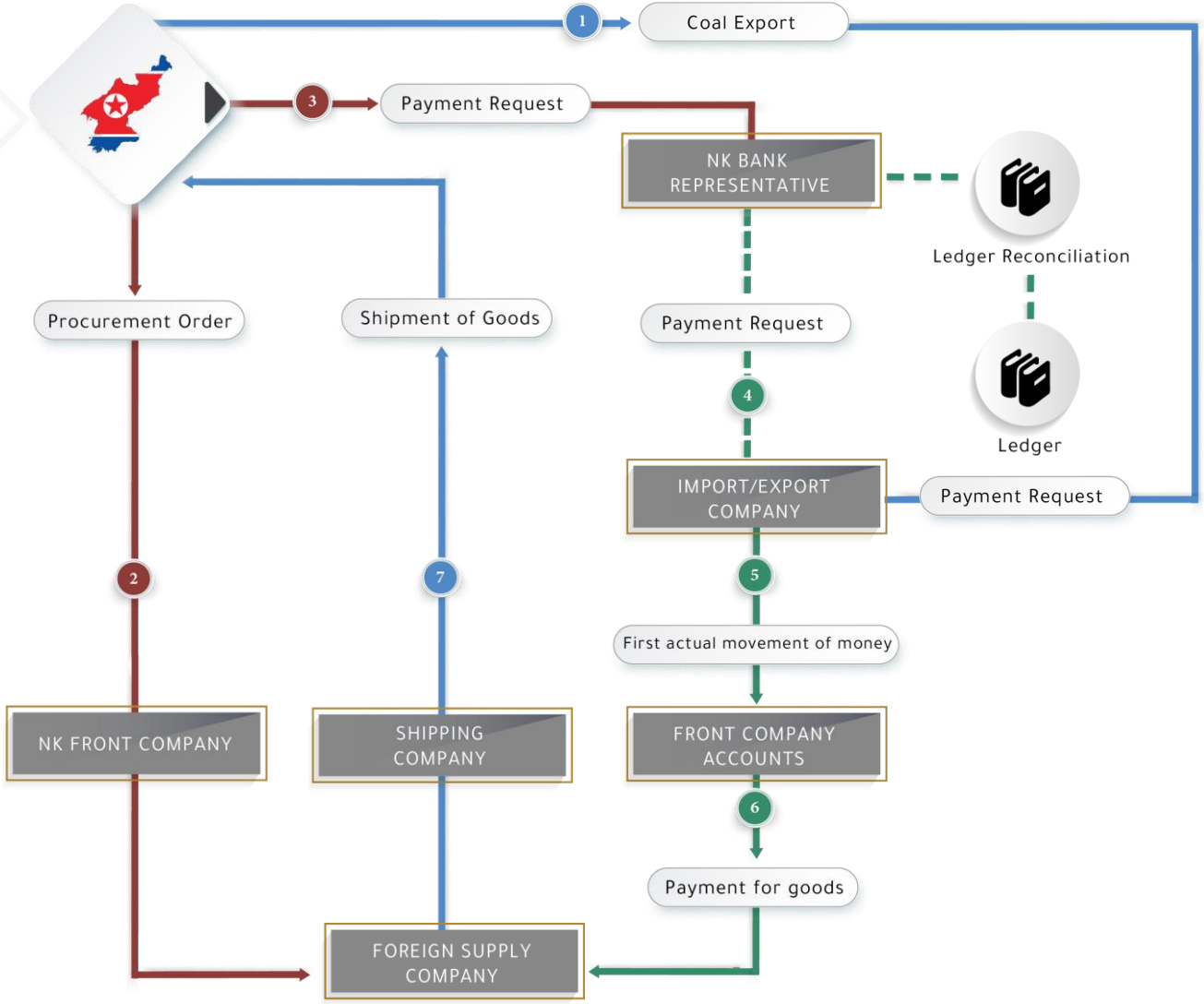
Categories of PF Risk Indicators

Customer Profile	Risk indicators that relate to the customer's profile, such as links to high-risk jurisdiction.
Account and Transaction Activity	Risk indicators that relate to the transaction activity, such as unusual transactions with unclear business purpose.
Maritime Sector	Risk indicators that relate to the maritime sector, such as shipments of goods that are incompatible with technical level of receiving country.
Trade Finance	Risk indicators that relate to the trade finance sector, such as inconsistencies in trade documents when providing letter of credits.

PF Case Study: Forged Document & Shipping of Dual-Use Items



DPRK Case Study



Source : FinCEN Advisory/FIN-2017-A008

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.

Recommendations to Banks

- Identify, understand, and assess proliferation financing risks for customers, products and services, and delivery channels.
- Conduct enhanced due diligence on customers and transactions linked to high-risk PF jurisdictions, particularly DPRK and Iran, and monitor for presence of front companies.
- Perform ongoing due diligence on correspondent banking relationships, including periodic reviews of respondents' CDD information.
- Screen trade-based documentations against the UAE Control List and verify end users of shipments.
- Report suspicious sanctions evasion activities related to PF by raising an STR/SAR to the UAE FIU.

Recommendations to Money Service Businesses

- Identify, understand, and assess proliferation financing risks for customers, products and services, and delivery channels.
- Conduct enhanced due diligence on customers and transactions linked to high-risk PF jurisdictions, particularly DPRK and Iran, and monitor for presence of front companies. EDD should include counterpart MSBs with a high PF risk profile.
- Be alert for payments, transfers, or hawalas that are conducted to facilitate trade of Dual-Use goods that are export controlled and ensure valid license is obtained.
- Integrate the PF red flags in your screening systems to help detect suspicious transactions related to PF sanctions evasion.
- Report suspicious sanctions evasion activities related to PF by raising an STR/SAR to the UAE FIU.

Recommendations to Insurance Firms

- Identify, understand, and assess proliferation financing risks for customers, products and services, and delivery channels.
- Conduct enhanced due diligence on transactions involving high-risk PF jurisdictions, particularly when providing insurance cover for parties that have a presence in those jurisdictions.
- When providing vessel insurance, screen the vessel name, in addition to other relevant parties, such as the vessel owner and operator, to ensure they are not linked to designated persons.
- When providing inventory insurance, screen the goods insured against the UAE Control List and ensure that your client holds a valid permit to trade in such goods before entering an insurance agreement.
- Report suspicious sanctions evasion activities related to PF by raising an STR/SAR to the UAE FIU.

Recommendations to DNFBPs

- Identify, understand, and assess proliferation financing risks for customers, products and services, and delivery channels.
- Conduct enhanced due diligence on transactions involving high-risk PF jurisdictions, particularly when providing insurance cover for parties that have a presence in those jurisdictions.
- Monitor for the presence of front companies when engaging in company formation services and verify the ultimate beneficial owners.
- Perform ongoing due diligence on counterparts in the DPMS supply chain, specifically when engaging with mining/production and wholesale/trading partners.
- Report suspicious sanctions evasion activities related to PF by raising an STR/SAR to the UAE FIU.

Executive Office Materials & Publications

CLICK HERE
For More Information

المكتب التنفيذي للرقابة وحظر الانتشار

EXECUTIVE OFFICE FOR CONTROL & NON-PROLIFERATION

United Arab Emirates

@EOCNUAE

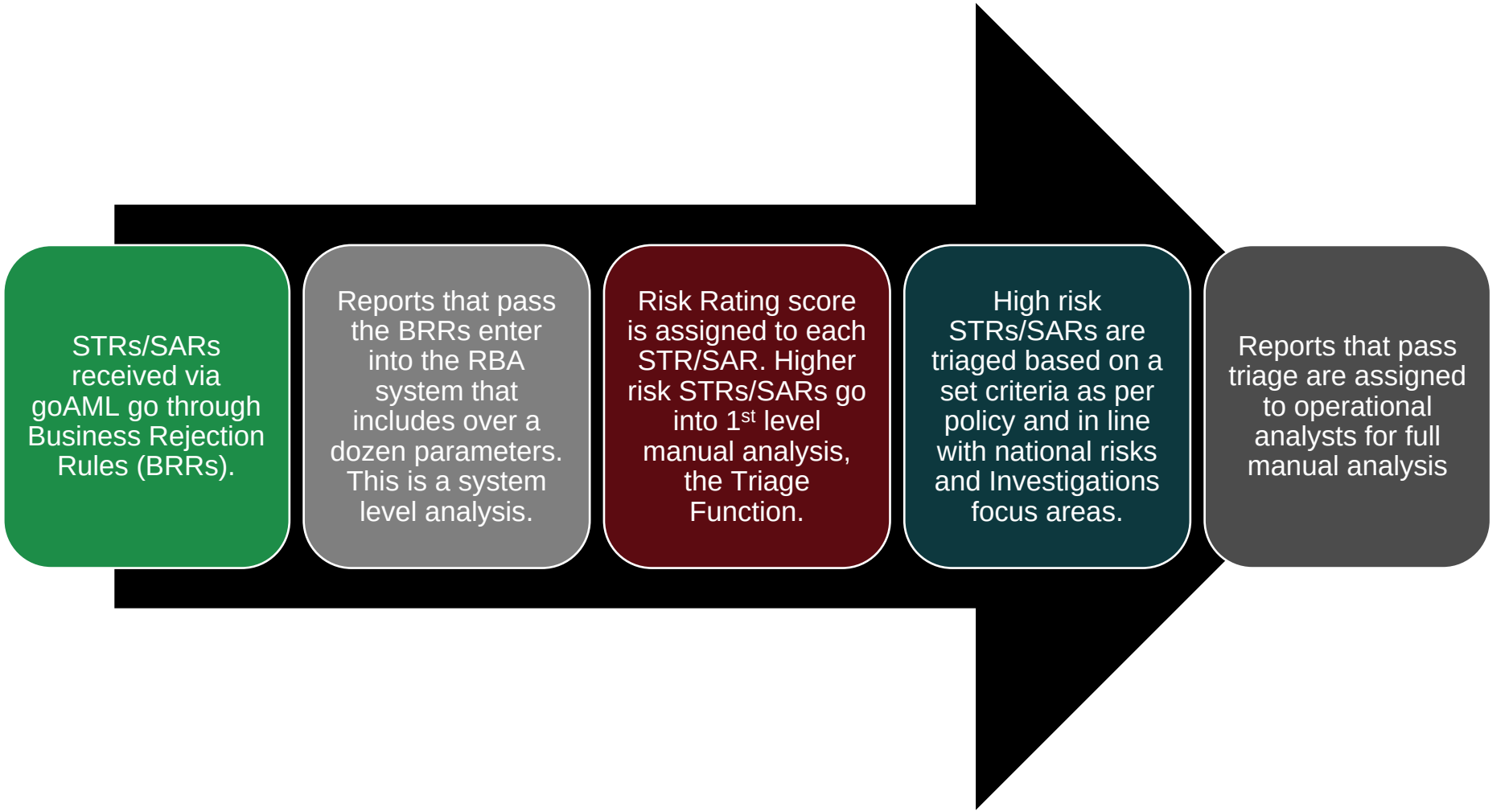
وحدة المعلومات المالية
Financial Intelligence Unit

Financial Intelligence Unit

STR/SARs and PF Specific Red flags

STR Lifecycle

STR Lifecycle



PF Specific Redflags

Red flags and goAML RFRs

- Red flags are common signs of suspicion that could mean that the transaction or activity might be part of PF.
- In goAML, Red flags are translated into Reasons For Reporting (RFRs)
- RFRs are made available to be linked to raised STRs, SARs and other report types.

Red flags and goAML RFRs

- PF - Transaction involves sale, shipment, or export of dual use goods incompatible with the technical level of the country to which it is being shipped.
- PF - Trade finance transaction(s) involving shipment route through country with weak export control laws or weak enforcement of export control laws.
- PF - The person or entity preparing a shipment lists a freight forwarding firm as the product’s final destination. Possible TBML
- PF - Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.
- PF - Customer or transaction is suspected of being linked (directly or indirectly) to IRAN’s nuclear weapons program.

Red flags and goAML RFRs, Cont.

- PF - Customer or transaction is suspected of being linked (directly or indirectly) to DPRK's nuclear-related, WMD-related, or ballistic missiles weapons program.
- PF - Based on the documentation obtained in the transaction, the declared value of the shipment is obviously under-valued vis-à-vis the shipping cost. (Possible TBML)
- PF - A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- PF - 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. Possible TBML
- PF – A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.

STR/SAR Dos

STR/SAR Best Practices

- Include a detail write up of the suspicions. Be detailed.
- Include the person/entity that you are reporting.
- Include all major counterparties.
- Explain why the transaction(s)/Activities are suspicious.
- Explain in detail what was done at the RE end and how the decision to raise the report was reached.
- Include details on the suspected transactions/amounts and the turnover of the account since inception.
- Make sure that all relevant documentation is attached to the report.

وحدة المعلومات المالية
Financial Intelligence Unit

Thank You