مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON RISKS RELATED TO PROLIFERATION FINANCE

11 September 2025

AGENDA

1. Purpose, Applicability and Legal Basis
2. Proliferation Financing and Proliferation Risk
3. Assessing and Mitigating Proliferation Financing Risks
4. Export Controls
5. Risk Indicators and Red Flags
6. Other topics and Q&A

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Purpose and Applicability of the Guidance

Purpose

- This Guidance does **NOT** constitute new regulation and does **NOT** introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- LFIs are expected to demonstrate compliance with requirements of this Guidance within one month from its coming into effect.

Applicability

This Guidance document applies to **all natural or legal persons that are licensed and/or supervised by the CBUAE** in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers;; and
- Insurance companies, agencies and brokers.

Legal Basis

- **Federal Decree Law No. 20 of 2018** on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended ("AML-CFT Law").

- **Cabinet Decision No. (10) of 2019** concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision") and its amendments.

- **Cabinet Decision No. (74) of 2020** Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments.

- **Cabinet Resolution No. (50) of 2020** concerning the control list annexed to Federal Law No. 13 for 2007 relating to commodities subject to import and export control.

- **Federal Decree Law No. (43) of 2021** on the commodities subject to non-proliferation.

- Notice No.: **CBUAE/BIS/2023/5960**, which mandates all LFIs to take steps to identify, assess, understand, and mitigate PF risks on an institutional level.

Proliferation Financing and Proliferation Financing Risks

Understanding Proliferation Financing

- Proliferation Financing ("PF") is the provision of financial services for the transfer and export of **nuclear, chemical, radiological, or biological weapons, and their means of delivery**. It involves, in particular, the financing of trade in proliferation sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation.

- For a country, inherent risk may exist due to close links with designated persons and entities under the DPRK and Iran PF-TFS regimes, or level of production of dual use goods or goods subject to export controls in the country, and trade patterns of such products, as well as loopholes in regulations aimed at the implementation of the of the relevant United Nations Security Council Resolutions (UNSCRs)

PF-related funding might occur at several stages and by various means, including through **raising, moving, and using funds**.

Understanding Risks Related to Proliferation Financing

The FATF defines PF risk as a function of three factors: threat, vulnerability, and consequence:

- **Threat** refers to a person or group of people, object, or activity with the potential to cause harm to, for example, the state, society, the economy, or the international order, including persons or entities designated under PF-related targeted financial sanctions ("TFS") ("PF-TFS"), their facilitators, their funds, as well as past, present, or future PF activities.

- **Vulnerability** refers to something that can be exploited by a threat or that may support or facilitate the breach, non-implementation, or evasion of PF-TFS.

- **Consequence** refers to the impact or harm that PF may cause, including the effect of the underlying proliferation activity on financial systems and institutions as well as the economy and society more generally .

Understanding Risks Related to Proliferation Financing (cont.)

To understand and mitigate PF risk, licenses financial institutions ("LFIs") should:

First

- Identify the extent to which state and non-state actors attempt to abuse their institutions to procure or raise funds for the procurement or development of WMD and the corresponding systems of delivery.

Second

- Assess the policies, procedures, and controls in place to counteract those threats and undertake remedial actions where they identify gaps or weaknesses in the design or operating effectiveness of their CPF program.

Third

- Continually monitor for emerging risks associated with PF, identifying trends, new methods used, and actors involved in potential PF activity, and should monitor for changes in applicable regulations and typologies so as to update and adjust their CPF programs accordingly.

Threats Related to Proliferation Financing (1/2)

PF threats and related sources of funding mainly derive from three categories:

- **Financial products directly related to trade in PF-sensitive goods.** The main threats derive from trade finance-related financing, the use or misuse of financial products and services, and trades related to persons or entities subject to United Nations Security Council ("UNSC") Resolutions ("UNSCRs").

- **Revenue-raising activities** may include the use of UAE-based front companies to raise revenue for sale of oil and petroleum-based products, cross-border smuggling of cash, gold or other high value goods to support state PF activities, real estate industry and/or related trades owned or operated by or on behalf of persons or entities subject to UNSCRs, cybercrime, restaurants or small to medium businesses which are largely cash-based businesses, wildlife trafficking, and drug trafficking.

- **Financial and corporate structures** to support movement of finances and cash may also be sources of PF, including the use of cryptocurrencies, use of local branches of banks and financial institutions based in countries of PF concern, use of hawala or bartering systems of value transfer, ease of use of front companies and shell corporations, use of Money Services Businesses for cash transfers for procurement of goods, and use of professional intermediaries and firms to mask end users.

Threats Related to Proliferation Financing (2/2)

PF threats can be posed by state and non-state actors. Under the FATF international standards, PF threats and CPF requirements are provided under the following UNSCRs:

- UNSCR 1540 (2004), regarding **non-state actors**;
- UNCSRs 1718 (2006), 2087 (2013), 2094 (2013). and 2270 (2016), regarding **the Democratic People's Republic of North Korea ("DPRK" or "North Korea")**; and
- UNCSR 2231 (2015), regarding the **Islamic Republic of Iran ("Iran").**

On 18 October 2023, the FATF communicated to all member countries that UNSCR 2231 (2015) related to Iran has ceased to apply, which means FATF Rec. 7 no longer requires countries to apply TFS to individuals and entities designated under said Resolution, and FATF Rec. 1 no longer requires countries to assess and mitigate risks related to individuals and entities subject to said Resolution as they related to the breach, non-implementation and evasion of PF-TFS.

FATF Report, June 2025: Complex Proliferation Financing and Sanctions Evasion Schemes
"Many countries still identify Iran and the Russian Federation as current PF threats even though they are not subject to UN proliferation related sanctions or covered under the FATF's definition of PF risk."

Vulnerabilities Related to Proliferation Financing (1/2)

Trade Finance	Trade-based money laundering ("TBML") and other forms of trade-based illicit finance involve the manipulation of trade transactions to disguise the true nature of the underlying financial activity and/or the identities of trade participants
Correspondent Banking	In the PF context, risks associated with facilitating international wires, check clearing, or providing trade facilities for dual-use, sensitive, or restricted goods underscore the importance of customer due diligence ("CDD")/know-your-customer ("KYC") measures, including the application of CDD/KYC as well as specific and enhanced due diligence ("EDD") measures, as appropriate, to respondent institutions.
Registered Hawala Providers (RHPs).	▪ RHPs may service jurisdictions or customer segments (or "end-users") that may present heighted PF risks. Moreover, similar to **money value transfer services ("MVTS")** and exchange houses, RHP are considered high-risk despite the relatively small size of the sub-sector and should therefore be subject to enhanced procedures and controls as laid out in this Guidance and in the CBUAE's Guidance for Registered Hawala Providers and Licensed Financial Institutions Providing Services to Registered Hawala Providers. ▪ **Unlicensed or unregistered Hawala Providers (UHPs).** Actors involved in PF may use UHPs to obscure the origins, destinations, and characteristics and details surrounding their transactions, as they provide an attractive vehicle for the transfer of illicit funds to high-risk PF jurisdictions, or for the purchase and payment of dual-use, sensitive, or restricted goods
Virtual Asset Service Providers (VASPs)	Illicit actors are also increasingly exploiting VASPs and using VAs to transfer value and hide the identity of proliferation actors. Illicit actors can exploit VASPs based in jurisdictions with little or no regulatory oversight to provide products to designated persons and entities.
Offshore Accounts	Proliferators and their networks may engage in cross-jurisdictional arbitrage and exploit regulatory gaps and AML/CFT/CPF deficiencies within specific financial sectors holding offshore accounts, to transfer funds under the guise of legitimate businesses to procure WMDs or fund the procurement of WMDs.

Vulnerabilities Related to Proliferation Financing (2/2)

Free Trade Zones	Commercial Free Zones ("CFZs") which offer duty-free importation of raw materials, machinery, parts, and equipment may be abused PF actors.
Insurance and Reinsurance	Various methods of abusing the insurance sector exist, including by acquiring insurance or reinsurance policies for fictitious vessels, **providing coverage for shipments** involving high-risk goods, such as dual-use items, obscuring the true contents of an insured vessel, or falsifying information related to goods, shipments, or their intended use.
Real estate	Real estate agents and brokers, may facilitate PF schemes through their involvement in property transactions which can involve substantial capital flows and asset transfers that can be exploited for PF activities. LFIs involved in financing real estate transactions or providing mortgage services are at risk of inadvertently facilitating PF through their indirect involvement via loans, credits, or other financial services linked to real estate.
Dealers in Precious Metals and Stones (DPMS)	Are susceptible of being used in international trade transactions to obfuscate the BOs or as means of payment in order to fund the procurement or procure WMDs, by State actors, particularly DPRK, and non-State actors, as highlighted by the UN Panel of Experts in 2019. LFIs providing services to DPMS or financing precious metals and stones ("PMS") transactions might be unwittingly involved in PF activity by facilitating trade finance transactions or servicing customers dealing with these high-value goods

Assessing and Mitigating Proliferation Financing Risks

Assessing and Mitigating Proliferation Financing Risks

The **FATF** plays an important role in assessing countries' technical compliance with and effective implementation of targeted financial sanctions pursuant to UNSCRs relating to the prevention, suppression, and disruption of proliferation of WMD and its financing. The following FATF Recommendations, Immediate Outcomes, and Guidance pertain to CPF:

- *Recommendation 1*: Requires stakeholders to identify, assess, understand and mitigate PF risk.
- *Recommendation 2*: Requires countries to adopt risk-based policies to combat illicit financing threats.
- *Recommendation 7*: requires countries to implement TFS relating to PF.
- *Immediate Outcome 11*: Persons and entities designated by the UNSCRs on proliferation of WMD must be identified, deprived of resources, and prevented from using assets derived from PF.

- *FATF 2021 Guidance on Proliferation Financing Risk Assessment.*
- *FATF 2018 Guidance on Counter Proliferation Finance.*
- *FATF 2008 Proliferation Financing Report.*

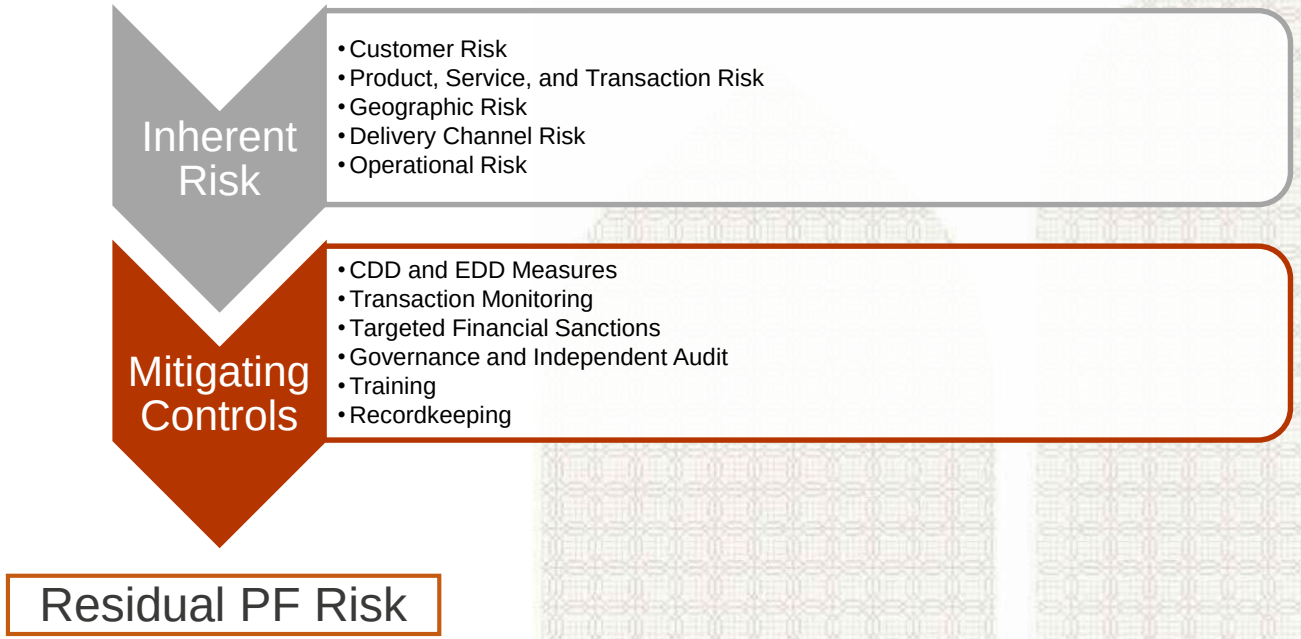
Assessing and Mitigating Proliferation Financing Risks

The **UAE legal and regulatory framework** counters PF through the implementation of targeted financial sanctions related to PF, export controls, and AML/CFT preventive and detective measures that assist public authorities and private sector entities in preventing, suppressing, and disrupting the proliferation of WMD and its financing.

- **Federal Decree Law No. (20) of 2018, Article 16.e.1**: FIs and DNFBPs shall undertake "Prompt application of the directives when issued by the competent authorities in the state for implementing the decisions issued by the UNSC.
- **Federal Decree Law No. (20) of 2018, Article 28**: Provides for prison and fine penalties for violators of Chapter 7 of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of WMD.
- **UAE Cabinet Decision No. (74) of 2020**: Concerning the implementation of UNSCRs on the suppression and combating of terrorism, terrorist financing, and countering the proliferation of WMD.
- **Cabinet Resolution No. (50) of 2020**: Contains the list of strategic and dual-use goods controlled under UAE law.
- **Federal Decree Law No. (43) of 2021**: Concerns commodities subject to non-proliferation and provides for restriction of certain commodities and the issuance of permits to trade in such items.

Institutional Proliferation Financing Risk Assessment

Proliferation financing risk assessment consists of identifying the institution's inherent PF risks based on the LFI's specific characteristics, business model, and activities; reviewing the design and operational effectiveness of an LFI's control framework to manage these risks; and determining the residual risk that remains after an LFI's controls are applied to its inherent risk.



Institutional Proliferation Financing Risk Assessment

LFIs are expected to evaluate, at a minimum, the differing levels of risk associated with their customers, products and services, delivery channels, geographic locations and markets.

Risk Factor	Description
Customers	An LFI's customer risk is based on the characteristics of its customer base, including the concentration of customers in risk-rated segments, customers' industries, professions, and entity type, and risk ratings of beneficial owners and other related parties, among other factors.
Products and Services	Product and service risk derives from the range of products and services that an LFI offers its customers and whether those products and services have characteristics that present elevated illicit finance risk.
Delivery Channels	Delivery channel risk stems from the extent to which an LFI's methods of account origination/customer onboarding, account servicing, and transaction facilitation limit its understanding of its customers' identities, activities, and counterparties.
Geographies	Geographic risk stems from an LFI's exposure—through its operating locations (including those of any global affiliates and branches located outside of the UAE), customer base, and transactions—to regions and jurisdictions that present an elevated degree of illicit finance risk.
Operating Structure	Operational risk refers to the probability of loss and disruptions to business that stem from ineffective or failed internal processes, people, or systems or from external events.

Proliferation Finance Risk Assessments and Risk-Based Approach

To implement an effective PF risk assessment, an LFI should have a well-developed risk assessment methodology that documents all the steps of the risk assessment process and the rationale that supports the PF risk assessment, such as reasoning behind chosen risk factors, scoring criteria, and instances when the LFI has chosen to deviate from standard practices. Although there is no standard risk assessment methodology, the PF risk assessment should consider the following **aspects of an effective program in connection with PF risks**:

- Use of technology to detect sanctions evasion behavior.
- Incorporating PF-specific information in the CDD process.
- Including PF risk in correspondent banking risk-ratings and EDD.
- Training to the FI's leadership and staff at all levels on PF-related issues.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Assessing Proliferation Financing Inherent Risks

Assessing Customer Risk

Individuals and entities already designated for their involvement in PF activities clearly present prohibitive risks to LFIs, but LFIs should also be **aware of the risks** of providing financial services to **individuals that are associated with designated persons** and to entities that are owned or controlled by sanctioned parties. Published case studies suggest that **the following customer types may present higher levels of PF risk**:

- Parties with links to countries of PF concern.
- Producers of dual-use goods.
- Small and medium-sized trading companies.
- Customers who use personal accounts for trade or business-related transactions.
- Customers who conduct cash-based businesses and are connected with high-risk jurisdictions for TF/PF.
- Shell and front companies.
- Newly incorporated entities with no known background/history.
- Shipping and logistics companies.
- Entities operating in the maritime sector.
- Academic and research institutions.
- DNFBPs, particularly TCSPs and DPMSs.
- VASPs.

Assessing Product, Service and Transaction Risk

LFIs should be cognizant of those **product and services that pose an elevated risk of abuse for PF** and should assess the risk that products and services they offer may be used to obtain funding or financing for WMD program activities or obtain dual-use or proliferation sensitive goods or services critical to the programs. LFIs should place special focus, among others, on :

- Traditional/documentary/open account trade finance.
- Cross-border wires, including those related to trade and those that may be related to the sending of proceeds of criminal activity to intermediary countries.
- Correspondent banking services.
- Products and services related to VA.

Certain trade finance transactions implicating controlled goods or technology present elevated PF risks for LFIs because these transactions are often **complex** in ways that allow individuals and entities to mask their intentions or underlying illicit activities.

Assessing Geographic Risk

Although only a relatively small number of countries have developed illicit WMD programs, activities related to these programs can span across the globe due to the volume and transnational nature of international shipping and trade, flexible trade finance agreements (e.g., open-trade accounts), and correspondent and nested banking relationships.

- Countries led by governments that are known or strongly suspected to be developing WMD present the highest geographical risk for FIs, particularly where these countries have been subject to UNSCR sanctions programs (i.e., North Korea).

- Geographic risk is not restricted to proliferating countries themselves. Countries and terrorist groups rely on transnational connections to procure illicit goods and services. For instance, North Korea relies on extensive corporate networks hosted in China, Hong Kong, Singapore, and Malaysia; in China, related companies are especially active in Liaoning and Jilin provinces.

The UAE lies directly across the Persian/Arabian Gulf from Iran and is a significant partner for international trade, **increasing** the UAE's potential exposure to sanctioned persons or entities in the region as well as to international trade and financial flows that carry heightened PF risks.

Assessing Delivery Channel Risk

Delivery channel risk stems from the extent to which an LFI's methods of account origination, account servicing, and transaction facilitation limit its understanding of its customers' identities, activities, and counterparties. The following are key drivers of inherent PF delivery channel risk:

- Use of non-face-to-face channels.
- Proportion of unsolicited (e.g., walk-in) customers.
- Reliance on delivery by or through a third party.
- Near-instantaneous or irrevocable settlement or processing (also a driver of product and service risk).

LFIs should be **cognizant of delivery channels that pose an elevated risk of abuse for PF** and should assess the risk that delivery channels can be used to obtain funding or financing for WMD program activities or for obtaining dual-use or proliferation sensitive goods or services critical to the programs.

Assessing Operational Risk

Operational risk encompasses risks of loss and disruptions to business that stem from ineffective or failed internal processes, people, or systems or from external events and is a function of the stability of an institution's compliance staff, systems, and policies. The following are **key drivers of operational risk**:

- Inadequate or fluctuating staffing levels in key CPF control functions.
- Material changes in the size or composition of the customer base.
- Fluctuations in sanctions screening, customer risk rating, and other technological systems or models used to support CPF compliance.
- The emergence of backlogs of transaction monitoring alerts or CDD/KYC refreshes.
- The occurrence of PF-related internal or external risk events, including material compliance breaches and changes to the risk or regulatory environment.
- Lower levels of understanding and application of CPF controls amongst employees, due to lack of training and familiarization with PF red flags and CPF regulatory requirements.

Assessing Proliferation Financing Controls

Counter Proliferation Financing (CPF) Controls

Effective risk mitigation is critical to protecting the LFI, complying with its legal obligations, and meeting supervisory expectations. LFIs should establish policies, procedures, and processes to understand their risk and take effective, risk-based steps to protect themselves from abuse and from illicit actors and transactions. The following list shows the fundamental elements of an effective mitigating control environment:

- CDD and EDD Measures.
- Transaction Monitoring and Suspicious Transaction/Activity Reporting.
- Targeted Financial Sanctions Obligations.
- Governance and Independent Audit.
- Training.
- Recordkeeping.

These CPF controls should be integrated into the LFI's larger AML/CFT program and supported with appropriate governance and training.

Establishing a Customer Risk Profile that Incorporates PF Risks

LFIs are required to understand the nature of the customer's business and the nature and purpose of the LFI's relationship with the customer, including the expected transactions/activities the customer will do using the LFI's products or services.

LFIs should consider various PF risk factors when assigning customer risk ratings, such as:
Customer-specific attributes
Transactional behavior
Red flags and risk indicators
External factors

LFIs methodology to assess PF risk should include the following:
Risk categories
Scoring system
Risk rating scale

Customer's industry codes (HS Codes – Harmonized System Codes) can allow targeted approaches to specific customers: PF-related questions, such as the specific technology or equipment the customer is manufacturing or trading should be asked to determine whether the customer is exposed to heightened PF risks.

Transaction Monitoring and Suspicious Transaction Reporting

LFIs must monitor activity by all customers to identify behavior that is potentially suspicious and that may need to be the subject of an STR or SAR. On a risk basis, LFIs should embed PF-specific indicators, typologies, and scenarios into their transaction monitoring systems to identify red flags, such as:

- Unusual patterns of transactions, such as round-tripping or layering;
- Transactions involving high-risk jurisdictions or individuals;
- Transactions involving **dual-use goods or technology**;
- Transactions involving front or shell companies;
- Transactions involving cash or non-face-to-face transactions;
- **Transactions involving unusual or non-commercial routes or channels**;
- Transactions that are inconsistent with the customer's business profile;
- Transactions that are inconsistent with expected transaction patterns;
- **Transactions associated with suspicious IP addresses or IP addresses.**

LFIs must file a **STR** or **SAR** when they have reasonable grounds to suspect that a transaction, attempted transaction, or 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.

Targeted Financial Sanctions Obligations

- The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the competent authorities of the UAE for implementing the decisions issued by the UNSC under Chapter VII of the Charter of the United Nations.
- Under Article 21 of the AML-CFT Resolution No. (74) of 2020, LFIs are required to have suitable risk management systems and take sufficient measures to identify whether a customer, or the beneficial owner of a customer, has been added to an international sanctions list or the Local List.
- LFIs are required to conduct screening prior to onboarding and on an ongoing basis, as discussed under section 3.4.1 above.

As a best practice, LFIs should maintain an internal watchlist of parties that are related to sanctioned persons or entities or that pose elevated risk to the LFI for other illicit finance-related reasons.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Targeted Financial Sanctions Obligations: Confirmed Matches

If an LFI identifies a confirmed match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List is identified, LFIs are required to take the following actions:

- Implement all necessary measures without delay as outlined in Article 15 of Cabinet Resolution No. (74) of 2020, to include **freezing without delay**, refraining from offering any funds or other assets and services, and **reporting freezing measures** to the EOCN and CBUAE; and
- If the confirmed match is a potential customer, reject the transaction immediately and report the case.

CABINET DECISION NO 74/2020: **Relevant UNSCRs** means all current and future UN Security Council resolutions relating to the suppression and combating of terrorism, terrorist financing and **proliferation of weapons of mass destruction and its financing**, including but not limited to Resolutions 1267 (1999), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.

CABINET DECISION NO 74/2020: defines **Sanctions List** as a list containing the names of individuals and organizations linked to **terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing**, and that are subject to **sanctions imposed as per UNSCRs and decisions of the Sanctions Committee**, along with information related to such persons and reasons for their listing.

Targeted Financial Sanctions Obligations: Partial Name Matches

If an LFI identifies a partial name match of an individual, entity, or group to the key identifiers published in the Sanctions List is identified, LFIs should take the following actions:

- **Cross-check** the identifiers published on the relevant sanctions list with the LFI's internal customer, beneficial ownership, and other data as well as external sources where appropriate to determine whether the partial name match is a confirmed match or can be waived as a false positive;
- If the **LFI is unable to determine** whether the partial name match is a confirmed match or a false positive, the **LFI should suspend any transaction and report the case** under Partial Name Match Report ("PNMR") through the goAML platform to the EOCN and the CBUAE and uphold the suspension measures until a response is received from the EOCN on the status of the partial name match.

LFIs are expected to submit a PNMR through the goAML platform within five business days of implementing the suspension measures. LFIs should ensure that all necessary information and documents regarding the potential match are submitted with the PNMR.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Governance and Independent Audit

- The specific preventive measures discussed above should take place within, and be supported by, a comprehensive AML/CFT program that is proportionate to the risks the LFI faces and organized in accordance with the "**three lines of defense**" model.
- All three lines of defense should report up to and have the active support and oversight of the LFI's **senior management**,
- Management Information and Reports related to PF alerts and internal investigations should be provided to senior management to enhance their understanding of the severity or scale of PF risks to the institution.

CPF Training and Record Keeping

Training

- The CPF training program should be conducted to ensure employees are aware of the risks related to PF, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls.
- Training should be **tailored and customized** to the LFI's risk and the nature of its operations and should be clearly documented in the LFI's CPF compliance program and associated training policies, procedures, plans, materials, and attendance records.

Record Keeping

- LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions.
- Records should be sufficient to permit reconstruction of individual transactions .
- LFIs should make the records available to the competent authorities immediately upon request.
- All records should be **retained for at least five (5) years** from the date of completion of the transaction or termination of the business relationship with the customer.

Export Controls

Export Controls

- While sanctions themselves do sometimes include specific technology or arms related restrictions, **export controls are typically administered through authorities** other than sanctions authorities.
- They are designed to **control access to sensitive technologies and items** that may have military application or the potential for dual-use, and implicate LFIs to the extent that they prohibit the financing of prohibited exports.
- LFIs should be familiar with the regulatory framework and international standards related to export controls associated with CPF. Among others, LFIs should be acquainted with the following:

National Export Control Laws	• Executive Office for Control and Non-Proliferation (EOCN) • Ministry of Defense (MOD) • Federal Authority for Nuclear Regulation ("FANR") • Federal Authority of Identity, Citizenship, Customs and Port Security ("ICP") • Security Industry Regulatory Agency ("SIRA")
International Export Control Regimes	• Wassenaar Arrangement • Nuclear Suppliers Group • Australia Group • Missile Technology Control Regime
UN Security Council Resolutions	• UNSCR 1540 (2004)

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Dual-Use or Controlled Goods

- When processing financial transactions related to trade and dual-use goods, LFIs are required to **screen against** the UAE Control List pursuant to Cabinet Resolution No. (50) of 2020 for potential matches and follow the steps set forth in the EOCN's *Guidance on Counter Proliferation Financing for FIs, DNFBPs and VASPs*, section 6.

- Lists of controlled chemical and non-chemical goods, which includes dual-use goods associated with the proliferation of WMDs, can be found on the EOCN's **website**.

Risk Indicators and Red Flags

Risk Indicators and Red Flags

EOCN PF Risk Factors Indicators: Customer Risk

During onboarding, a customer refuses or provides vague or incomplete information about their proposed trading activities;

A customer or its associated persons appears in sanctioned lists or negative news;

A customer is a person connected with a country of proliferation or diversion concern;

A customer deals with Dual-Use goods, goods subject to export control 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;

A customer affiliated with a university or research institution is involved in the trading of Dual-Use goods or goods subject to export control;

A customer's activity does not match the customer's business profile, or end-user information does not match the end-user's business profile; and

A new customer requests a letter of credit transaction while awaiting approval of new account.

Risk Indicators and Red Flags

EOCN PF Risk Factors Indicators: Transaction Risk

- 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 or domiciled in countries with weak 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;
- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies;
- 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 PF standards;
- A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally;
- Transactions are made on the basis of “ledger” arrangements that obviate the need for frequent international financial transactions;
- Occasionally, these companies will make transfers to balance these accounts;
- A customer uses a personal account to purchase industrial items that are under export control;
- Account holders conduct transactions that involve items controlled under Dual-Use or export control regimes; and
- Transactions associated with a customer’s frequent travel to or from high-risk countries associated with proliferation activities.

Risk Indicators and Red Flags

EOCN PF Risk Factors Indicators: Maritime Risk

- 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;
- The 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;
- 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;
- A shipment of goods is made in a circuitous fashion;
- A shipment of goods is inconsistent with normal geographic trade pattern;
- A shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards; and
- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons.

Risk Indicators and Red Flags

EOCN PF Risk Factors Indicators: Trade-Finance Risk

A trade finance transaction involves a shipment route through a country with weak export control laws or weak enforcement of export control laws;
A transaction involves persons or 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;
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; and
Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

Risk Indicators and Red Flags

EOCN PF Sanctions Evasion Red Flags and Typologies

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 in the UAE.
Dealings with sanctioned goods or under embargo, such as with oil or other commodities, or dual-use items.
Identifying documents 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.
Very 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.

Conclusion and Questions

Thank You