المكتب التنفيذي
للرقابة وحظر الانتشار
EXECUTIVE OFFICE FOR
CONTROL & NON-PROLIFERATION

اللجنة الوطنية لمواجهة غسل الأموال ومكافحة
تمويل الإرهاب وتمويل التنظيمات غير المشروعة
National Anti Money Laundering and Combatting Financing
of Terrorism and Financing of Illegal Organizations Committee

Proliferation Financing

National Risk Assessment

United Arab Emirates

2026

www.eocn.gov.ae

Table of Contents

Executive Summary

The United Arab Emirates (UAE) recognizes proliferation financing (PF) as a serious threat to global peace and security and has made combating financial crime a national priority. The Proliferation Financing National Risk Assessment (PF NRA) underscores the country's strong commitment to identifying PF threats and vulnerabilities that could be expoloited to support the proliferation of Weapons of Mass Destruction (WMD). Anchored in a robust legal and institutional framework, the assessment reflects the UAEs' proactive, risk-based approach to protecting its financial system and fulfilling its international obligations.

The UAE has established a strong legal, regulatory, and operational framework to implement targeted financial sanctions (TFS) and counter WMD proliferation and its financing. Competent authorities operate in close coordination to support risk identification, intelligence and financial information collection, supervision, enforcement, and international cooperation. UAE competent authorities are supported by a wide range of preventive, supervisory, and enforcement tools aimed at detecting, disrupting, and deterring PF networks and activities.

In October 2020, the Financial Action Task Force (FATF) revised Recommendation 1 and its Interpretive Note to require countries to identify, assess, understand, and mitigate risks related to PF. This includes risks associated with the breach, non-implementation, or evasion of targeted financial sanctions obligations stipulated under United Nations (UN) Security Council Resolutions (UNSCRs) relating to the prevention, suppression and disruption of proliferation of WMDs and its financing. In response, the UAE has undertaken a PF NRA to ensure a comprehensive understanding of its exposure to PF risks and to apply proportionate risk-based mitigation measures and controls.

This document provides the main outcomes of the PF NRA, as well as identifies PF-specific typologies and trends aimed at enhancing understanding of PF risks facing the UAE. Both public and private sectors are encouraged to utilize the findings from the PF NRA to develop / refine strategies, and set policies / internal procedures to prioritise the risks and allocate resources effectively.

1 The UAE PF NRA included UNSCR 1718 (DPRK) and UNSCR 1737/2231 (Iran), applicable during the time of the assessment.

National Threats

The UAE has identified PF threat actors that utilize various methods to evade sanctions imposed pursuant to UNSCRs 1718 and 1737 / 2231. The main threat actors include state-backed procurement networks and agents operating on behalf of the Democratic People's Republic of Korea (DPRK) and Iran that could misuse the UAE's financial system by conducting revenue-raising activity for PF purposes and facilitate PF-related fund transfers.

IRAN - UNSCR 2231 / 1737

- Use of Trade Finance products and services, and providing fake or fraudulent documents related to shipping, customs, or payments to facilitate transactions in procurement of PF-related goods
- Use of personal (or 3rd party) accounts to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business
- Use of UAE-based front companies operating in the oil and petrochemical sector for revenue-raising purposes
- Use of front companies and shell corporations or brokers for trade finance (for restricted, controlled, or Dual-Use Goods (DUGs)

DPRK - UNSCR 1718

- Cross-border smuggling of cash, gold or other high value (HV) goods to support state PF activities or PF networks benefiting DPRK
- Cybercrime – e.g., hacking into Virtual Assets Service Providers (VASPs) accounts to obtain value
- Use of Cryptocurrencies to avoid the formal financial system
- Use of intermediaries to mask parties to transactions and end users

National Vulnerabilities

The UAE's status as a **global financial, trade and transhipment hub**, as well as its' **geographic location**, neighboring a PF State Actor (Iran) sanctioned by the UN, elevates the PF risk level facing the country.

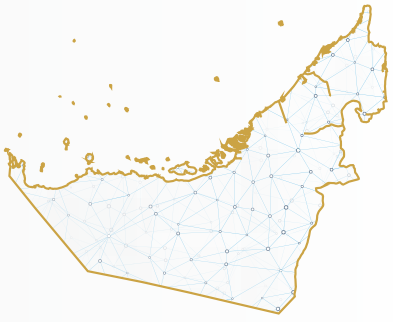
In addition, the UAE's status as a trade hub naturally leads to an **increased presence of customs brokers and freight forwarders** (often with limited due diligence measures), which further elevates the PF risk facing the country through processing proliferation-sensitive shipments.

Furthermore, the **existence of a large number of Commercial Free Zones (CFZs) and complex ownership structures** that make it difficult to identify ultimate beneficial owners (UBOs) pose a PF vulnerability, whereby PF actors could establish, through company formation services, front companies with complex ownership structures in order to either act as revenue raising fronts or to facilitate shipments of dual-use and proliferation sensitive goods.

The **recent growth of the VASPs sector** also presents an emerging PF vulnerability, particularly in the context of revenue-raising activities through PF state-sponsored hacking operations, and leveraging the sector's transaction anonymity and speed features to transfer PF-related funds.

Overall Country Risk

Considering the UAE's robust legal and operational framework in implementing TFS, extensive supervisory efforts to enforce against TFS breaches, and private sector's understanding of TFS obligations, **the risk of breaches and non-implementation of TFS is considered minimal**. However, the UAE faces an **elevated risk in relation to evasion of TFS**.



▲ **Risk of evasion of TFS** ▼ **Risk of breaches and non-implementation of TFS**

As a result, the **overall PF risk** at the country level was rated as **Medium-High**.

Scope and Methodology

The scope of the PF NRA is centered around FATF's Recommendations 1 and 7 (UNSCR 1718 – DPRK and 1737 / 2231 – Iran) and focuses strictly and only to the potential breach, non-implementation or evasion of the TFS obligations referred to in Recommendation 7.

Recommendation 7's obligations apply to UNSCRs that call for implementation of TFS relating to the prevention, suppression and disruption of proliferation of WMDs and its' financing. Recommendation 7 further requires countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of (a) any person or entity designated by the UN, (b) persons and entities acting on their behalf or at their direction, and (c) those owned or controlled by them.

The PF NRA was developed utilizing a hybrid methodology, built on resources published from international bodies and expert houses, as well as typologies identified by UAE national authorities, to tailor the risk assessment based on the UAE context in terms of PF threats and vulnerabilities.

The methodology analyzed threat and vulnerability factors to arrive at inherent risk, following which mitigating measures and control factors were taken into consideration to arrive at the residual risk.

The type of information and data collected for the PF NRA compromised both qualitative and quantitative data, including surveys, interviews, case studies, international reports, and open-source information.

The PF NRA used a rating scale ranging from Low to High as defined in the table below:

Risk Rating	Definition
Low	The risk associated with the activity, process, or system is **exceptionally minimal**. There are few or no potential negative consequences, and the likelihood of adverse events occurring is extremely Low.
Medium-Low	The risk associated with the activity, process, or system poses relatively **little to moderate risk**. While there could be some potential negative consequences, they are unlikely to occur frequently, and the impact is generally limited.
Medium	The risk associated with the activity, process, or system is **moderate**. There are notable potential negative consequences, and they could occur occasionally under normal operating conditions.
Medium-High	The risk associated with the activity, process, or system poses **significant risk**. There are substantial potential negative consequences, and they are likely to occur regularly or frequently without intervention.
High	The risk associated with the risk associated with the activity, process, or system is **exceptionally elevated**. There are severe potential negative consequences, and they are almost certain to occur without effective controls or mitigation measures in place.

Threats

Threats are defined as "legal persons/entities, objects or activities that have the potential to cause PF risk". In this document, "Threats" are focused on threat activities (factors) as these are broader than focusing only on designated individuals or entities listed by the United Nations Security Council under PF-related UNSCRs.

The threat factors discussed below are applicable to both mainland and Financial Free Zone (FFZs) sectors.

DPRK - UNSCR 1718

The main threats posed by DPRK is through PF actors' misuse of the virtual asset sector for revenue-raising purposes and moving funds to finance and support DRPK's PF programs. The DPRK regime specifically relies on cybercrime through state-sponsored hacking groups to access virtual assets, and utilizes intermediaries and middlemen to transfer PF-related funds. Another threat typology is utilization of DPRK diplomats and intermediaries for cross-border smuggling of cash, gold, or other high value goods.

The PF NRA identified the below main threats related to DPRK actors:

Cross-border smuggling of cash, gold or other high value (HV) goods to support state PF activities or PF networks benefiting DPRK.

Case Study

A bank identified trade finance transactions pertaining to shipment of luxury goods, ostensibly meant for diplomatic staff of the DPRK based in Country X. The shipments were disguised as legitimate goods meant for the ultimate consumption of diplomatic staff of the DPRK in Country X. However, freight and shipping documentation indicated that the luxury goods were likely headed for the ports of the DPRK either through mid-sea ship transfers and/or through freight forwarding from third country ports.

Cybercrime – e.g., hacking into accounts to obtain value, largely used by the DPRK

Case Study

Republic of Korea (South Korea) authorities estimated that State-sponsored DPRK cyberthreat actors had stolen virtual assets worth around $1.2 billion globally since 2017, including about $630 million in 2022 alone. A cybersecurity firm assessed that in 2022, DPRK cybercrime had yielded cyber currencies worth over $1 billion (at the time of theft), which is more than double the total proceeds in 2021 (the variation in recent cryptocurrency values might have affected the USD equivalency of these amounts).

Reference: UN Panel of Experts Report to President UNSC, March 2023, S/171/2023 para 160

Use of Cryptocurrencies to avoid the formal financial system

Case Study

An intermediary on behalf of the DPRK used an unwitting UAE-based resident to convert crypto to fiat (AED) using an Over the Counter (OTC) service to fund the purchase of a military grade vehicle.

Use of intermediaries to mask parties to transactions and end users

Case Study

The DPRK regime employed a middleman to act as an intermediary to purchase and deliver a high-end military vehicle to the DPRK. The intermediary approached a locally regulated armoring company based in the UAE, misrepresented the ultimate beneficiary and destination, and attempted to circumvent export restrictions through a change in beneficial ownership after being informed by authorities that the shipment of the armored vehicle was restricted.

Iran - UNSCR 1737 / 2231

Iranian PF networks utilize different typologies than DPRK. Specifically, threats linked to Iranian PF networks mainly stem from their use of trade finance products and other money value transfer and hawala services to procure proliferation-sensitive goods. Illicit actors have been found to use fraudulent trade and shipping documentation and use of personal or 3rd party accounts to purchase industrial items that are under export control.

In addition, threats emanate from establishing UAE-based front companies to raise revenue for the sale of oil and petroleum-based products and for shipping DUGs to Iran.

The PF NRA identified the below main threats related to Iranian actors:

Use of Trade Finance products and services, and providing fake or fraudulent documents related to shipping, customs, or payments to facilitate transactions in procurement of PF-related goods

Case Study

Company A, involved in the import/export of goods and materials, had mislabeled and falsified export documents related to a shipment containing devices used in the production of missiles and other WMD-related systems to hide the shipment's origin and nature with the intention of re-exporting the items to Iran. Inspection of trade documents showed that Company A had forged documents related to the value and type of goods being shipped, declaring the actual value below the fair market value, in addition to the goods being controlled under the UAE Control List.

Use of personal (or 3rd party) accounts to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business

Case Study

Company X, based in a commercial free zone, had submitted three permits to export goods listed in the UAE Control List to Iran. The documents submitted by Company X included a bill of lading and a bill of sales and purchase (BSP), which had conflicting information on the seller's information and the country of origin of the shipment.

Company X had submitted a forged bill of lading, which declared itself as the shipper, while the BSP identified the seller as another company located in Country X, and that the purported seller primarily trades in food products thus its business was not consistent with the item being shipped.

Case Study

Person Z (linked to a sanctioned entity) used the UAE as a transit point for a low-value shipment containing a sample of dual-use goods (controlled under the UAE Control List) destined for Iran. Person Z had used his own bank account, as well as those of his companies, to support the sanctioned entity.

Use of UAE-based Iranian front companies to raise revenue for sale of oil and petroleum-based products.

Case Study

STRs by banks highlighted inconsistencies between the annual income of Person D and his business activity. Investigations revealed that Person D worked as an intermediary, arranging sales contracts for Iranian oil companies in Country X to benefit sanctioned groups.

Use of front companies and shell corporations or brokers for trade finance (for restricted, controlled, or DUGs)

Case Study

Company A, based in the UAE, submitted a permit request to export an electronic item manufactured in Country B to Iran. Upon additional information requests, Company A declared the item's specifications slightly below the threshold for it to be considered as a DUG under the UAE Control List. An inspection of the shipment concluded that Company A provided a false declaration, and the actual technical specification of the item was above the dual-use threshold. Furthermore, the exporter did not hold the valid license to export the electronic item from the manufacturing country and used a general license to circumvent the export control system in Country B.

Vulnerabilities

Vulnerabilities are those conditions which can be exploited by threats or might be used in support of, or to facilitate threats. This document segregates vulnerability factors into four main categories:

- Geographic and Environmental
- Legal Persons and Arrangements
- Legal and Institutional
- Economic and Technological

Geographic and Environmental

Proximity to Iran

The UAE's close proximity to Iran presents a high vulnerability rating for exposure to Iran-related PF activity across all sectors.

Financial, Trade and Transshipment Hub

The UAE is a major financial, trade and transshipment hub. Notably, vulnerabilities might be especially high in those sectors dealing with trade finance. As with the volume of international trade, the overall financial transaction volumes make it easier to obscure the actual nature of transactions; and the identities and backgrounds of relevant parties/counterparties, if not properly scrutinized. As such and given the size and transaction volumes (specifically those involving trade), this factor poses a vulnerability to the UAE.

In addition, due to the UAE's status as a financial hub, several global VASPs have set up operations in the UAE and at an increasing pace. Due to their global operations and reach, these VASPs are exposed to unwittingly facilitating transactions for PF purposes through VASPs with lower compliance functions located abroad and hence face a high exposure.

Legal and Institutional

The UAE has a legal framework in place to combat PF and regulate transacting in controlled items. In addition, the UAE's Anti-Money Laundering Law (Federal Law No. 10 of 2025) has recently been updated to criminalize the act of PF, thereby strengthening the legal framework by requiring Reporting Entities to conduct PF institutional risk assessments and submit STRs/SARs related to PF to the Financial Intelligence Unit. This indicates that the UAE has an established and robust legal framework for combating PF, rendering limited vulnerability for all Financial Institutions (FIs) and VASPs sectors.

However, this vulnerability is slightly more among Designated Non-Financial Businesses and Professions (DNFBPs) due to weaker detection and reporting culture given their more limited capabilities, resources and PF awareness, along with recent update of PF legislation and compliance requirements.

Legal Persons and Arrangements

Lack of transparency of legal persons and legal arrangements, including UBO

The UAE has made progress toward corporate transparency, most notably through the implementation of a National Economic Register (NER). The NER makes all basic company ownership information publicly available and ultimate beneficial ownership (UBO) information accessible to law enforcement.

The UAE's ease of doing business, corporate formation, and the presence of a large number company registers increases vulnerabilities associated with lack of transparency of legal persons across virtually all sectors. Given the general typology of front companies in illicit finance, and the prevalence of general trade and import/export companies in the UAE, especially those registered in CFZs, this poses as an elevated vulnerability for the UAE.

Economic and Technological

Limited knowledge, lack of regulations of, or limited outreach related to TFS and evasion

The Executive Office for Control and Non-Proliferation has conducted numerous TFS and PF training seminars, webinars, and other awareness raising events and outreach sessions with FIs, DNFBPs, VASPs, supervisory and regulatory and other competent authorities in the past five years, with local and international leading experts in the field.

However, due to the recency of the virtual assets space and the technical nature of the underlying VA technology, limited knowledge of VAs misuse for PF evasion purposes amongst the private sector is considered a vulnerability facing the UAE.

Dual-use or controlled goods – including chemical or petrochemical industries and/or trade

UAE Customs has adopted the PLACI system (Pre-Loading Advance Cargo Information), which is a global air cargo security initiative requiring carriers and forwarders to submit detailed cargo data to authorities before loading, allowing for risk assessment to prevent illicit items (like explosives/weapons) from entering the supply chain. The PLACI system has been integrated in the National Advance Information Center systems that operate under the Federal Authority for Identity, Citizenship, Customs & Port Security.

However, due to the presence of industries such as petrochemicals and nuclear power facilities and related technologies in the UAE, and the UAE's status as a financial, trade and import/export hub, this vulnerability is elevated in the jurisdiction generally. Additionally, there are inherent difficulties in accurately detecting such items given their technical specifications, particularly by the private sector. As such, the presence of industries and the trade in such items presents an elevated vulnerability in the UAE.

Existence of CFZs/over-reliance on friendly business practices to attract foreign investment

The UAE's CFZs and Departments of Economic Development at the emirate-level were implemented and designed to facilitate company establishment and promote a business-friendly environment.

While market entry requirements in terms of AML/CFT/CPF are uniform across jurisdictions (mainland, CFZ and FFZ) and are guided by the same minimum standards, the ease of doing business in the UAE and the volume of established companies exposes the UAE to vulnerabities associated with front and shell companies that could be misused for PF purposes.

Sectoral Risk
Mainland & Financial Free Zones

Financial Institutions and Virtual Assets Service Providers

The sector that presents the highest PF risk exposure in the UAE is the **VASPs** sector, assessed as **High** in the **mainland** due to the anonymity and speed in which funds can be transferred through VASPs by PF actors to support PF activities, in addition to VASPs (particularly exchange platforms) exposure to state-sponsored hacking operations by the DPRK through the infamous Lazarus Group to raise revenue for their nuclear program. While the licensed VASPs sector in the UAE is diligently regulated and monitored, they are exposed to risks emanating from transactions with unlicensed VASPs, which operate in most cases in foreign / offshore jurisdictions. VASPs risk was assessed as **Medium-High** in the **FFZs**, mainly due to Abu Dhabi Global Market being one of the first regulators adopting VASP regulations globally (in 2018), with Dubai Financial Services Authority following in 2022.

Banks, Exchange Houses (EHs), and Registered Hawala Providers (RHPs) risk was assessed as **Medium-High** in the **mainland**.

Banks in the mainland are exposed to PF risks through trade finance products whereby PF actors could use such products to directly finance the procurement of proliferation-sensitive or DUGs. Since PF actors can mistate, misrepresent, or forge trade documents (e.g. invoices, bill of sales, customs declaration forms, etc.), banks that offer trade finance products face an elevated PF risk. Banks also face a risk through “open account” transactions whereby PF actors could use direct wire transfers to procure DUGs from suppliers. In addition, banks in the mainland service both retail and corporate customers, thereby expanding the client base type and elevating the PF risk exposure.

EHs and RHPs in the mainland are exposed to PF risk mainly through supporting traders and companies through currency exchange and cross-border money transfers (i.e., sending payments to suppliers).

Banks and **Money Service Businesses (MSBs)** risk was assessed as **Medium** in the **FFZs**.

Although banks based in the FFZs provide trade finance products and are exposed to PF risks, they face a relatively lower risk compared to mainland banks due to the fact that they predominantly provide wholesale banking services (corporate customers), handle relatively lower volumes of trade finance transactions, and are branches of global banks with well-established compliance programs.

In terms of MSBs, they are exposed to PF risk mainly through the provision of cross-border transfer to corporate clients, however, they face a relatively lower risk than mainland EHs since they have relatively limited cross-border transfers, and transfers are purely account-based (cash transactions are not permitted in the FFZs). Hawaladars are also not permitted to operate in the FFZs.

The **Maritime Insurance** sector risk was assessed as **Medium** in the **mainland**. Firms that offer maritime insurance products, such as insuring ships, vessels, and cargo, are indirectly exposed to PF risks whereby PF actors could utilize maritime insurance products to facilitate the transfer or shipment of DUGs. However, the sector faces lower PF risks relative to traditional FIs as they are non-depository in nature and the settlement conducted by them are backed by adequate documentation. In addition, cargo insurance policies are subject to additional due diligence measures by the banks as they are involved in facilitating such services as part of the trade financing process. The sector was assessed as **Medium-Low** in the **FFZs,** mainly due to the relatively limited number of firms offering maritime insurance products in the FFZs and majority being captive insurance firms focusing on reinsurance.

The **Stored Value Facilities (SVFs)** sector's risk in the **mainland** was assessed as **Medium-Low**. While SVFs provide money-transfer and remittance services through their Retail Payment Service Providers (RPSP) license, they typically cater to retail clients and merchants (SMEs) and provide services exclusively to resident retail clients (wallets are linked to national ID and local mobile phone numbers) and UAE-based merchants, thereby limiting the cross-border exposure. It's worth noting that **FFZs** do not host SVF firms.

The **Securities** sector risk was assessed as **Low** in both the **mainland** and **FFZs**. The range of products offered by securities firms have low exposure to PF risk and trade finance. In addition, securities firms do not accept cash deposits and funding of accounts is made through banks.

Designated Non-Financial Businesses and Professions

In general, the **DNFBP** sector in the **FFZs** constitute a small population of overall DNFBPs in the UAE (approximately %2), and hence the risk exposure across the sectors is relatively lower compared to mainland DNFBPs.

The **Dealers in Precious Metals and Stones (DPMS)** sector risk was assessed as **Medium** in the **mainland**. Although the DPMS sector does not have direct exposure to trade finance activities, the sector is exposed to the risk of cross-border smuggling of cash, gold, or other high-value goods (sometimes by mules) to support state PF activities or PF networks. The DPMS sector faces an elevated risk due to gold being an attractive revenue raising source for PF actors, and the active presence of bullion traders and refineries in the UAE.

Company Service Providers (CSPs) risk was assessed as **Medium** in the **mainland**. CSPs are indirectly exposed to PF risks mainly through the provision of company formation services whereby such services might be used in the formation of front or shell companies that operate as part of extended PF networks, and other corporate means to obscure ownership and the nature of a business. **Law Firms and Legal Consultants** risk was assessed as **Medium-Low** in the **mainland** due to the relatively limited number of firms that provide company formation services. Majority of the sector provides services exclusive to providing legal advise and court litigation and do not engage in company formation services.

Audit and Accounting Firms and **Real Estate Brokers** risk was assessed as **Low** in the **mainland**. These sectors face minimal PF risks since they are not involved in any trade finance activities or company formation services.

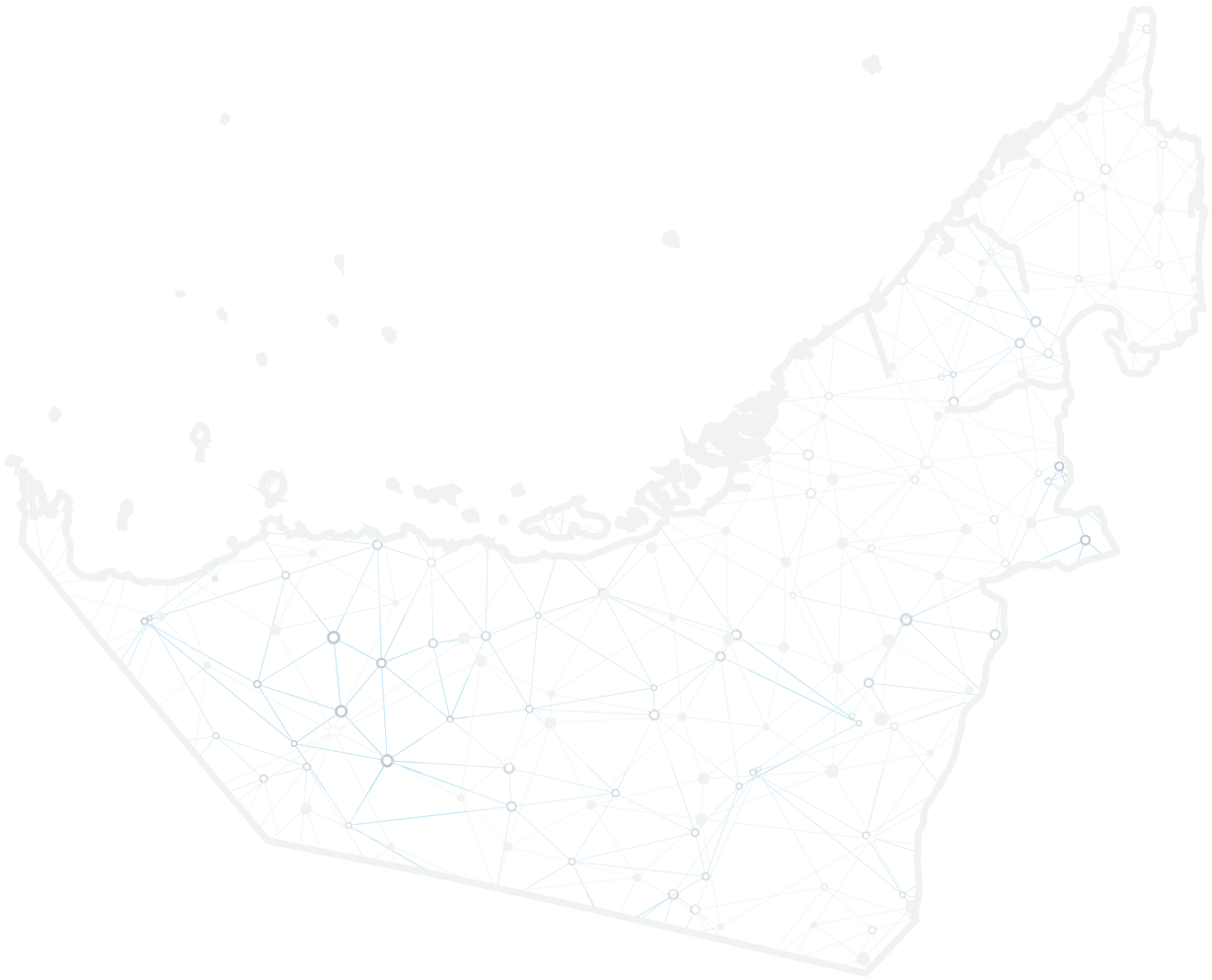
CSPs risk was rated as **Medium-Low** in **FFZs**. While CSPs in FFZs also face PF risks arising from provision of company formation and corporate structuring services, they are tightly supervised by Dubai Financial Services Authority and Abu Dhabi Global Market on AML regulations.

DPMS, Law Firms and Legal Consultants, Audit and Accounting Firms, and Real Estate Brokers risk was assessed as **Low** in the **FFZs**. In relation to DPMS, the FFZs do not host any bullion traders, refineries, or smelters and are limited to luxury jewelry stores and boutiques. The remaining sectors face negligible PF risks since their operations do not involve activities considered higher risk for PF (e.g. trade finance, cross-border transfers, and/or company formation services).

Conclusion

The UAE continues to demonstrate a strong national commitment to countering PF by maintaining a robust legal, regulatory, and operational framework aligned with international standards. While the country's position as a global financial and trade hub naturally exposes it to elevated risks—particularly relating to TFS evasion, misuse of trade finance, front companies, and vulnerabilities within emerging sectors such as virtual assets—the UAE has taken significant steps to mitigate these challenges.

The PF NRA findings reinforce the importance of sustained coordination among competent authorities, enhanced supervision, strengthened private sector compliance, and continued investment in awareness and capacity building efforts. By adopting a proactive, risk based approach, the UAE is well positioned to effectively detect, prevent, and disrupt PF related activities and safeguard the integrity of its financial system.



Annex – Definitions

Dual-Used Goods (DUGs)

refers to items that can have both civilian and military applications. Controls on dual-use items are designed to prevent the proliferation of goods or technology that can have military applications or other uses deemed by governments as having national security or other implications.

Proliferation Financing

refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Weapons of Mass Destruction (WMDs)

refers to weapons that cause harm to numerous human beings and cause threat to life and biosphere through their catastrophic consequences, such as nuclear, biological, chemical and radiological.

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).

Targeted Financial Sanctions

refers to asset freezing and prohibition from making funds or other assets or services available either directly or indirectly, for the benefit of designated individuals, entities, or groups listed in the Sanctions Lists.

Annex – Acronyms

AML	Anti Money Laundering
CFZs	Commercial Free Zones
CSPs	Company Service Providers
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
DPRK	Democratic People's Republic of Korea
DUGs	Dual-Use Goods
EHs	Exchange Houses
FATF	Financial Action Task Force
FFZs	Financial Free Zones
FIs	Financial Institutions
MSBs	Money Service Businesses
PF	Proliferation Financing
PF NRA	Proliferation Financing National Risk Assessment
RHPs	Registered Hawala Providers
SVFs	Stored Value Facilities
TFS	Targeted Financial Sanctions
UAE	United Arab Emirates
UBO	Ultimate Beneficial Owner
UN	United Nations
UNSCR	United Nations Security Council Resolution
VASPs	Virtual Asset Service Providers
WMD	Weapons of Mass Destruction