Proliferation Financing Regional Risk Assessment of GAFILAT

A Reference Guide for GAFILAT Countries



October 2026

HIGH-RISK SECTORS FOR PROLIFERATION FINANCING:

REGIONAL RISK ASSESSMENT AND REFERENCE GUIDE FOR GAFILAT COUNTRIES

October 2026

This document has been developed by GAFILAT with the support of U.S. INL Cooperation within the framework of the GAFILAT Program – "Mentoring Member States during the 5th Round of FATF MERs and FURs.

© October 2026.

Partial or total reproduction of this work is prohibited without due authorization from the Executive Secretariat of GAFILAT.

Table of Contents

Executive Summary 6

1. Introduction 9

2. Structure of the Report and Methodology 11

3. WMD Proliferation and the Role of Financing 15

4. High-Risk Sectors 30

4.1. Financial Sector 30

4.1.1. Global Risk 30

4.1.2. Regional Risk 33

4.1.3. Key Red Flags for Financial Institutions 44

4.2. Dual-Use Sector 46

4.2.1. Global Risk 46

4.2.2. Regional Risk 50

4.2.3. Key Red Flags for Illicit Procurement of Sensitive Goods 58

4.3. Maritime industry 60

4.3.1. Global Risk 60

4.3.2. Regional Risk 61

4.3.3. Key Red Flags for the Maritime Sector 65

4.4. Free Trade Zones (FTZs) 68

4.4.1. Global Risk 68

4.4.2. Regional Risk 69

4.4.3. Key Red Flags for FTZs 71

4.5. Relevant DNFBPs: Trust and Company Service Providers; Legal Professionals (Lawyers), Notaries, Accountants. 73

4.5.1. Global Risk 74

4.5.2. Regional Risk 75

4.5.3. Key Red Flags for TCSPs, Legal Professionals (Lawyers), Accountants, and Notaries 76

4.6. Relevant DNFBPs: dealers in precious metals and stones 79

4.6.1. Global Risk 79

4.6.2 Regional Risk....80
4.6.3. Summary of Red Flags for Dealers of Precious Metals and Stones....81
4.7. Virtual Asset Service Providers (VASPs)....83
4.7.1. Global Risk....83
4.7.2. Regional Risk....85
4.7.3. Summary of Red Flags for VASPs....88
5. Overall WMD Proliferation and Proliferation Financing Risk Profile of the GAFILAT Region....91
6. Policy Recommendations....97
7. Annexes....101
Annex I. Country matrices of CPF regional situation (confidential)....101
Annex II. Detailed Red Flags for High-Risk Sectors....101
Annex III. Sample interactive exercise for training purposes....101
Annex IV. List of relevant resources....101



Executive Summary

Executive Summary

1. An incident involving a weapon of mass destruction (WMD) in any part of the world will have a major impact on the entire world. No region can consider itself beyond its reach. For example, a single nuclear detonation can kill and injure many thousands of people, contaminate the environment, disrupt trade, supply chains, and financial operations far beyond the borders of a target state. Preventing financing of WMD proliferation is a critical tool in reducing the risk of the devastation a WMD event would cause. States must therefore implement appropriate measures to mitigate the risk of proliferation financing (PF) and prevent the devastating consequences of such an event.

2. This report provides an overview of the current state of preventing and combating proliferation financing in the GAFILAT region, raises awareness of the risks associated with high-risk sectors for proliferation financing, assesses regional risk exposure, and provides policy recommendations. At the core of this report is the assessment of the following high-risk sectors: the financial sector; the dual-use sector; the maritime industry (and inland waterway, including inland ports and navigable waterways); free trade zones (FTZs); trust and company service providers (TCSPs); legal professionals (lawyers), accountants, and notaries; dealers in precious metals and stones; and virtual asset service providers (VASPs). The financial sector is simultaneously the most exposed sector to proliferation financing and the one with more advanced controls. The analysis focuses on PF risks associated with implementing UN targeted financial sanctions (TFS) against DPRK and Iran, in line with the scope of FATF Recommendation 7.

3. The assessment draws on country surveys submitted by 16 GAFILAT jurisdictions, mutual evaluations conducted by GAFILAT, supplemented by FATF and GAFILAT documents, open-source resources, virtual consultations with delegations, and the regional workshop held in Santiago, Chile, in 2025.

4. The report provides granular detail on how jurisdictions address each high-risk sector. Collected data suggest uneven implementation of risk-minimizing measures across jurisdictions and sectors.

5. The region is not among the most exposed to proliferation, but that does not mean that the risks do not exist. The following factors contribute to the region's vulnerabilities: challenges remaining in some jurisdictions with implementation of TFS without delay, transit, transshipment, re-export, and brokering of sensitive goods; FTZs; uneven supervision and oversight of high-risk designated non-financial businesses and professionals (DNFBPs), the maritime sector, and VASPs; lack of comprehensive export control systems; and a false sense of security (perception of the risk as low). A sense of security may stem not only from apparent low exposure but also from the counter-proliferation financing architecture that focuses primarily on financial obliged entities and their role in checking against the lists of UN-designated entities and individuals, without fully integrating key authorities—such as Customs, maritime authorities, ports, FTZs, commercial and vessel registries, foreign trade authorities, and strategic non-financial sectors. As a broader context, many jurisdictions in the region have diplomatic relations with the DPRK and Iran, and some of them have substantive trade relations with Iran.[1]

[1] While FATF Standards do not require jurisdictions to refrain from maintaining diplomatic relations with the DPRK and Iran, FATF Recommendation 19 regarding higher-risk countries mandates enhanced measures or countermeasures against certain states, including these two.

6. Overall, legal-regulatory frameworks for TFS are strong across the region, but implementation track records are weaker.

7. The report's recommendations focus on operationalizing existing legal-regulatory frameworks; completing national PF risk assessments; closing legal gaps (discussed sector-by-sector); strengthening detection and prosecution capacity; minimizing siloing between export control authorities and financial crime prevention authorities; encouraging PF-focused risk management by all financial institutions, regardless of size; strengthening oversight over and training across FTZs, the maritime sector, high-risk DNFBPs, and VASPs; and learning from regional peers.



CHAPTER 1

Introduction

1. Introduction

8. Financing is an integral component of the proliferation of weapons of mass destruction. At every stage of the proliferation process, from raising funds to acquiring sensitive goods and technology from manufacturers or resellers and delivering them to the final destination, proliferators interact not only with the financial sector but also with a wide range of critical non-financial actors. They include manufacturers, exporters, freight forwarders, Customs brokers, port operators, ship registries, free trade zones, corporate service providers, metal traders, and VASPs.

9. The analysis of sectors most vulnerable to proliferation financing is the focus of this report. The sectors analyzed — identified through an examination of responses to the project's country surveys and international trends — include the financial sector; the dual-use sector (industries producing goods and technology that can be used for both civil and military purposes); the maritime industry; FTZs; TCSPs; legal professionals (lawyers), accountants, and notaries; dealers in precious metals and stones; and VASPs.

10. Despite its geographical distance from the main proliferant states – the DPRK and Iran – the GAFILAT region is not immune to proliferation financing risk. In fact, several factors make it vulnerable, including the presence of multiple economies with significant dual-use sectors, high-volume ports, numerous FTZs, illegal gold mining, diplomatic relations with the DPRK and Iran, and weaker oversight of VASPs, to mention a few.

11. The report serves multiple objectives. It provides a regional risk assessment, offers a manual for understanding global risks connected with high-risk sectors, and offers policy recommendations.



CHAPTER 2

Structure of the Report and Methodology

2. Structure of the Report and Methodology



2.1 Structure

12. The first section of the report starts with a high-level overview of the risks associated with the proliferation of WMD, the role of financing in WMD proliferation, key international legal instruments to combat proliferation financing, and an analysis of how the two main proliferators sanctioned by the United Nations – DPRK and Iran – operate and finance their proliferation activities.

13. The second, core section of the report focuses on high-risk sectors for proliferation financing: the financial sector, the dual-use sector, the maritime industry, FTZs, TCSPs, legal professionals (lawyers), notaries, and accountants, dealers in precious metals and stones, and VASPs. For the analysis of each sector, the report is structured into three components: 1) a global risk assessment based on the expertise of the project team, international typologies and data from reliable open sources of information; 2) a regional risk assessment based on the information provided by GAFILAT delegations and additional research when data was limited; and 3) a compilation of relevant Red Flags, drawn from the guides and documents published by FATF, relevant documents from different jurisdictions – members of the Global Network, and from specialized international organizations.

14. The final section of the report summarizes the regional risk assessment and provides policy recommendations.

15. Annex I includes country matrices that are available to GAFILAT jurisdictions for internal use and are not part of the public report. Confidential matrices are available via the secure GAFILAT portal. Additionally, Annex I includes a sample country survey that may serve as a starting point for domestic risk assessments in this area.

16. Annex II offers detailed lists of Red Flags for high-risk sectors.

17. Annex III includes a sample interactive exercise for training purposes.

18. Annex IV provides a list of relevant resources.

2.2 Methodology

19. The project relied on a five-component methodology described in the section below:

    (1) Analysis of GAFILAT reports, Mutual Evaluation Reports (MERs), FATF and FATF-style regional bodies' reports and guidances, and expert publications;
    (2) Distribution of country surveys and collation of received data into country matrices;
    (3) Virtual consultations with delegations;
    (4) Insights from GAFILAT delegations shared during an in-person regional workshop on Strengthening Latin American Efforts to Combat the Financing of the Proliferation of Weapons of Mass Destruction" held in Santiago, Chile, in September 2025;
    (5) Write-up of the report.

20. The first stage of the project involved analysis of FATF and GAFILAT reports and guidances, MERs, and expert publications with the aim of establishing a baseline assessment of the proliferation-financing threat landscape and jurisdictions' overall capacity to address financial crime. These documents allowed to analyze a general picture of the challenges posed by proliferation financing and a broader regional landscape of WMD and proliferation financing controls.

21. For a more nuanced understanding of the regional situation, more detailed information from GAFILAT jurisdictions was necessary. For that purpose, the project lead developed a comprehensive country survey. The questionnaire-based survey consisted of 17 sections and included 53 questions (See Annex I). The request for data focused on the following: legal-regulatory basis for implementing proliferation financing controls, supervisory authorities for relevant high-risk sectors, national proliferation risk assessments, sector-specific information on the dual-use sector, VASPs, shipping industry, trust and company service providers, free trade zones, diplomatic relationships, and trade with the DPRK and Iran. Delegations were also encouraged to submit relevant pieces of legislation. Out of eighteen jurisdictions, sixteen responded to the survey. They include Argentina, Bolivia, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, and Uruguay.[2] GAFILAT gratefully acknowledges the significant value of data provided via country surveys.

22. After the initial analysis of country survey responses, GAFILAT and the project lead conducted follow-up virtual consults with sixteen delegations to clarify specific questions and request additional information. The consultations provided additional valuable information critical for the analysis presented in this report.

[2] Although two countries (Costa Rica and Cuba) did not participate directly in the survey—as they are currently undergoing their mutual evaluation process within the framework of the GAFILAT 5th Round of Mutual Evaluations—these delegations provided general data that were factored into the regional analysis whenever possible.

23. Finally, in September 2025, GAFILAT organized a regional Workshop for Latin American Strengthening of the Fight Against Financing the Proliferation of Weapons of Mass Destruction in Santiago, Chile. Chile's Financial Intelligence Unit co-hosted the workshop and shared its national experience with developing a National Risk Assessment (NRA). The workshop served a dual purpose: it provided training on advanced topics in proliferation financing and offered an opportunity for further information exchange among the jurisdictions and with GAFILAT. Two international subject-matter experts – Dr. Togzhan Kassenova and Dr. Jonathan Brewer – served as lead presenters and facilitators for the workshop, alongside presentations by the various delegations and the GAFILAT Secretariat.

24. The final phase of the project consisted of drafting the report based on all data collected from the jurisdictions, the MERs, and open sources of information.

25. The regional conclusions reflect aggregated trends derived from available information and do not imply that the identified vulnerabilities, deficiencies, or risk levels are present uniformly across all jurisdictions. Findings should be interpreted with due regard for differences in legal frameworks, institutional capacities, data quality, and the stage of development of national assessments.



CHAPTER 3

WMD Proliferation and the Role of Financing

3. WMD Proliferation and the Role of Financing



3.1. Global Impact of a WMD Event

26. Proliferation of weapons of mass destruction is a global threat. Weapons of mass destruction refer to nuclear, chemical, and biological weapons. In some countries, the definition also includes radiological weapons. Any incident involving a weapon of mass destruction will have a far-reaching impact. No country in the world can consider itself fully safe from a potential WMD event.

27. Among weapons of mass destruction, nuclear weapons hold the highest destructive power. A nuclear event will have the most profound consequences, both in the immediately affected areas and beyond. Depending on the yield of the weapon used, the human toll will be from hundreds of thousands to millions of people injured and killed. The environment will be severely contaminated, and the local economy will collapse. Basic services, such as food, water supply, medical care, and law enforcement, will become unavailable, potentially leading to societal breakdown.

28. The impact of a nuclear event will not be confined to the state's borders. It will have far-reaching global consequences. Radioactive fallout will travel across national borders and reach remote locations. Supply chains and financial and economic transactions will be interrupted. Entire industries will collapse. Survivors will become refugees and enter neighboring countries.

29. If, for example, DPRK detonates a 10-kiloton nuclear weapon in an airburst over a major urban center in Latin America, the approximate number of fatalities will be more than 100,000 people, and casualties – more than 350,000 people.[3]

30. To put it in perspective, consider the impact of a nuclear exchange between India and Pakistan. Experts calculated that, in addition to immediate tens of millions of fatalities, more than 2 billion people will die of starvation in the months and years that follow as a result of the Sun-blocking soot and its impact on crop production.[4]

31. A detonation of even a single nuclear device in a major seaport will have a ripple effect across the world. A tabletop study conducted by RAND[5] simulated a nuclear terrorist attack in the port of Long Beach, California. In RAND's assessment, there would be "reasonable prospects for extended closures of all U.S. ports," which would severely impact global trade.[6]

3.2. The Role of Financing in WMD Proliferation

32. Proliferators cannot buy a ready-made weapon on the international market, but they can buy dual-use goods and technology that are useful in WMD and missile programs. Dual-use goods and technology can be used for both peaceful (civilian) and military programs. For example, a trigger spark – a small, benign-looking device – is a necessary part of a medical device called a lithotripter. A lithotripter is a noninvasive device that uses high-amplitude shock waves to break down kidney stones, bladder stones, or ureteral stones into small, passable fragments. At the same time, a trigger spark can also be used to trigger an explosion of a nuclear device. Chemical precursors are used to produce fertilizers but can also be used to produce chemical weapons. A laboratory bioreactor (fermenter) is used for producing vaccines, enzymes, and industrial biotech products. The same equipment can be repurposed to produce harmful biological agents if paired with illicitly procured materials and know-how.

33. Countries rely on dual-use goods and technology in everyday life; therefore, they cannot be banned. Instead, governments regulate trade in sensitive items through export controls and sanctions regimes. Countries with export control systems require companies to obtain licenses (permits) before trading in such goods. During the licensing process, relevant government authorities analyze that the end-use, end-users, and final destination of goods and technology are legitimate and for peaceful purposes. That way, legitimate trade in dual-use goods and technology proceeds for the benefit of societies without increasing proliferation risks. Sanctions regimes restrict trade in sensitive items with countries, entities, or individuals believed to be proliferators.

---

[3] For modelling the impact of a nuclear attack, please see NukeMap, developed by Professor Alex Wellerstein, https://nuclearsecrecy.com/nukemap/.

[4] Lili Xia, Alan Robock, Kim Scherrer, Sheryl S. Harrison, Benjamin Leon Bodirsky, Isabelle Weindl, Jonas Jägermeyr, Charles G. Bardeen, Owen B. Toon, Ryan Heneghan, "Global Food Insecurity and Famine from Reduced Crop, Marine Fishery and Livestock Production Due to Climate Disruption from Nuclear War Soot Injection," National Food. 2022 August; 3 (8): pp. 586-596.

[5] https://www.rand.org/topics/global-security.html.

[6] Charles Meade, Roger C. Molander, "Considering the Effect of a Catastrophic Nuclear Attack," RAND Corporation, Santa Monica, 2006.

34. Proliferators constantly seek to acquire dual-use goods and technology from the international market. They employ evasion techniques to evade export controls and sanctions. Some of the tactics they use are the following.
    - They use front companies and intermediaries to pose as domestic buyers of goods, so that suppliers do not seek a license (permit) from the government.
    - They order items slightly below a controlled threshold – for example, equipment that is slightly technically inferior and is not included on the list of goods requiring a license (national control list). In such cases, suppliers also do not need to seek a license (permit), and proliferators escape extra government scrutiny.
    - Proliferators can also order goods to a third destination – a non-sanctioned country with weak export and AML controls – and from there re-export sensitive items to either DPRK or Iran. Sometimes, after the payment has been made, the customer changes the order from non-controlled to controlled goods.

35. In most cases, proliferators pay for this procurement through formal financial institutions, leading to two potential scenarios. First, financial institutions may inadvertently facilitate proliferation. Second, if they possess the necessary expertise and capacity to detect proliferation financing, they can help prevent the proliferation of weapons of mass destruction and make the world safer. That said, it is important to note that financial institutions are not expected to become technical experts on dual-use goods themselves; rather, they require clear channels for consultation and follow-up with competent authorities—particularly those responsible for strategic trade.

36. Another component of proliferation financing is fundraising. The UN Security Council sanctions regime against DPRK specifically prohibits DPRK from earning money abroad because the Security Council recognized that at least part of the funds raised directly help the advancement of its nuclear and missile programs. Under UN Security Council Resolutions, DPRK is banned from exporting armaments, selling various commodities, such as sand or coal, and sending its workers overseas, to name a few prohibitions.

37. Due to the lack of a universal definition of "proliferation financing," fundraising by other proliferators, such as Iran, cannot be as easily seen as part of proliferation financing as in the case of the DPRK. However, the fundraising component is relevant due to unilateral sanctions regimes and prevention of other types of financial crime, such as money laundering and terrorism financing.

38. The concept of proliferation financing is increasingly expanding into the virtual assets domain. Proliferators use virtual assets to move and launder funds, evade sanctions, and engage in illicit activities that support their proliferation objectives.

3.3. International Obligations: UN Security Council Resolutions and FATF Recommendations

39. There are two sources of international obligations on proliferation financing: UN Security Council Resolutions (UNSCRs) and FATF Recommendations.

40. UN Security Council Resolutions represent hard law. All UN member-states are required to implement them. UN Security Council Resolution 1540 (2004) and subsequent resolutions on domestic proliferation

controls, as well as resolutions on the DPRK and Iran, are directly relevant for international obligations to prevent proliferation financing.

UN Security Council Resolution 1540

41. UNSCR 1540 requires all UN member-states to implement domestic proliferation controls, including on financing, to prevent non-state actors from obtaining WMDs. Two paragraphs of UNSCR 1540 are directly relevant to proliferation financing.

42. The Operative Paragraph 2 of UNSCR 1540 states:

> "..all States, in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them.[7]"

43. The Operative Paragraph 3d of UNSCR 1540 states that states must:

> "…establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as financing,[8] and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations."

44. The terms "financing" and "proliferation financing" were not explicitly defined under Resolution 1540 or its subsequent resolutions. Subsequent UN Security Resolution 2325 (2016) noted the need for greater attention to proliferation-finance measures and was the first Security Council Resolution to explicitly mention "proliferation finance." In 2022, in another follow-up, Resolution 2663 upheld and encouraged compliance with the proliferation-finance component of Resolution 1540.[9]

UN Security Council Resolutions on DPRK

45. The UN Security Council established a broad sanctions regime against the DPRK to curb its WMD program. In 2006, the DPRK conducted missile tests, and the UN Security Council issued Resolution 1695, which required all UN member-states to prevent the sale of missile- and WMD-related goods and technologies to and from the DPRK. The UNSCR 1695 also established a requirement for states to prevent "…the transfer of any financial resources in relation to the DPRK's missile or WMD programmes."[10] Later the

[7] UNSCR 1540, 2004, Operative Paragraph 2.

[8] UNSCR 1540, 2004, Operative Paragraph 3.

[9] For example, Operative Paragraph 12 calls for more attention to numerous issues, including proliferation financing.

[10] UNSCR 1695, July 15, 2006.

same year, the DPRK conducted its first nuclear test. The UN Security Council responded with a new set of sanctions codified in UNSCR 1718, which included expansive restrictions on any trade in WMD-related goods and technologies with the DPRK.

46. UNSCR 1718 introduced targeted financial sanctions and established a list of entities and individuals engaged in or providing support for the DPRK's WMD and missile programs. The Resolution obligated UN member-states to freeze the funds, assets, and economic resources of designated entities and individuals.[11] In conjunction with UNSCR 1718, the UN Security Council provided a list of sensitive goods and technologies associated with nuclear programs.[12] The list was expanded over the years.

47. UNSCR 1874 (2009) expanded the financial sanctions by prohibiting transactions that would provide financial support to the DPRK's missile and WMD programs.[13] By 2013, UN Security Council resolutions expanded the list of designated entities and individuals, the list of controlled items, and the scope of controls.[14] UNSCR 2094 prohibited access to international systems (banking, provision of financial services, international trade) where access could contribute to the DPRK's prohibited activity.[15]

48. UNSCRs 2321, 2371, 2375, and 2397, adopted in 2016-2017, imposed additional restrictions on the imports and exports of various goods, including seafood, machinery, coal, iron, and other commodities. In addition, the DPRK was prohibited from sending its laborers overseas. These extensive restrictions are aimed at curbing the DPRK's fundraising abilities.

49. The UN Panel of Experts on the DPRK, which monitored sanctions implementation and provided valuable data on the DPRK's sanctions evasion, was dissolved in 2024. FATF noted that its dissolution "presents a major challenge for monitoring violation of sanctions related to the DPRK."[16]

UN Security Council Resolutions on Iran

50. In 2006, the UN Security Council adopted Resolution 1696 that demanded that Iran halts its uranium enrichment program.[17] The same year, the UN Security Council adopted Resolution 1737, which imposed sanctions on Iran for failing to stop its uranium enrichment program, imposed a ban on the supply of nuclear-related technology and materials, and imposed an asset freeze on key individuals and entities related to Iran's enrichment program.[18] In 2007, UNSCR 1747 imposed an arms embargo on Iran and called upon "States and international financial institutions not to enter into new commitments for grants,

[11] UNSCR 1718, October 14, 2006.

[12] For compilations of prohibited items, see "Lists of Items Prohibited for Export to and Import from The Democratic People's Republic Of Korea pursuant to Security Council Resolution 1718 (2006)," https://main.un.org/securitycouncil/en/sanctions/1718/prohibited-items.

[13] UNSCR 1874, June 12, 2009.

[14] UNSCR 2094, March 7, 2013; UNSCR 2087, January 22, 2013.

[15] UNSCR 2094, March 7, 2013.

[16] *Complex Proliferation Financing and Sanction Evasion Schemes*, FATF, 2025, p. 13, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

[17] UNSCR 1696, July 31, 2006.

[18] UNSCR 1737, December 23, 2006.

financial assistance, and concessional loans" with Iran.[19] UNSCR 1803 (2008) established that states should exercise vigilance on public finance when it comes to trade with Iran and over the activities of financial institutions with banks domiciled in Iran. UNSCR 1803 decided that all states should take measures to prevent supply, sale or transfer of prohibited items from their territories, or by their nationals, or using their flag vessels or aircraft. Importantly, it also called upon states to inspect the cargoes to and from Iran, of aircraft and vessels owned or operated by Iran Air Cargo and the Islamic Republic of Iran Shipping Line, provided there are grounds to believe an aircraft or a vessel is carrying prohibited goods.[20] UNSCR 1835 (2008) called upon Iran to comply with prior resolutions and meet the requirements of the IAEA Board of Governors.[21]

51. UNSCR 1929 (2010) obliged States to prevent Iran from accessing "financial resources or services" that would enable its acquisition of prohibited goods and called for more expansive restrictions, including on providing insurance services to Iran. It also established the Panel of Experts to support the UN Iran Sanctions Committee's work.[22] UNSCR 2224 (2015) extended the mandate of the Panel of Experts.[23]

52. In 2015, five permanent members of the UN Security Council (the United States, the United Kingdom, Russia, France, and China), plus Germany, and the High Representative of the EU - signed a Joint Comprehensive Plan of Action (JCPOA) with Iran, known as the Iran Nuclear Deal. JCPOA imposed restrictions on Iran's nuclear activities. As a direct result, the UN Security Council adopted Resolution 2231 (2015), which endorsed the JCPOA and set the stage to terminate previous UN resolutions targeting Iran's nuclear program on JCPOA Implementation Day (January 16, 2016). UN retained arms embargo on Iran for 5 years until 2020. UN restrictions on Iran's ballistic missile program expired in 2023. UNSCR 2231 prohibited making assets or financial services available or conducting financial transactions related to certain nuclear- and ballistic missile-related items, and arms and other materials without UN Security Council approval. In conjunction with UNSCR 2231, the UN Security Council maintained a list of designated entities and individuals.[24]

53. In 2023, UN sanctions on Iran's nuclear and missile program expired (reinstated in 2025). In 2018, the United States abandoned the JCPOA, and Iran gradually resumed activities formally prohibited under the agreement. In 2025, the "snapback" mechanism was initiated to reimpose UN sanctions on Iran. All provisions of UNSCRs 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010) have been re-applied. The measures contained in paragraphs 7, 8, 16-20 of UNSCR 2231 (2015) were terminated.[25]

[19] UNSCR 1747, March 24, 2007.

[20] UNSCR 1803, March 3, 2008.

[21] UNSCR 1835, September 27, 2008.

[22] UNSCR 1929, June 9, 2010.

[23] UNSCR 2224, June 9, 2015.

[24] UNSCR 2231, July 20, 2015.

[25] Resolution 2231 (2015) on Iran Nuclear Issue, https://main.un.org/securitycouncil/en/content/2231/background.

FATF Recommendations*

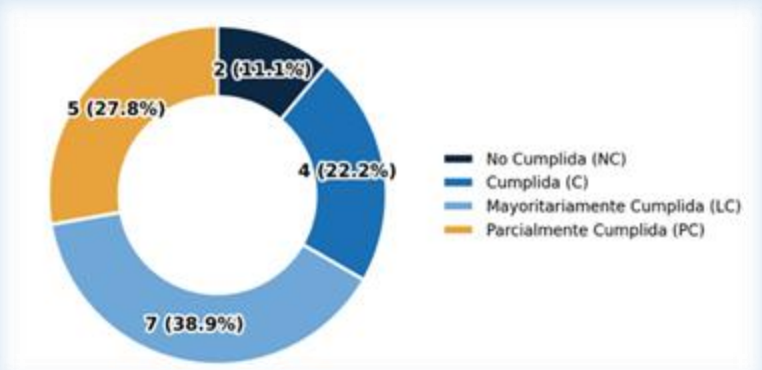
**The following section presents compliance statistics for the region within the framework of the GAFILAT 4th Round of Mutual Evaluations. At the time this document was prepared, no reports on GAFILAT delegations for the 5th Round had been approved.*

54. Several FATF Recommendations provide an important source of international legal obligations for preventing the financing of the proliferation of weapons of mass destruction.

55. FATF Recommendation 7 requires member jurisdictions to implement targeted financial sanctions against the DPRK and Iran and states:

> "Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require 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, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations."[26]

Regional Compliance (4th MER) Rec. 7



[26] Recommendation 7, The FATF Recommendations, as amended June 2026, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

56. Based on the 18 MERs conducted during the GAFILAT 4th Round of Mutual Evaluations, regarding Recommendation 7, 4 jurisdictions received a rating of Compliant (no deficiencies), 7 of Largely Compliant (minor deficiencies), 5 of Partially Compliant (moderate deficiencies), and 2 of Non-Compliant (major deficiencies).

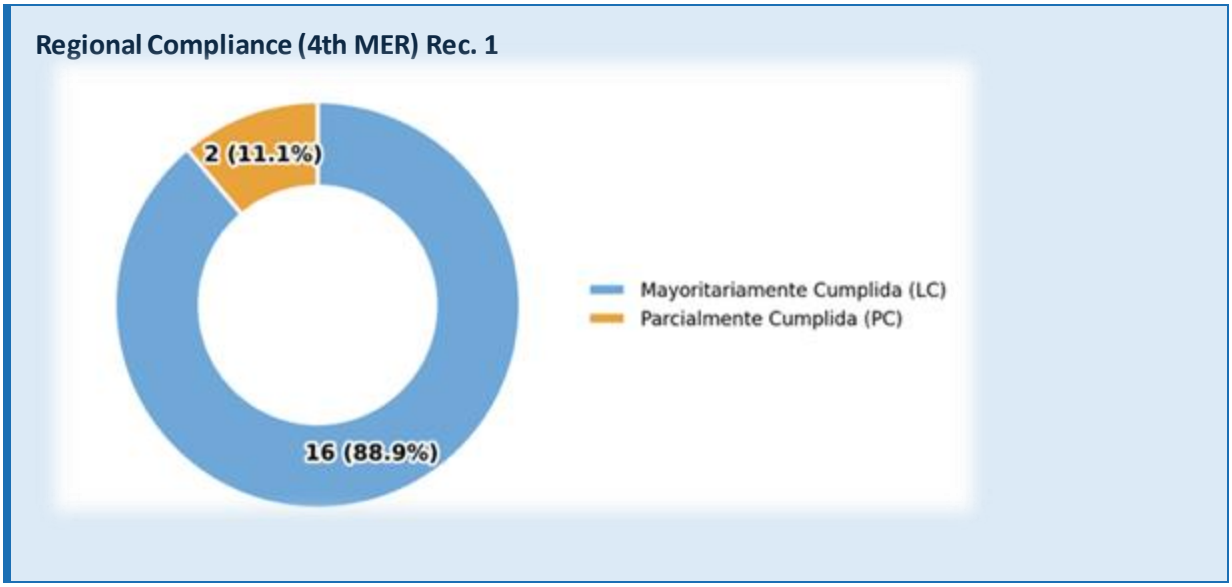
57. **It is important to note that, at the international level, there are additional unilateral or autonomous sanctions regimes that are used by a significant number of AML/CFT/CPF obliged entities, but which do not form part of the FATF Standards. Consequently, they are not subject to mutual evaluation, and references to such sanctions in this document are made to address the full range of factors and operational measures surrounding this subject matter.**

58. FATF Recommendation 1 requires member jurisdictions to conduct a national proliferation financing risk assessment.

59. The relevant part of Recommendation 1 states:

> "[…] Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7. Countries should take proportionate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose. Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are proportionate to the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.
>
> Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective and risk-based action to mitigate their money laundering, terrorist financing and proliferation financing risks."[27]

[27] Recommendation 1, The FATF Recommendations.

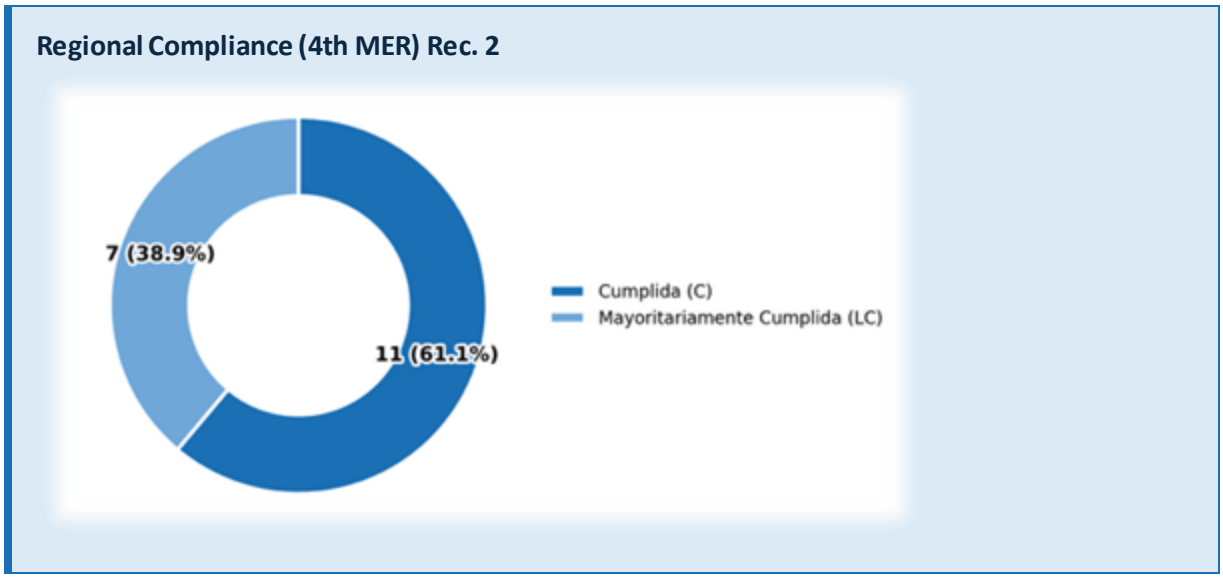


60. Based on the 18 MERs conducted during the GAFILAT 4th Round of Mutual Evaluations, regarding Recommendation 1, 16 jurisdictions received a rating of Largely Compliant (minor deficiencies) and 2 received a rating of Partially Compliant (moderate deficiencies).

61. FATF Recommendation 2 requires national coordination and cooperation on proliferation financing:

> "Countries should have national AML/CFT/CPF policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.
>
> Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation)."[28]

[28] Recommendation 2, The FATF Recommendations.



62. Based on the 18 MERs conducted during the GAFILAT 4th Round of Mutual Evaluations, regarding Recommendation 2, 11 jurisdictions received a rating of Compliant (no deficiencies) and 7 received a rating of Largely Compliant (minor deficiencies).

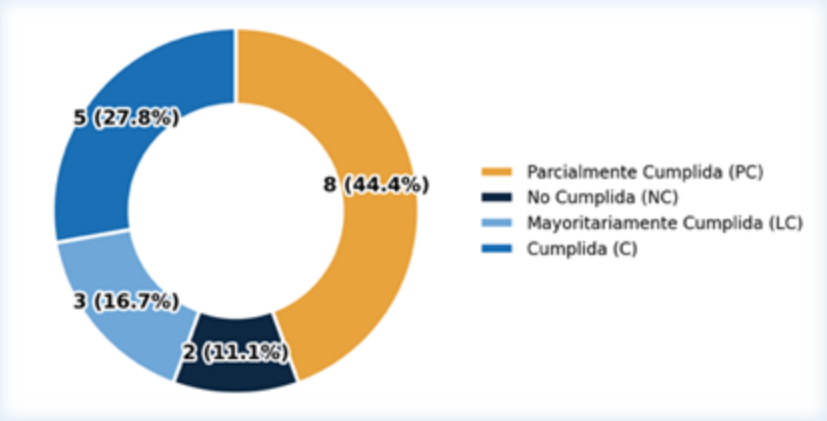
63. Recommendation 15 on new technologies is also relevant, as virtual assets can be used for proliferation financing and sanctions evasion:

> "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.
>
> To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."[29]

64. In accordance with Recommendation 1, countries should identify, assess, and understand the risks of money laundering, terrorist financing, and proliferation financing arising from virtual asset activities and the activities and operations of VASPs.

[29] Recommendation 15, The FATF Recommendations.

Regional Compliance (4th MER) Rec. 15



65. Based on the 18 MERs conducted during the GAFILAT 4th Round of Mutual Evaluations, regarding Recommendation 15, 5 jurisdictions received a rating of Compliant (no deficiencies), 3 of Largely Compliant (minor deficiencies), 8 of Partially Compliant (moderate deficiencies), and 2 of Non-Compliant (major deficiencies).

66. Immediate Outcome 11 in the FAFT Methodology pulls together Recommendation 7 and elements of Recommendations 1, 2, and 15:

> "Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs."[30]

67. For the purposes of this study, it is important to note that Recommendation 1 and Recommendation 7 are limited to the risk associated with non-compliance, failure to implement, or evasion of obligations arising from United Nations targeted financial sanctions (TFS). These obligations constitute only a portion of the restrictions imposed on the DPRK and Iran under relevant UN Security Council resolutions. Recommendation 1 reiterates that the requirement to conduct a national proliferation risk assessment applies in the context of TFS implementation. This report analyzes the commercial, maritime, Customs, logistics, corporate, and technology sectors; while these sectors do not in themselves expand the scope of Recommendation 7, they constitute the channels through which the evasion, concealment, or non-compliance of PF-related TFS can occur. Notwithstanding the narrow definition in Recommendation 7, the FATF employs a broader operational definition of PF for the purposes of its Guidance documents—one that extends beyond the application of TFS. For example, in the 2021 *Guidance on Proliferation Financing Risk Assessment and Mitigation*:

> "The financing of proliferation refers to the risk of raising, moving, or making available funds, other assets, or other economic resources, or financing, in whole or in part, to persons or entities

[30] Immediate Outcome 11, Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems, FATF, p. 166, https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.

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."[31]

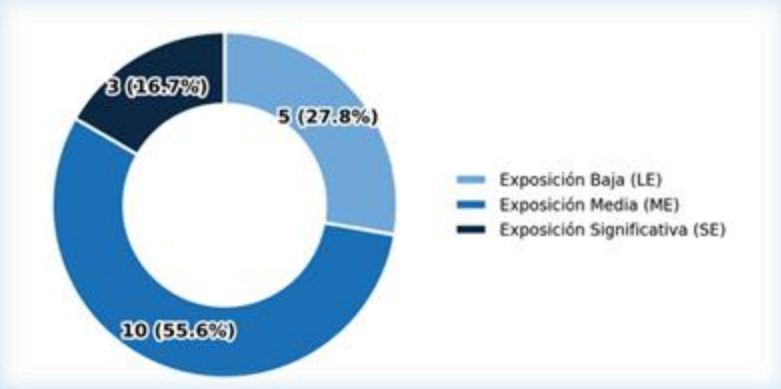
68. With WMD proliferation defined as:

"[T]he 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."[32]

69. Moreover, in its latest 2025 report, *Complex Proliferation Financing and Sanctions Evasion Schemes*, FATF does not limit relevant case studies to the DPRK and Iran.[33]

70. That said, it is important to note that, for the purposes of FATF mutual evaluations, compliance with PF-related obligations focuses on Recommendations 1, 2, 7, and 15, and on IO 11, and the guidances are not binding, although recommended.[34]

Regional Compliance (4th MER) IO 11



[31] Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, 2021, p. 8, https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html.

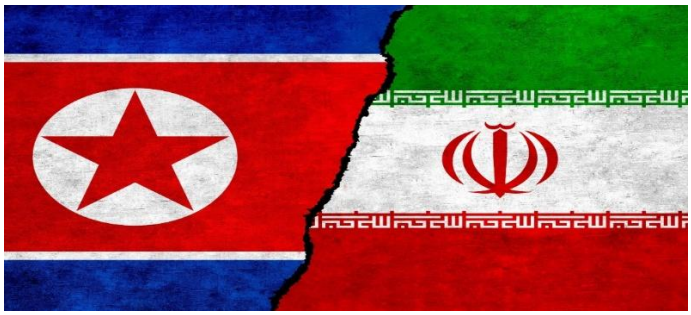
[32] *Ibid.*

[33] *Complex Proliferation Financing and Sanctions Evasion Schemes*, FATF, 2025.

[34] Footnote 19, Interpretative Note to Recommendation 7: Recommendation 7 is focused on targeted financial sanctions. However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

71. Based on the 18 MERs conducted during the GAFILAT 4th Round of Mutual Evaluations, regarding Immediate Outcome 11, 3 jurisdictions received a rating of Substantial (the Immediate Outcome is achieved and moderate improvements are required), 10 received a rating of Moderate (the Immediate Outcome is achieved to some extent and considerable improvements are required), and 5 received a rating of Low (the Immediate Outcome is not achieved or is achieved insignificantly, and fundamental improvements are required).

3.4. Proliferators in Focus: the DPRK and Iran



72. The report focuses on DPRK and Iran because the UN Security Council has recognized them as proliferators, and the FATF Recommendations, specifically Recommendation 7, focus on these two jurisdictions. However, as noted earlier, the global threat of proliferation and the existing universe of relevant typologies also involve other actors.

73. DPRK possesses approximately 50 nuclear warheads and nuclear material to produce even more nuclear weapons. In addition to nuclear warheads and nuclear material it already has, the country operates facilities that can produce plutonium and enrich uranium. Both highly enriched uranium and plutonium are types of nuclear material that can be used in the production of nuclear weapons. DPRK has also developed short-, medium-, and long-range missiles, including intercontinental missiles. According to technical experts, DPRK has the capacity to equip its short- and medium-range missiles with nuclear warheads, and possibly its longer-range missiles as well.[35]

74. Iran does not have nuclear weapons but maintains an advanced nuclear program. According to the IAEA, until 2003, Iran pursued an organized nuclear weapons program. As of June 2025, Iran had over 9,000 kilograms of uranium stored, and 440 kilograms of this uranium had been enriched to 60%, close to weapons-grade levels, according to the International Atomic Energy Agency (IAEA).[36] Since the military operations carried out by the United States and Israel in June 2025, the IAEA has been unable to verify the amount of material in Iran.

[35] Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight, "North Korean Nuclear Weapons, 2024," *Bulletin of the Atomic Scientists* 80, No. 4 (2024), 251.

[36] "Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015), GOV/2025/50, IAEA, September 8, 2025, p. 8, https://www.iaea.org/sites/default/files/documents/gov2025-50.pdf.

75. Iran's missile program and unmanned aerial vehicle (UAV) capabilities pose a serious threat to international security. The Annual Threat Assessment of the U.S. Intelligence Community concluded in 2025: "Iran has fielded a large quantity of ballistic and cruise missiles as well as [UAS] that can strike throughout the region and continues efforts to improve their accuracy, lethality, and reliability."[37] The current size of Iran's ballistic missile inventory, after the U.S. and Israeli strikes on Iran in 2025 and 2026, is uncertain.[38]

76. DPRK and Iran procure dual-use goods and technology from the international commercial market. In most illicit procurement cases, they rely on formal financial institutions for payments. Both countries are also increasingly using virtual assets to launder and move funds. The cases of DPRK and Iran highlight the importance of proliferation financing controls. Strengthening proliferation financing controls would make it harder for these two proliferator states to procure the sensitive goods and technology they use to advance their military programs.

77. The subsequent section of the report provides real-life examples of how the DPRK and Iran use the high-risk sectors for proliferation activities.

[37] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, March 2025, p. 24, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf#page=24.

[38] "U.S. Military Operations Against Iran's Missile and Nuclear Programs," Congressional Research Library, U.S. Congress, March 6, 2026, https://www.congress.gov/crs-product/IN12665.



CHAPTER 4

High-Risk Sectors

4. High-Risk Sectors

4.1. Financial Sector



4.1.1. Global Risk

78. The financial institutions, by default, have the highest exposure to proliferation financing – they provide financial services that can contribute to the proliferation of WMD. The vulnerabilities faced by the financial institutions can be divided into several categories: (1) transactions directly connected with the procurement of dual-use goods and technology; (2) transactions connected with fundraising for proliferation; (3) transactions connected with servicing high-risk sectors.

(1) Transactions directly connected with the procurement of dual-use goods and technology

79. Financial institutions struggle to identify if transactions are relevant to the procurement of sensitive (dual-use) items for illicit purposes. As discussed earlier, dual-use goods and technology have many peaceful applications and are easily available on the international commercial market. The information about goods that financial institutions see when facilitating transactions is limited. The descriptions can be vague ("spare parts," "machine equipment," and so on), not sufficient to determine whether the goods belong to the dual-use category. Financial institutions do not have the technical expertise to identify dual-use goods and technology. It is also difficult for financial institutions to determine whether goods are part of

legitimate trade or are illicitly procured for proliferation purposes without dedicated risk management effort.

80. Another challenge is identifying the final end-use, end-user, and destination of the goods. Proliferators rely on deceptive tactics: they falsify who, where, and for what purpose will use the goods. When purchasing goods from a supplier, procurement agents can claim that the goods are intended for a domestic company. In that case, the supplier and the government will not conduct extra scrutiny because no export-licensing process applies. Using another evasion tactic, procurement agents can buy goods slightly inferior to controlled items; in that case, no export-control checks apply, but the goods can still be used for military purposes. Another common technique is for procurement agents to pretend that a good is going to a third jurisdiction that is not under sanctions or not a proliferant state. For example, it may look to a financial institution that a transaction supports the purchase of equipment that will go to a Chinese company, when in fact, the product it will eventually be shipped to the DPRK. Similarly, the paperwork might indicate that a piece of equipment is being shipped to a UAE-based company when, in fact, it is destined for Iran.

81. Even ensuring that entities and individuals designated by the UN Security Council (the implementation of UN targeted financial sanctions as required by FATF Recommendation 7) are not parties to transactions involving sensitive goods is complicated. Designated entities and individuals hide behind front and shell companies and the names of associates. Therefore, simple screening against lists of designated entities and individuals without additional risk management tools is insufficient.

82. Unlike typologies for money laundering (ML) and terrorism financing (TF), proliferation financing (PF) typologies are less straightforward and harder to operationalize. To give just one comparative example. PF does not involve a defined monetary threshold and can entail transactions of ordinary amounts consistent with legitimate trade. Consequently, the absence of anomalies linked to transaction amounts should not be considered sufficient grounds to rule out potential cases of PF.

83. In sum, the lack of technical expertise, the vagueness of proliferation financing typologies, the common use of dual-use goods and technology in international trade, and deceit techniques employed by proliferators make it hard for financial institutions to identify transactions connected with the illicit procurement of sensitive goods.

(2) Transactions in support of fundraising for proliferation

84. It is even harder for financial institutions to implement controls on transactions that may be connected to fundraising for proliferation. This is complicated for two main reasons: (1) the unevenness of international obligations to prevent the fundraising component of proliferation financing, depending on the proliferant country in question, and the general vagueness of national obligations when it comes to stopping fundraising; (2) the practical limitations financial institutions face in identifying whether transactions are part of fundraising for proliferation purposes.

85. The broad UN Security Council sanctions imposed on the DPRK restrict Pyongyang's ability to sell various commodities and the use of global financial services in general, making most economic activities involving international markets by the DPRK illicit. Funds obtained by the DPRK abroad contribute to its military program. A broad sanctions regime against the DPRK de facto imposes obligations on UN member states to prevent the DPRK government from fundraising.
86. In the case of Iran, the international legal basis for the fundraising component of proliferation financing is less straightforward. Between 2016 and 2025, while UN nuclear-related sanctions on Iran were lifted

under the Joint Comprehensive Plan of Action (JCPOA), the targeting of Iran's revenue generation was left mainly to unilateral (autonomous) measures by the U.S. and the EU. UNSCR 2231 (2015) did not include prohibitions on Iran's fundraising activities. The "snap back" of UN sanctions against Iran on September 27, 2025, resurrected the pre-2015 UN sanctions architecture, which includes some fundraising-related components. For example, UNSCR 1747 (2007) calls upon all states and international financial institutions "not to enter into new commitments for grants, financial assistance, and concessional loans, to the Government of the Islamic Republic of Iran, except for humanitarian and developmental purposes."[39] Still, UN Security Council resolutions on Iran never went as far as those on the DPRK in terms of fundraising activities.

87. Instead, unilateral (autonomous) sanctions, such as those imposed by the United States and the EU, have been more extensive in scope and were designed to cap Iran's fundraising activities. (*read in line with paragraph 57)*[40]

88. At the same time, FATF's Recommendation 7, with its requirement to implement UN targeted financial sanctions, de facto means that restrictions on fundraising activities apply only to designated entities and individuals and those associated with them.

89. When it comes to practice, detecting transactions that can be tied to fundraising for proliferation purposes is even harder than detecting transactions in support of the procurement of sensitive goods. The link between the transaction and a proliferation act is not linear and hard to identify.

(3) Transactions connected with servicing high-risk sectors

90. The third dimension of risk that financial institutions face is via servicing high-risk sectors. Key high-risk sectors – dual-use sector; maritime sector; FTZs, trust and company service providers; legal professionals

[39] UNSCR 1747 (2007), p. 3, https://docs.un.org/en/S/RES/1747%20(2007).

[40] For example, U.S. Executive Order 13902 provides authority to sanction key sectors of Iran's economy to deny the Iranian government financial resources that can be used to fund and support its nuclear and missile programs, terrorist activities, and malign regional influence. (U.S. Executive Order 13902, https://www.justice.gov/eoir/page/file/1234236/dl). In recent years, the U.S. government expanded targeted sanctions related to Iran's petrochemical sales. (See, for example, "Treasury Expands Targeted Sanctions on Iranian Petroleum and Petrochemical Sectors in Response to Attack on Israel," Press Release, U.S. Department of Treasury, October 11, 2024, https://home.treasury.gov/news/press-releases/jy2644; "Treasury Tightens Sanctions on Iran's Oil Network Supporting its Military," Press Release, U.S. Department of Treasury, November 20, 2025, https://home.treasury.gov/news/press-releases/sb0322; "Sanctioning Additional Entities That Have Traded in Iran's Petroleum," Press Release, U.S. Department of State, March 20, 2025, https://www.state.gov/sanctioning-additional-entities-that-have-traded-in-irans-petroleum). The 2025 National Security Presidential Memorandum/NSPM-2 directs an enforcement campaign that denies Iran and its proxies access to revenue. (National Security Presidential Memorandum/NSPM-2, The White House, February 4, 2025, https://www.whitehouse.gov/presidential-actions/2025/02/national-security-presidential-memorandum-nspm-2/.)

The EU autonomous restrictive measures reinstated after the 2025 UN sanctions "snapback" include a ban on imports of Iranian crude oil, natural gas, and petrochemical and petroleum products, as well as a freeze on the assets of the Central Bank of Iran and major Iranian commercial banks. ("Iran Sanctions Snapback: Council Reimposes Restrictive Measures," Press Release, Council of the European Union, September 29, 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/09/29/iran-sanctions-snapback-council-reimposes-restrictive-measures/; "EU Sanctions Against Iran," Council of the European Union, https://www.consilium.europa.eu/en/policies/sanctions-against-iran/.)

(lawyers), accountants, notaries; dealers in precious metals and stones; VASPs – rely on financial institutions for their operations.

91. Below are three illustrative examples of this secondary exposure.

Example 1

A bank issues a letter of credit to a shipping company operating a vessel controlled by the DPRK and involved in moving commodities in violation of UN sanctions. In this scenario, the bank inadvertently contributes to sanctions evasion.

Example 2

A bank provides an off-ramp for converting cryptocurrency into fiat. The cryptocurrency exchange involved did not carry out stringent KYC and allowed DPRK agents to exploit their services for laundering cryptocurrency stolen during a cyber attack. In this scenario, an unsuspecting bank will inadvertently contribute to DPRK's fundraising efforts.

Example 3

A company registered in a free trade zone facilitated an illicit transfer of sensitive goods through a free trade zone. The company's payment transactions were routed through a local bank, thereby making it part of the illicit procurement scheme.

4.1.2. Regional Risk

92. The regional risk assessment of the financial sector is based on responses to country surveys submitted by 16 jurisdictions and, where necessary, has been supplemented by virtual follow-up meetings.

93. The country survey was designed to compile a general picture of legal frameworks; progress on national risk assessment; training and guidance provided by competent authorities; supervision and STR requirements; KYC procedures implemented by financial institutions; and proliferation financing detection and investigations.

Legal frameworks

94. Domestic legislation is the foundation of any national system for implementing proliferation financing controls. To assess the broader legal-regulatory environment relevant to proliferation financing, the country survey asked GAFILAT jurisdictions whether they have legal frameworks to implement FATF Recommendation 7. Submitted data was supplemented with open-source data to assess the legal frameworks for implementing UN Security Council Resolution 1540.

95. At a high level, the region-wide legal framework for implementing targeted financial sanctions in line with the relevant UN Security Council Resolutions and FATF Recommendation 7 shows progress. While

regulatory challenges remain—as evidenced by the statistics in the "Regional Compliance (4th MER)" section—it can be concluded that the framework is generally robust across the region. Of 16 jurisdictions that participated in country surveys, 14 – Argentina,[41] Bolivia, Brazil, Chile, Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay – reported having legal frameworks for implementing UN Security Council targeted sanctions, in line with FATF Recommendation 7. Similarly, most GAFILAT jurisdictions have legal frameworks in place to implement UN Security Council Resolution 1540.

National proliferation financing risk assessment and risk management

96. An important component of implementing proliferation financing is risk assessment and risk management.[42] The country surveys, whose objective was to obtain primary regional information, included questions that would provide an indication of three critical components: (1) national proliferation financing risk assessment; (2) the requirement for financial institutions to conduct proliferation risk assessments, and (3) the actual implementation of proliferation financing controls by financial institutions.

97. When it came to national proliferation financing risk assessment, only 9[43] GAFILAT jurisdictions – Argentina,[44] Brazil, Chile, Colombia, Mexico, Nicaragua, and Peru – conducted national proliferation risk assessments. Additionally, 3 jurisdictions – Bolivia, Panama, and Paraguay – reported that their national risk assessments were in progress. In Panama's case, the process is in its final stage before approval by the National Commission against Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction. Meanwhile, Ecuador reported that, although its National Risk Assessment is not yet complete, it has initiated internal processes to ensure the assessment includes a proliferation financing component. As a reminder, revised FATF Recommendation 1 requires jurisdictions to conduct a national risk assessment of proliferation financing (defined narrowly as the implementation of UN targeted financial sanctions). The 5th round of mutual evaluations commenced in 2024 using the revised 2022 Methodology and Procedures, examines whether a country has met all the technical requirements of each of the 40 FATF Recommendations in its laws, regulations, and other legal instruments, including revised FATF Recommendation 1. GAFILAT members should treat completing national proliferation risk assessments as a priority.

98. As some jurisdictions in the region have yet to complete their national proliferation risk assessment, the country survey allowed for delegations to reflect on their *perception* of the level of risk. The following patterns emerged from the responses. The average perceived risk in the region is low. This warrants caution, as assuming the risk is low can create a false sense of security. Proliferators' sophisticated evasion tactics, and the fact that financial institutions can be exposed to proliferation financing even when sensitive goods do not physically originate in or transit through their national territories, create vulnerabilities that are hard to quantify.

[41] Asset freezing is being regulated by the FIU only, but the country is in the process of regulating domestically all components required under FATF Recommendation 7.

[42] In line with paragraphs 3 and 4 of the Interpretative Note of FATF Recommendation 1.

[43] Costa Rica and Cuba did not participate directly in the survey, as they were undergoing their mutual evaluation processes at the time this report was drafted (May 2025). However, they have conducted PF NRAs, details of which are provided in Annex I.

[44] The first National Risk Assessment (NRA) was conducted in 2019, followed by a second in 2022; Argentina is currently in the process of updating the third NRA in this field.

99. The survey also asked GAFILAT jurisdictions whether financial institutions are required to conduct institutional proliferation financing risk assessments. Only 10 jurisdictions – Argentina, Bolivia, Colombia, Ecuador, El Salvador, Mexico, Nicaragua, Panama, Peru, and Uruguay – reported that such a requirement exists. To remind, FATF Recommendation 1 Interpretative Note 1 says: "Financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks."[45]

100. This section of the survey sought to determine which sectors GAFILAT jurisdictions consider high risk for proliferation financing by asking them to name such sectors. Many responded "none" or left the answers blank. Colombia, Ecuador, Peru, and Uruguay named specific high-risk sectors; Mexico and Paraguay identified areas of concern or vulnerability; and Guatemala flagged VASPs as a potential emerging risk. Colombia stood out with the most nuanced answer based on responses from several competent authorities.

101. Among the sectors mentioned by the responding jurisdictions:

(1) financial and money services, including money transfer and remittance companies, currency exchange and foreign-exchange market intermediaries;
(2) VASPs;
(3) Trade, transport, and logistics sector, including foreign-trade and export/import companies, ports, airports, free trade zones, and transport companies;
(4) Manufacturing, industry, and goods sector, including specific industries relevant to dual-use goods and technology, such as chemical and biological, and high-tech industry, mineral extraction and dealers in precious metals and stones;
(5) non-profit organizations.

102. Responses provided in country surveys in Annex I mention several sectors that are identified as high risk and described in detail in this report.

Training and guidance

103. Training and guidance provided by competent authorities to government agencies and the private sector are critical in improving the implementation of proliferation financing controls. The country survey asked GAFILAT jurisdictions to report on whether competent authorities offer relevant training and guidance.

104. Out of 16 reporting jurisdictions, 15 shared that their competent authorities provide training on proliferation financing. The country surveys show that GAFILAT and external partners play an important role in providing proliferation financing training in the region, in addition to training offered by domestically initiated efforts.

105. The majority – 11 out of 16 reporting jurisdictions (Argentina, Bolivia, Chile, Colombia, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Paraguay, and Peru) – provide guidance (guidelines or other

[45] Interpretative Note 1, The FATF Recommendations, as amended October 2025, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. p. 32.

forms of assistance) on proliferation financing. Below is a table of select examples of provided guidance relevant to proliferation financing.

Table 1. Select Examples of Guidance on Proliferation Financing

	Country	Select Examples
1.	**Argentina**	▪ The Financial Information Unit (UIF) released the FATF report on this subject, highlighting key deficiencies in the global response to proliferation financing and sanctions evasion. ▪ As a responsible producer and exporter of sensitive and dual-use materials and technology, the Argentine Republic systematically incorporates—into its outreach and training activities—the risks associated with the financing of the proliferation of weapons of mass destruction (WMD), as well as the importance the National State places on preventing and combating it. ▪ Accordingly, this topic is included in the agendas of all awareness-raising and outreach activities organized by the State for the private sector, academia, institutions, and public officials regarding the export control of sensitive, military, and dual-use materials and technology. ▪ Notable among these are the biannual outreach sessions organized by the National Commission for the Control of Sensitive Exports and Military Materials (CONCESYMB) for the domestic industrial sector. ▪ Furthermore, WMD proliferation financing is addressed through specific panels led by competent bodies and experts—such as the Financial Information Unit (UIF) and the Central Bank of the Argentine Republic (BCRA)—during international cooperation initiatives with foreign partners regarding non-proliferation and export controls. These initiatives include, among others, activities organized jointly with the United States Department of Energy (DOE), the U.S. Government's Export Control and Related Border Security (EXBS) Program, and Germany's Federal Office for Economic Affairs and Export Control (BAFA); these events occasionally feature the participation of representatives from the industrial sector and academia.
2.	**Bolivia**	▪ Specific Instructions for financial and non-financial Reporting Entities, with a risk management approach for implementing preventative measures in the fight against laundering of illicit proceeds, terrorism financing, and proliferation financing. ▪ Specific Instructions for Reporting Entities on the implementation of United Nations Security Council resolutions.

		▪ Guide for the implementation of targeted financial sanctions within the framework of United Nations Security Council Resolutions.
3.	**Chile**	▪ The UAF provides publicly accessible content to regulated entities and the general public, for example through the development of a brochure and audiovisual materials related to this topic, in addition to publishing a red-flag guide on ML/TF/PF, among other related materials.
4.	**Colombia**	▪ The UIAF has a "Guide for the implementation of United Nations Security Council resolutions on terrorist financing and the financing of the proliferation of weapons of mass destruction": https://www.uiaf.gov.co/sites/default/files/2024-06/Cartilla%20Sanciones%20Financieras%20Dirigidas%202018.pdf ▪ The Financial Superintendence of Colombia (SFC) has an explanatory video on the "Interadministrative Cooperation Agreement between the Ministry of Foreign Affairs, the Office of the Attorney General, the Financial Superintendence, and the Financial Intelligence Unit," for compliance with Resolutions 1267 of 1999, 1373 of 2001, 1988 of 2011, and 1737 of 2006, FATF Recommendations 6 and 7, and Article 20 of Law 1121 (2006): https://www.youtube.com/watch?v=K5cNQjqtnk4 ▪ The following information is available to reporting entities in the "Targeted Financial Sanctions: FATF Recommendations 6 and 7" menu on the Financial Superintendence website: https://www.superfinanciera.gov.co/publicaciones/10109831/industrias-supervisadas-sistema-de-administración-de-riesgo-de-lavado-de-activos-y-financiamiento-del-terrorismo-sanciones-financieras-dirigidas-recomendaciones-y-del-gafi-10109831/ ▪ The Financial Superintendence of Colombia publishes on its website the following supervisory guides covering PF-related topics, with the aim of publicizing the approach of the methodologies implemented by the supervisor and that must be taken into account by reporting entities:

		https://www.superfinanciera.gov.co/publicaciones/10086577/industrias-supervisadassistema-de-administracion-de-riesgo-de-lavado-de-activos-y-financiacion-del-terrorismo-10086577/
		
		Published guides:
		
		- SARLAFT Guide.
		- Good Practices Guide for Assessing the Quality of Customer Data of Entities Supervised by the SFC.
		- Guide for Evaluating the Identification of ML/TF/PF-WMD Risks of Entities Supervised by the SFC.
		  ○ Annex 1. Flowchart for Evaluating ML/TF/PF-WMD Causes.
		  ○ Annex 2. Flowchart for Evaluating ML/TF/PF-WMD Controls
		- Guide on Perspectives Regarding Politically Exposed Persons - PEPs - Based on the Supervisory Exercise.
		- Guide for Supervising the Process of Identifying the Direct Beneficial Owner in the Share Capital Composition of Customers of Entities Supervised by the SFC.
		- Conceptual Framework for Monitoring and Evaluating the SARLAFT of Entities Supervised by the SFC.
		
		▪ SuperSociedades (Superintendence of Companies): guidance is provided through training, legal compliance consultations, events for the proper implementation of SAGRILAFT (Self-Control and Comprehensive Risk Management System for Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction), and responses to inquiries/requests submitted to our supervisors. The guidance is aimed primarily at the private real sector of the economy.
		
		▪ The Ministry of Defense is developing the "Anti-Terrorism Strategy for the Security and Defense Sector" with the objective of preventing and addressing various terrorist actions, mitigating their impact, and contributing to the protection of the Colombian population and state.

5.	**El Salvador**	▪ The "Guide on Red Flags and TF/PF threats" is published on the FIU website and is aimed primarily at the private sector: https://www.fiscalia.gob.sv/wp-content/uploads/2024/08/Senales-de-Alerta-para-Prevencion-

		de-LDA-FT-FPADM-2024.pdf The FIU is responsible for issuing guidance and Red Flags on these topics.
6.	**Guatemala**	▪ Through regulations directed at reporting entities, the IVE imposes the specific obligation to constantly review their databases and other records to determine whether their clients, users, or persons with whom they do business or contract for goods or services, including attempted transactions, match persons designated by the UNSC. If matches are detected, reporting entities must immediately freeze any property, asset, fund, value, transfer, or account that may belong to or be controlled, directly or indirectly, by the obligated persons or entities, and must report this to the "Prosecutor's Office against Money Laundering or Other Assets." In this regard, the procedures that reporting entities must follow in such cases are expressly established in the instructions issued by the IVE.
7.	**México**	▪ The National Banking and Securities Commission (CNBV) has provided guidance to supervised entities in relation to PF through working groups and through the drafting and publication of the Guide on the financing of the proliferation of weapons of mass destruction in the national territory. The purpose of the Guide is to provide guidelines, elements, and criteria that supervised entities may take into account when implementing policies, criteria, measures, and procedures in order to prevent and detect acts, omissions, or transactions that may encourage or provide aid, assistance, or cooperation, or that may be related to PF. This document was prepared in coordination with the Financial Intelligence Unit (UIF).
8.	**Nicaragua**	▪ All AML/CFT/CPF supervisors provide feedback/guidance to their reporting entities (circulars, directives, manuals, executive summaries, etc.).
9.	**Panamá**	▪ UAF publishes a catalogue of typologies, including those identified for proliferation financing on its website. The catalog of identified typologies is intended for all obliged entities and primarily directed at the private sector. However, it can serve as a reference source for competent authorities in their investigations related to both ML/TF and PF. This catalog can be found at: https://www.uaf.gob.pa/Catalogo-de-Tipologias-y-Senales-de-Alerta
10.	**Paraguay**	▪ Paraguay provides various forms of guidance on the financing of the proliferation of weapons of mass destruction (PF), both to reporting entities and to other authorities and stakeholders.

		These tools include the Asset Freezing Protocol Guide, issued by SEPRELAD, which clearly defines the procedures, timelines, criteria for identifying suspicious assets, the responsibilities of reporting entities, and notification mechanisms in the event of matches with persons or entities linked to PF. This document was prepared on the basis of Law No. 6419/19 (which regulates the freezing of assets related to terrorism and the proliferation of weapons of mass destruction) and United Nations Security Council resolutions. ▪ Based on the aforementioned Guide, the delegation provides proactive and detailed assistance on the freezing of assets associated with PF; a clear step-by-step structure, with defined roles and timelines for reporting entities; and a framework that promotes compliance with national regulations and relevant international standards. ▪ Paraguay has also made available the Procedure for requesting delisting from the United Nations Security Council 1718 (2006) Sanctions List, implemented by SEPRELAD, which constitutes a specific guide for natural persons, legal persons, or States wishing to request the removal of a name from the sanctions list imposed under that resolution. ▪ Technical materials on PF-related issues aimed at the private sector have also been disseminated. For example, Bulletin No. 2 promotes the use of list-screening simulations, and Bulletin No. 20 addresses regional terrorist financing risk and the assessment of the AML/CFT/CPF system; both were issued by the Central Bank of Paraguay. ▪ In addition, as part of the supervision carried out by the Securities Superintendency, compliance with obligations is assessed through checklists, including those issued by the United Nations Security Council (UNSC), and recommendations are made to strengthen the controls applied by reporting entities in this regard.

		▪ Following the same approach, the Superintendency of Insurance provides guidance to insurance companies through written comments and clarification meetings, as well as through specific training sessions when particular needs are identified.
11.	**Perú**	▪ The National Risk Assessment on TF and PF has been published: https://www.sbs.gob.pe/Portals/5/jer/ESTUDIO-ANALISIS-RIESGO/2024/ENR%20FT%20FPADM%202024.pdf ▪ A freezing toolkit has also been developed to guide reporting entities in complying with targeted financial sanctions: https://www.sbs.gob.pe/prevencion-de-lavado-activos/listas-de-interes

Supervision and STR requirement

106. When implementing proliferation financing controls on the ground, supervision and STR requirements are important. It is important to note that the obligation to report suspicious transactions related to proliferation is not explicitly set out in the FATF Standards as a standalone requirement. However, such activities may fall within the scope of the concept of underlying criminal activity. In this regard, some countries adopt an approach that goes beyond the minimum requirements of FATF Standards, which is a positive development.

107. Supervisors in 15 of the 16 jurisdictions that submitted responses, Argentina, Bolivia, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Paraguay, Peru, and Uruguay, monitor or supervise financial institutions' compliance with targeted financial sanctions.

108. In total, 14 jurisdictions – Argentina, Bolivia, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Paraguay, Uruguay – require suspicious transaction reports or other types of reports for proliferation financing or for related targeted financial sanctions.

KYC procedures

109. The country survey asked jurisdictions whether KYC procedures applied by their financial institutions include a proliferation financing component. All jurisdictions that participated in the survey responded "Yes," with one jurisdiction providing a more nuanced answer that indicated that the majority, but not all, financial institutions include a PF component in their KYC procedures.

110. The main tool for implementing targeted financial sanctions is automated screening of customers against sanctions lists; all participating jurisdictions reported using it. Financial institutions use the UN Security Council consolidated sanctions list and, in many cases, lists from third jurisdictions (*see paragraph 57*), such as the U.S. OFAC, the European Union, and the UK/HM Treasury lists. Several

jurisdictions mentioned Interpol, the FBI, and other lists. The software-based screening solutions rely on various private-sector vendors.[46]

111. Supporting this screening core are broader due diligence and risk management tools. In most cases, financial institutions couple list screening with customer due diligence (CDD) and KYC processes that gather information on clients' economic activity, geographic exposure, sources of funds, and politically exposed person (PEP) status. Financial institutions also monitor negative media.

112. The majority of reporting jurisdictions have special procedures to reduce sanctions evasion risks and proliferation financing risk through trade finance. A subset of jurisdictions with more advanced export controls and proliferation financing controls described screening the underlying documentation of foreign-trade transactions – vessels, routes, ports, shipping companies, tariff headings, and cargo descriptions, as well as validating dual-use goods to identify potential military end-uses.

113. It is important to note that responses to the country survey on KYC tools used by financial institutions relied on sample answers from reporting entities and, by design, could not reflect the full picture. It is safe to assume that some financial institutions with greater capacity have more extensive relevant controls than, for example, small- or medium-sized institutions. Having said that, the fact that jurisdictions reported their financial institutions using tools beyond list-scanning is a very important and positive data point as list-scanning alone cannot fully guarantee the implementation of targeted financial sanctions. As discussed earlier, designated entities and individuals often hide behind front and shell companies and names of associates.

114. One pattern that emerged from the submitted responses is that financial institutions in the region implement broader sanctions-related controls than the domestic legislation requires. Usually, this happens for two reasons: (1) the subsidiaries of foreign banks with headquarters in the United States or the EU follow the compliance rules of their headquarters; (2) financial institutions are concerned about potential secondary sanctions that can disrupt their operations or access to correspondent banking. Representatives of several financial institutions in the GAFILAT region confirmed that they are following sanctions lists issued by third countries (for example, the United States, Canada, and the EU). For proliferation financing controls, these good practices that go beyond minimum compliance with domestic regulations can be positive. However, at the jurisdictional level, this can create tension between foreign policy objectives and private sector interests. Moreover, the uneven implementation of proliferation financing controls, with some financial institutions doing more and others less, underscores that a jurisdiction is as secure as its weakest link.

Detection and investigation

115. The country survey included a component that was designed to get a picture of detection and disruption of proliferation financing in the region. In that regard, data was requested on the number of relevant STRs filed and any investigations launched.

[46] Among those mentioned by the delegations are LexisNexis Bridger Insight and its World Compliance data source, SWIFT's sanctions and transaction screening system, World-Check, Monitor Plus modules, as well as tools from Safewatch and Moody's.

* Note: The software and IT solutions presented here are limited to those mentioned by the delegations in the project's country surveys and do not imply endorsement or promotion of their use by GAFILAT.

116. Out of 16 jurisdictions participating in the survey, 12 reported that no STRs related to proliferation financing were filed. Meanwhile, 3 jurisdictions reported between 1 to 6 STRs filed, and 1 jurisdiction described the data as "confidential." One more jurisdiction reported that no STRs were submitted but noted that during 2022-2026, it identified 12 matches with the UN Security Council sanctions lists, with 8 cases turning out to be false positives and 4 resulting in the freezing of funds.

117. On whether any PF-related investigations were launched in the last 10 years, 14 of 16 jurisdictions reported that none were launched, with 1 jurisdiction responding "Yes." And the FIU of another jurisdiction that reported freezing funds in 4 cases of confirmed matches with the UN Security Council sanctions lists could not attest whether further actions by other relevant agencies were taken after the freeze.

118. Two observations are warranted based on the responses. First, the 4 jurisdictions that responded to the question on STRs with data (and 1 jurisdiction that responded positively to a question on a proliferation financing investigation) are among the countries with more advanced economies, more advanced export control and/or proliferation financing systems. This can suggest, but does not prove, a correlation: countries with more advanced economies or major transit/transshipment hubs might have greater exposure to risks, and, at the same time, their more advanced control systems and private-sector awareness create more opportunities for detection. Second, while most jurisdictions did not receive any STRs relevant to proliferation financing, this does not guarantee that there is no false negative based on the fact that proliferators are extremely sophisticated in their evasion techniques. Continued outreach and awareness-raising targeted at the private sector are critical to mitigating the risks.

Summary

119. Based on country surveys from 16 GAFILAT jurisdictions, the regional picture for financial institutions is one of strong legal foundations paired with uneven, still-maturing implementation. The legal-regulatory framework for targeted financial sanctions, in line with the implementation of FATF Recommendation 7, is robust: 14 of 16 jurisdictions report frameworks in place. Similarly, legal frameworks for implementing UNSCR 1540 are also in place in most of the region. Oversight is similarly broad, as 15 jurisdictions supervise financial-institution compliance with targeted financial sanctions and 14 require STRs for proliferation financing.

120. National proliferation risk assessment lags behind the legal architecture. Only 9 jurisdictions have completed a national proliferation risk assessment, with 3 more are in progress. Only 10 require financial institutions to conduct their own institutional proliferation financing risk assessments. National and institutional proliferation financing risk assessments are among obligations under revised FATF Recommendation 1 to be assessed in the 5th-round Mutual Evaluations underway since 2024. Perceived regional risk is low and this may create a false sense of security. It is important to remember that proliferators use sophisticated evasion techniques and financial institutions can be exposed to proliferation financing risks even when sensitive goods do not physically cross their national territory.

121. At the level of financial institutions, all delegations reported that controls center on automated screening of customers against sanctions lists, drawing on the UN consolidated list and other unilateral lists. Screening is reinforced by customer due diligence, PEP identification, negative-media monitoring and, in more advanced systems, trade-finance document screening and dual-use-goods validation.

122. A notable pattern is over-compliance: many financial institutions, particularly subsidiaries of U.S., Canadian, and EU banks, and those wary of secondary sanctions or loss of correspondent banking, apply third-country lists beyond domestic requirements. While positive for proliferation financing controls, this can lead to uneven implementation and can generate tension between private-sector caution and national policy.

123. Detection and investigation of proliferation financing remains minimal: 14 jurisdictions reported no PF-related STRs and launched no investigations, with some limited activity concentrated in more advanced economies – a possible, but not confirmed, indicator of both greater exposure and stronger detection capacity.

4.1.3. Key Red Flags for Financial Institutions[47]



1. Designated-party and sanctions exposure

- **Sanctions-list match —** a customer, counterparty, beneficial owner, or signatory matches, or shares identifiers (address, phone, passport, email, virtual-currency address) with a name on the UN or unilateral (autonomous) sanctions lists.
- **DPRK or Iran nexus —** any direct or indirect connection, including transactions involving DPRK or Iranian financial institutions or state-owned entities.
- **Shared signatory —** the same individual acts as officer or signatory across multiple unrelated companies, a known DPRK representative-network indicator.

2. Customer profile and dual-use trade

- **Profile mismatch —** transaction size, frequency, or geography is inconsistent with the customer's stated business or industry.
- **Unverifiable controlled goods —** trade in dual-use or controlled items with no credible end-user, end-use certificate, or export license, or evasiveness when queried.
- **High-risk sectors —** defense, aerospace, nuclear technology, advanced chemicals, dual-use electronics, precision manufacturing, or maritime shipping.

3. Ownership opacity and front/shell companies

- **Opaque structures —** layered shell companies, nominee directors, or multi-jurisdictional arrangements with no legitimate commercial rationale.
- **Co-location —** unrelated companies share owners, addresses, phone numbers, or staff and transact in circular patterns.
- **Newly formed shell companies —** recently incorporated, thinly capitalized entities with no physical premises claiming to trade high-value or sensitive goods.

4. Geography and routing

- **High-risk jurisdictions —** transactions originate from, route through, or involve DPRK, Iran, or FATF grey-list or black-list jurisdictions.

[47] The Consolidated List of Red Flags for Financial Institutions with a list of references is available in Annex II (a). The list of key Red Flags—including the one in Annex II (a)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

- **Transshipment patterns —** goods or funds routed via known 'gateway' jurisdictions, with intermediate countries named as end-use destinations inconsistent with their commercial capacity.

5. Transaction and trade-finance anomalies

- **Structuring/layering —** multiple transactions below reporting thresholds, or circular flows that obscure origin and destination.
- **Trade-document discrepancies —** mismatches in goods description, HS code, quantity, or value (over/under-invoicing), or vague descriptions ("electronic components," "machinery," "chemicals").
- **Missing information —** absent or incomplete end-user certificate, or correspondent payments lacking originator/beneficiary data.

6. Maritime and shipping

- **AIS manipulation —** transponder switched off or spoofed, or location data inconsistent with stated port calls.
- **Ship-to-ship transfers —** transfers at sea or in free trade zones, especially of UN-sanctioned commodities (in DPRK's case - petroleum, coal, seafood, iron ore).
- **Identity changes —** unexplained change of vessel name, flag, owner, or operator, particularly where the prior identity had sanctions links.

7. Virtual assets, cyber, and customer conduct

- **Illicit crypto exposure —** wallets on the U.S. SDN list or linked to DPRK cyber groups (APT38/ Lazarus), or use of mixers, tumblers, or anonymity-enhancing tools.
- **Digital location anomalies —** login/transaction IP inconsistent with stated location or tied to a sanctioned jurisdiction; payment patterns matching DPRK overseas IT-worker typologies.
- **Evasive behavior —** contradictory due-diligence answers, undue urgency, or sudden account closure or fund transfer immediately after a sanctions alert or enhanced due diligence (EDD) request.

4.2. Dual-Use Sector



4.2.1. Global Risk

124. The dual-use industry encompasses actors involved in manufacturing and trading goods and technologies with dual-use applications. Proliferators cannot buy ready-made weapons on the open market; instead, they procure dual-use items that they can then use in their weapons programs.

125. The international community established international treaties and multilateral export control regimes (MECRs) to prevent the spread of WMDs and their delivery systems. The Nuclear Nonproliferation Treaty (NPT),[48] the Biological and Toxin Weapons Convention (BWC),[49] and the Chemical Weapons Convention (CWC)[50] exist to stop the proliferation of nuclear, biological, and chemical weapons. These instruments set obligations and guidelines for all Member States.

126. The multilateral export control regimes coordinate the enforcement of export controls on dual-use goods and technologies used to develop WMDs, delivery systems, and conventional weapons. Regimes such as the Nuclear Suppliers Group (NSG), the Australia Group, the Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement develop consensus-based control lists of dual-use items that governments should regulate to prevent proliferation and adopt best practices for export controls. The commitments undertaken within the MECRs are political in nature and do not constitute international legal obligations like those of a treaty. As part of national export control systems, countries adopt national control lists – items that are subject to licensing (permit) requirements. National control lists can rely, in part or in full, on the control lists associated with international treaties and multilateral

[48] NPT, https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140_sp.pdf.
[49] BWC, https://disarmament.unoda.org/es/our-work/weapons-mass-destruction/biological-weapons/biological-weapons-convention.
[50] CWC, https://www.opcw.org/sites/default/files/documents/CWC/CWC_es.pdf.

export control regimes. In countries with export controls, companies must apply to their governments for a license (permit) before engaging in trade transactions involving controlled goods. Globally, many jurisdictions have adopted the lists of MECRs, even without being members of those regimes.

127. A useful example of a consolidated list of dual-use goods can be found in the EU Dual-Use Items Control List.[51] This list incorporates goods contained in the four MECRs mentioned in the previous paragraph. The list is organized into 10 categories (Categories 0-9) and is updated regularly to reflect changes adopted in the MECRs.

Table 2. Examples of dual-use goods included in the MECRs[52]

1. Nuclear Suppliers Group (NSG)

Beryllium metal and alloys



Triggered spark gaps



Thermal ionization mass spectrometers



2. Australia Group

Fermenters



Special valves



[51] Annex I to Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02021R0821-20230526.

[52] Non-exhaustive list for illustrative purposes only.

3. Missile Technology Control Regime (MTCR)

Cruise missiles



Unmanned aerial vehicles



4. The Wassenaar Arrangement

Military vehicles, like battle tanks



Military electro-optical infrared systems



Advanced encryption products



128. In addition, international and unilateral (autonomous) sanctions regimes can prohibit trade in sensitive goods with specific jurisdictions.

129. Proliferators and agents acting on their behalf use a range of tactics to procure dual-use goods and technology in violation of export controls and sanctions. The following are some of the more common methods used.

Table 3. Select common methods of illicit procurement

Common method 1:

Proliferators can pretend that goods are obtained for domestic use. When a manufacturer receives what appears to be a domestic order, there is no need to apply to the government for an export license (permit), thereby buyers avoid additional scrutiny of the transaction.

Common method 2:

Proliferators can falsify end-use, end-user, and destination. For example, a buyer can state that an item is destined for a research lab at a university in jurisdiction A, when in fact the item will be transferred from jurisdiction A to jurisdiction B and used by a military institution in a WMD program. In such a case, the exporter will apply for an export license (permit) stating that the goods will be used solely for civilian purposes in Jurisdiction A.

Common method 3:

Proliferators can also choose to procure items that are slightly technically inferior, whose specifications are below the controlled threshold, and therefore they do not appear on the national control list. For example, a national control list includes a machine tool with a specifically identified high-rotor-speed rating. A proliferator can order a machine tool at a slightly lower speed that does not meet the controlled threshold and does not fall under the export license (permit) requirement. In such a scenario, an exporter will not apply for an export license (permit).

Common method 4:

Proliferators rely on front companies and agents in third countries to evade sanctions. For example, an order for goods will not come in the name of a designated entity or individual. Instead, a different entity or individual name will be used. Proliferators exploit jurisdictions with weak export controls as transit/transshipment points for illicitly procured goods. They also exploit free trade zones (FTZs) (free economic zones), as special provisions for FTZs designed to ease flow of trade also mean less oversight.

Common method 5:

Procurement agents can also buy used equipment, bypassing manufacturers, and instead targeting companies that either used the equipment themselves or are engaged in resale.

Common method 6:

Proliferators can transfer controlled technology, software, and technical data in intangible form.

Unlike a shipment of hardware, technology and software can be moved electronically — by email, file download, cloud storage, or remote access to a server. For example, a technical expert can upload controlled design specifications, source code, or manufacturing data to a cloud server and grant access to a recipient in another jurisdiction or transmit the files directly by encrypted email. Intangible transfer can also occur through the provision of technical assistance, training, or know-how — including to a foreign national located within the supplier country (a “deemed export”) — whereby knowledge is conveyed without any item ever crossing a national border.

130. Financial institutions serve a wide range of actors in the dual-use sector, including manufacturers, traders, shippers, brokers, and others. In cases of illicit procurement of sensitive items, manufacturers,

traders, and brokers of dual-use goods, as well as financial institutions, unintentionally become involved in proliferation schemes.

131. Beyond proliferators' evasion techniques, financial institutions face a serious capacity limitation in identifying financial transactions linked to the illicit procurement of dual-use goods and technology. The information financial institutions see, such as parts of the wire description, provides only a vague idea of the goods involved, such as "spare parts," "repair equipment," and so on. Without additional effort, it is unclear whether the goods in question are sensitive, subject to export controls (if any exist in a given jurisdiction), or part of a legitimate trade transaction. Even when more information is available about a product, compliance teams will, in most cases, be unable to determine whether it is dual-use because they lack the technical expertise.

132. The amounts typically involved in proliferation financing do not involve a defined monetary threshold and are consistent with legitimate commercial trade. This means that, unlike money laundering, which usually involves large amounts, proliferation financing has no amount thresholds for detection.

4.2.2. Regional Risk

133. In total, 16 GAFILAT jurisdictions responded to the distributed country survey. The survey included questions on the dual-use industry, export control systems, and guidance on proliferation financing for the manufacturers of dual-use goods.

134. Based on the data received, the following patterns emerge. The majority of GAFILAT jurisdictions are not major producers of dual-use goods and technology. In the region, 4 jurisdictions can be considered significant users of dual-use goods and technology – Argentina, Brazil, Chile, and Mexico.[53] All jurisdictions have exposure to some dual-use goods and technology by virtue of handling radioactive and nuclear material, chemical, and biological components. These items are used in various sectors, including nuclear science, medicine, agriculture, and others.

135. Although the region is not among the major producers of sensitive goods, the risks and vulnerabilities associated with dual-use goods and technology remain. First of all, all countries in the region rely on dual-use goods and materials and must either produce or import them. Therefore, sensitive goods are present in the region. Second, several countries have relevant sectors, and it is expected that the share of the dual-use production sector in the region will gradually increase. Third, several jurisdictions are major transit and transshipment hubs, meaning a high volume of cargo, including sensitive goods, passes through their territories. Finally, the presence of numerous Free Trade Zones (free economic zones, special economic zones, etc.) increases exposure to illicit goods movement.

Lack of export control systems on dual-use goods and technology

136. While some GAFILAT jurisdictions have developed robust, comprehensive, and effective control systems for the export of sensitive and dual-use materials, these remain the exception in the region.

[53] Ecuador and Honduras reported presence of limited dual-use sector.

137. Argentina's export control system for sensitive materials, military goods, and dual-use items is based primarily on Decree No. 603/1992, which establishes the Regime for the Control of Sensitive Exports and Military Materials and defines the core functions of the National Commission for the Control of Sensitive Exports and Military Materials (CONCESYMB). This is a tripartite body comprising the Ministries of Foreign Affairs, International Trade and Worship; Defense; and Economy, with the participation of technical agencies specializing in each of the controlled technologies, as well as the Customs authority. Argentina requires a license for the export of sensitive goods. As the only developing country participating in all four major multilateral export control regimes - the Australia Group, the Nuclear Suppliers Group, the Missile Technology Control Regime, and the Wassenaar Arrangement- and, additionally, in the Zangger Committee, its national control lists reflect the lists agreed upon in those forums and are updated periodically.

138. Brazil's main legal foundation for its export control system is *Law No. 9,112 (1995)*,[54] which established measures governing the export of sensitive items and related technologies and created the Interministerial Commission for the Control of Exports of Sensitive Goods (CIBES). Brazil requires licensing of trade operations involving sensitive goods. The implementing regulations on the issuance of licenses, permits, certificates, and other documents are codified in CIBES *Resolution No. 40 (2025)*.[55] Brazil's national control list focuses on items from two out of four multilateral export control regimes of which it is a member – the Chemical Weapons Convention, the Biological and Toxin Weapons Convention, the Nuclear Suppliers Group, and the Missile Technology Control Regime. While Brazil is not a member of the Australia Group, the items that appear on the Australia Group's control list are substantively covered in Brazil's national control list. The biological list includes microorganisms (including added indigenous microorganisms) and equipment for the production of biological and toxin weapons, while the chemical list includes equipment for the production of dual-use chemicals. These goods do not appear on the control lists of the Chemical Weapons Convention or the Biological and Toxin Weapons Convention. In this regard, the lists were created to comply with the provisions of United Nations Security Council Resolution 1540.

139. Mexico regulates sensitive and dual-use exports administratively through the Ministry of Economy. In 2011, Mexico adopted an "Accord" (*Acuerdo por el que se sujeta al requisito previo*[56]) establishing an export control system for sensitive goods. Mexico's national control list includes items from three (out of four) multilateral export control regimes of which Mexico is a member – the Wassenaar Arrangement, the Australia Group, and the Nuclear Suppliers Group. Mexico's Ministry of Economy is the licensing authority.

140. Panama has developed and adopted legislation to establish an export control system. The export control system is based on the *Executive Decree No. 81 (2017)*,[57] which provides measures to control the trade and safe transportation of dual-use material for national and international security reasons.

---

[54] *Law No. 9,112 (1995),* https://www.planalto.gov.br/ccivil_03/leis/l9112.htm.

[55] *Resolution No. 40 (2025),* https://antigo.mctic.gov.br/mctic/opencms/legislacao/outros_atos/resolucoes/Resolucao_Cibes_n_40_de_28042025.html.

[56] *Agreement subjecting to a prior requirement from the Ministry of Economy the export of conventional arms, their parts and components, dual-use goods, software and technologies susceptible to diversion for the manufacture and proliferation of conventional weapons and weapons of mass destruction* (2011), https://dof.gob.mx/nota_detalle_popup.php?codigo=5196224.

[57] *Executive Decree No. 81 (2017),* https://www.amp.gob.pa/decreto-ejecutivo-81-de-2017/.

Panama also passed *Resolution 001 (2018)*,[58] which incorporates the European Union's Dual-Use Items Control List into Panama's National Harmonized List of Dual-Use Goods. The National Council for Trade and Safe Transportation and the Technical Committee for Trade and Safe Transportation were created by *Decree No. 81 (2017)*, which established measures to control the trade and safe transportation of dual-use materials for national and international security reasons, in accordance with UNSCR 1540.

141. In Chile, the National Congress is currently processing the corresponding bill.

142. All jurisdictions have some controls in place for safety and security reasons, primarily on goods and materials that can be considered hazardous, such as nuclear/radioactive materials, chemical and biological materials, explosives, and so on.

143. We use the example of El Salvador to illustrate how even when countries do not have a dedicated single law on export control of sensitive goods, components of relevant controls can be found in different pieces of legislation and institutional practices. For example, *the Law on the Control and Regulation of Weapons, Ammunition, Explosives, and Similar Items* regulates the import, export, manufacture, and commercialization of firearms, ammunition, and products for similar use intended for military or police purposes.[59] *Law on the Control and Regulation of Regulation on Narcotic Drugs, Psychotropic Substances, Precursors, Chemical Products, and Related Products* regulates import and export of such items.[60] *Law on the Protection of Plant Health, Animal Health and Safety of Unprocessed Food of Animal and Plant Origin*[61] regulates the entry, transport, and movement of plants, animals, and their product and by-products. *The Law on the Control of Pesticides, Fertilizers, and Agricultural-Use Products*[62] regulates import and transport of fertilizers. Several Customs-related pieces of legislation, such as the *Customs Simplification Law*,[63] the *Organic Law of the General Directorate of Customs*,[64] and the *Central American Uniform Customs Code*,[65] establish and regulate Customs procedures and enforcement rules. Institutionally, the Import and Export Processing Center of the Central Reserve Bank (CIEX) facilitates export and import permits, including those for dual-use goods. While there is no single list for dual-use goods, CIEX refers to the competent institutions depending on the nature of the product. The Ministry of Defense authorizes the import and export of weapons, explosives, ammunitions, military equipment,

[58] *Resolution 001 (2018)*, https://vlex.com.pa/vid/resolucion-n-001-adopta-737311125.

[59] *Law on the Control and Regulation of Weapons, Ammunition, Explosives, and Similar Articles*, 1999, https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/1990-1999/1999/07/8889A.PDF.

[60] *Regulation on Narcotic Drugs, Psychotropic Substances, Precursors, Chemical Products, and Related Products*, 2013, https://www.srs.gob.sv/wp-content/uploads/2022/09/REGLAMENTO-DE-ESTUPEFACIENTES-PSICOTROPICOS-PRECURSORES-SUSTANCIAS-Y-PRODUCTOS-QUIMICOS-Y-AGREGADOS.pdf.

[61] *Law on the Protection of Plant Health, Animal Health and Safety of Unprocessed Food of Animal and Plant Origin*, 2025, https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2020-2029/2025/05/10A158.PDF.

[62] *The Law on the Control of Pesticides, Fertilizers, and Agricultural-Use Products*, 1973, amended, https://www.ecolex.org/es/details/legislation/decreto-legislativo-no-315-ley-sobre-control-de-pesticidas-fertilizantes-y-productos-para-uso-agropecuario-texto-refundido-lex-faoc105134/.

[63] *Customs Simplification Law*, 1999, https://transparencia.mh.gob.sv/downloads/pdf/DC5117_36_Ley_de_Simplificacion_Aduanera.pdf.

[64] *Organic Law of the General Directorate of Customs*, 2005, https://infotrade.minec.gob.sv/wp-content/uploads/48_Ley_Organica_de_la_Direccion_General_de_Aduanas.pdf.

[65] *Central American Uniform Customs Code*, 2008, https://www.transparenciafiscal.gob.sv/downloads/pdf/DC5085_2_Codigo_Aduanero_Uniforme_Centroamericano_(CAUCA).pdf.

dual-use products, chemical substances, or hazardous materials if they are related to military use. The Superintendency of Health Regulation issues permits for import and export for regulated products, including hazardous chemicals. The Ministry of Agriculture and Livestock issues authorizations for the import of biological agrochemicals.

144. The absence of, or the nascent stage of, export controls for dual-use goods and technology in the majority of GAFILAT jurisdictions may constitute a relevant regional vulnerability. The lack of dedicated export control systems means there is no legal basis to screen, license, or deny exports, imports, or other transactions involving dual-use goods and technology.

Registration of producers of dual-use goods and technology

145. One of the best practices for national export control systems is to require producers of dual-use goods and technology to register with the government. This requirement is separate from the license (permit) requirements for trade transactions. The absence of producer registration is meaningful only where there is an actual dual-use industry. In jurisdictions with almost non-existent or non-significant dual-use industry, the absence is expected and is not a vulnerability.

146. In the GAFILAT region, only Argentina,[66] Brazil and Mexico – 3 jurisdictions with significant dual-use industries – require producer registration in a meaningful sense; Ecuador and the Dominican Republic also reported a requirement, though neither has a significant dual-use sector. The majority of jurisdictions, including some with significant dual-use industries, reported no requirements for registration for dual-use goods producers, which is unsurprising given the lack of advanced dual-use sectors and export control systems. Some jurisdictions reported registration requirements that are partially relevant. For example, Bolivia requires importers of materials related to dual-use products to register and request an import authorization from STN-OPAQ and AETN. Honduras, like other jurisdictions without advanced export control systems for dual-use goods and technology, regulates chemical precursors, radioactive materials, and radiation-emitting equipment, and reported that companies that use the above-mentioned items should be registered with the government. Similarly, Ecuador reported relevant registration requirements that, given its lack of a comprehensive export control system for dual-use goods and technology, likely apply to specific categories of goods (e.g., ammunition).

Siloing of export controls and financial crime prevention authorities

147. Another layer of vulnerability lies in the disconnect between export control authorities and financial crime prevention authorities. In the GAFILAT region, formal information-sharing mechanisms between export control authorities and financial crime prevention authorities are largely lacking. Several factors can contribute to this lack of efficient communication, including information protection regulations (e.g., banking secrecy), technological incompatibility between authorities, low state-level priority, or a lack of developed joint processes.

[66] In Argentina, producers in dual-use industries must be registered and licensed according to the technology involved: nuclear (ARN - Nuclear Regulatory Authority) or chemical (REARQUIM - Chemical Weapons Registry of the Argentine Republic).

148. The country survey asked about procedures, platforms, or other mechanisms for information-sharing between export control authorities and authorities responsible for preventing financial crimes. Before assessing the patterns that emerged from the responses, it is worth noting that platforms for regular exchange of information between Customs and financial authorities, for example, on import/export declarations, are not the same as a dedicated information-sharing tool specifically designed to combat proliferation financing and export control violations.

149. In total, 15 jurisdictions responded to a question about procedures, platforms, or other mechanisms for information-sharing between export control authorities and financial crime prevention authorities.

150. In Argentina, the General Customs Directorate (ARCA) is a reporting entity before the Financial Intelligence Unit (UIF) under Article 20 of *Law 25,246* and UIF *Resolution 38/2011*, but this represents a general Customs-to-FIU reporting obligation, not a dedicated export control/proliferation financing information-sharing platform.

151. In Bolivia, several inter-institutional cooperation agreements exist that can facilitate relevant information-sharing, including (1) National Customs Office-Bolivian Police (Anti-Narcotics Force) that provides mechanisms for access to and exchange of information; (2) National Customs Office-Bolivian Police (Special Crime Fighting Force) have coordination mechanisms for information-sharing and technical/operational cooperation; (3) FIU-Customs interinstitutional agreement that provides access to and exchange of import/export declaration data, goods declaration forms, and sworn-declaration information on cross-border currency movements; (4) FIU-Ministry of Defense joint action protocol that provides guidelines and coordination mechanisms for the analysis of information on terrorism financing and proliferation financing.

152. Brazil has a mechanism that directly supports information sharing between export control authorities and financial crime prevention authorities. The General Coordination of Sensitive Goods (CGBS) under the Ministry of Science, Technology, and Innovation (MCTI), responsible for Brazil's export control policy for sensitive goods, is authorized to use the Electronic Exchange System (SEI-C). This platform is managed by COAF, Brazil's FIU, administratively linked to the Central Bank of Brazil. The platform enables the sharing of financial intelligence information with competent authorities, including export control officials. The legal provisions for the information-sharing are supported by *Law 9.112/1995*, *Decree 4.214/2002*, and Central Bank of Brazil *Resolution 427/2024*.

153. In Colombia, the National Tax and Customs Directorate (DIAN) maintains coordination with the Financial Information and Analysis Unit (UIAF), the Office of the Attorney General (FNG), and the Fiscal and Customs Police (POLFA), as well as other competent authorities through national cooperation forums and mechanisms. DIAN is also in the process of implementing specialized platforms for secure information management promoted by the World Customs Organization, including the RILO (Regional Intelligence Liaison Office).

154. The Dominican Republic has mechanisms for information exchange among competent authorities regarding AML/CFT/CPF, particularly through the coordination of export and import authorities. Generally, obligated entities have no direct procedures, platforms, or communication channels with the authorities responsible for controlling the export of tangible or intangible goods, as such coordination is managed institutionally among competent authorities under the prevailing legal framework, as necessary.

155. In Ecuador, working groups work with the National Customs Service of Ecuador (SENAE) to establish formal mechanisms for information exchange.

156. In El Salvador, no dedicated export control-financial crime information-sharing platform exists. However, as in other jurisdictions, relevant legal provisions provide a foundation for relevant information exchange. For example, Article 52 of the *Special Law for the Prevention, Control, and Sanction of Asset Laundering, Terrorism Financing, and Proliferation Financing of Weapons of Mass Destruction* obligates state agencies to cooperate. Inter-agency coordination exists among the Financial Intelligence Unit, Attorney General's Office, National Civil Police, Ministry of Public Security and Justice, General Directorate of Customs, Ministry of National Defense, Maritime Authority, and the National Registry Center (responsible for real estate, company incorporation registries), as well as with an external body - INTERPOL.

157. Guatemala does not have a dedicated export control system. Similar to other jurisdictions, legal provisions for relevant but not all-encompassing information-sharing can be found under specific agreements. For example, (1) the Tax Administration Superintendency (SAT) and IVE (Financial Intelligence Verification Entity) exchange intelligence information under an Interinstitutional Cooperation Agreement signed on November 26, 2004, covering prevention of tax violations, money laundering, and related crimes; (2) A July 18, 2023 agreement between the Guatemalan Migration Institute (IGM), Superintendency of Banks (SIB), and SAT established mechanisms for sharing information via an interconnected IT system on persons transporting USD 10,000 or more in cash. The IVE has legal authority to request information from any public or private entity under Articles 28 and 34 of the *Law Against Money Laundering or Other Assets*.

158. Honduras responded "Yes" to the question on the information exchange between export control authorities and authorities responsible for preventing financial crimes, but without elaboration.

159. Mexico has a mechanism that meets the direct purpose of information-sharing between export control authorities and financial crime prevention authorities. Under the agreement establishing CANDESTI (the inter-agency committee for strategic trade controls), one of CANDESTI's functions is to establish rules for the exchange of reports, data, and technical cooperation relevant to Mexico's international obligations on matters of disarmament, terrorism, and international security. Through CANDESTI's various working groups, different agencies have procedures and platforms for exchanging information between export control and financial crime prevention authorities.

160. Nicaragua does not produce dual-use goods or technology. However, it has a mechanism that can be used for relevant information exchange. In 2024, the Presidential Council for Coordination, Cooperation, and Information Exchange, which includes the General Directorate of Customs Services as an export control body and the National Police as the financial crime prevention authority, signed an *Inter-Institutional Agreement No. 01-2024*. This is a protocol for Coordination, Cooperation, and Information Exchange for the prevention, combat, and prosecution of organized crime, drug trafficking, money laundering, terrorism financing, proliferation financing of WMDs, and other related crimes.

161. Panama has mechanisms that allow export and re-export operations to be traced through the Commercial Movement Document, which the National Customs Authority monitors. Nevertheless, it is essential to strengthen information-sharing and inter-agency coordination between the authorities responsible for export controls and those responsible for preventing financial crime.

162. In Paraguay, interinstitutional agreements allow information exchange between the National Directorate of Tax Revenue (Customs Directorate General) and SEPRELAD (FIU). SEPRELAD has access to the databases of the National Directorate of Tax Revenue (DNIT) for intelligence purposes, which enables filtering of information on persons, jurisdictions, activities and traded goods. For nuclear and radiological goods specifically, the Radiological and Nuclear Regulatory Authority maintains a list of controlled materials that is shared with the Customs to help identify sensitive materials and has access to the importer's single-window system.

163. In Peru, Customs can share information with the FIU through Suspicious Transaction Reports (STRs), but no dedicated platform exists for information exchange between export control authorities and financial crime prevention authorities. Customs agents are reporting entities and may submit STRs to the FIU through the PLAFT (Portal de Prevención de Lavado de Activos y Financiemento del Terrorismo) portal. The FIU may also request information from Customs agents through the same portal.

164. In Uruguay, information sharing can take place within the framework of the TF/PF Working Group, which meets semiannually and holds extraordinary sessions when issues of interest arise.

165. In sum, most GAFILAT jurisdictions lack dedicated procedures, platforms, or mechanisms for information-sharing between export control and financial crime prevention authorities. Even where relevant agreements exist, they are often general Customs cooperation tools rather than dedicated frameworks for preventing the illicit procurement and movement of sensitive goods. This siloing creates a critical vulnerability: if a transaction does not trigger a financial Red Flag but involves a sensitive product going to a sanctioned or proliferation-sensitive destination, or vice versa, it may pass undetected through both systems. The lack of coordination among these key authorities in the CPF system reduces the state's ability to detect proliferation indicators. Taken in isolation by each authority, these indicators may not be enough to prompt action but analyzed together they would reveal a significant risk.

166. Only a few jurisdictions have dedicated procedures, platforms, or mechanisms for information-sharing between export control authorities and financial crime prevention authorities. As a rule, they are present in jurisdictions with comprehensive export control systems on dual-use goods and technologies.

167. Several jurisdictions reported legal requirements, procedures, and mechanisms that, while not designed specifically for information-sharing between export control authorities and financial crime prevention authorities on dual-use goods and technology, could serve as a foundation for such information-sharing if/when governments decide to do so. For example, several jurisdictions reported having more general information-sharing mechanisms, such as on cash movements, broader legal obligations for relevant authorities to cooperate, and legal requirements for Customs agents to submit Suspicious Transaction Reports.

168. The main recommendation for GAFILAT jurisdictions in this context is to consider export controls and financial crime prevention as mutually reinforcing systems that would benefit from clear procedures, mechanisms, and platforms for information sharing.[67] Jurisdictions can think of how to use existing legal provisions, procedures, mechanisms and platforms for such information exchange.

[67] Togzhan Kassenova, "Challenges with Implementing Proliferation Financing Controls: How Export Controls Can Help," *World ECR: The Journal of Export Controls and Sanctions*, May 2018, https://carnegieendowment.org/posts/2018/05/challenges-with-implementing-proliferation-financing-controls-how-export-controls-can-help.

Geographic factors

169. One additional factor that is also relevant to the discussion of vulnerabilities associated with dual-use goods and technology: (1) the volume of cargo being transited or transshipped through a jurisdiction; and (2) the presence of Free Trade Zones. Even if a jurisdiction is not a major producer of dual-use goods and technology, its territory can be used to transfer sensitive goods. Both factors are extremely relevant to the regional risk profile. The GAFILAT region is home to major transit/transshipment hubs and many FTZs. FTZs are particularly vulnerable to being exploited by proliferators for illicit transfers of goods. These factors will be discussed in detail in the subsequent sections of the report.

Summary

170. The region is, for the most part, not a major producer of dual-use goods and technology: only four jurisdictions — Argentina, Brazil, Chile, and Mexico — can be considered significant users, though every jurisdiction has some exposure by virtue of handling radioactive and nuclear material and chemical and biological components across sectors such as nuclear science, medicine, and agriculture. The absence of major production does not eliminate the risk. All countries rely on dual-use goods and must either produce or import them, so sensitive items are present throughout the region; several jurisdictions have relevant sectors whose share of production is expected to grow gradually; and a number serve as major transit and transshipment hubs, meaning high volumes of cargo — including sensitive goods — pass through their territories. The presence of numerous free trade zones further increases exposure to the illicit movement of goods.

171. Only a few jurisdictions have established comprehensive export control systems for dual-use goods while all jurisdictions maintain some safety- and security-based controls on hazardous goods such as nuclear, radioactive, chemical, and biological materials and explosives. The absence or nascent stage of dedicated export controls across most of the region is a fundamental vulnerability, because without such systems, there is no legal basis to screen, license, or deny transactions involving dual-use goods. A related gap is producer registration, a recognized best practice: only three jurisdictions require it in a meaningful sense.

172. Another vulnerability is the siloing of export control authorities and financial crime prevention authorities. Only Brazil and Mexico have mechanisms built for this direct purpose — Brazil through the Electronic Exchange System (SEI-C) managed by its FIU, COAF, and Mexico through the inter-agency CANDESTI committee and its working groups — and, as a rule, such mechanisms appear in jurisdictions that already operate comprehensive export control systems. Elsewhere, the arrangements that exist are largely general customs-cooperation or FIU-reporting tools — cash-movement reporting, broad statutory duties to cooperate, or Suspicious Transaction Report obligations for Customs agents — rather than frameworks designed to detect the illicit procurement and movement of sensitive goods. This siloing is a critical vulnerability: a shipment of sensitive goods bound for a sanctioned or proliferation-sensitive destination may clear Customs without raising concern if its financing looks routine, while a payment that raises a financial Red Flag may never be linked to the goods it pays for. In either case, the warning sign visible sign to one authority never reaches the other, and the transaction may pass undetected through both systems. The lack of coordination among these key authorities in the CPF system reduces the state's

ability to detect proliferation indicators. Taken in isolation by each authority, these indicators may not be enough to prompt action but analyzed together they would reveal a significant risk. These vulnerabilities are compounded by geography — the region's role as home to major transit and transshipment hubs and to many free trade zones, the latter being particularly susceptible to exploitation for illicit transfers.

173. The main recommendation is that jurisdictions treat export controls and financial crime prevention as mutually reinforcing systems and build clear information-sharing procedures, drawing where possible on existing legal provisions.

4.2.3. Key Red Flags for Illicit Procurement of Sensitive Goods[68]



1. Customer and end-user profile

- Customer, consignee or address closely resembles a party on a restricted-party list (UN sanctions list, national denial list, lists of unilateral sanctions regimes, others).
- Stated end-use is civilian, but the end-user is linked to the military, the defense industry, or a government research body — or a purported civilian end-user's address is found to be a military facility or co-located with military facilities in a country of concern.
- Recently incorporated company, hard to verify in open sources and with little or no web presence, based in a known diversionary or transshipment jurisdiction, that is unfamiliar with the product's performance characteristics but still wants it.

2. End-use and end-use plausibility

- Stated end-use is implausible, or the customer gives an unconvincing explanation of the technical sophistication of the items or the extent to which they are needed in its normal business.
- Order is inconsistent with the customer's needs or apparent scale of operations, or an order for "parts" or "components" is sufficient to service far more controlled end-items than the destination is known to possess.
- A diversion of the stated end-use is perceived or suspected.

3. Item and technical mismatch

- Item is incompatible with the destination's technical level, or product capabilities do not fit the buyer's line of business.
- Customer requests a product that is overly capable for the stated application, or unusual customization or modification requests raise concerns about the potential applications of the modified product.

[68] The Consolidated List of Red Flags for Dual-Use sector with a list of references is available in Annex II (b). The list of key Red Flags—including the one in Annex II (b)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

- Item has known dual-use, military or otherwise sensitive applications, or is a leading-edge product attractive to proliferators (still being developed, few domestic customers, or technically superior to established competitors).

4. Shipping, routing, and logistics

- A freight-forwarding firm is listed as the product's final destination, consignee, or final end customer, or the stated end-user is a trading company, distributor, or entity based in a Free Trade Zone, so the true final destination is unknown.
- Shipping route is abnormal for the product and destination; the transaction routes through, or payment originates from, a third country not otherwise involved and known as a transshipment point; or there is a last-minute change in shipment or payment routing previously scheduled to or from a country of concern.
- Delivery dates are vague or planned for out-of-the-way destinations; usual incoterms, container/truck sealing, or consignee/end-user confirmation of receipt are refused; or a maritime customer uses corridors known as transshipment routes.

5. Documentation, behavior and licensing

- When questioned, the buyer is evasive or unclear about whether the item is for domestic use, export or re-export; declines routine installation, training or maintenance; or requires unusual or excessive confidentiality regarding destinations, customers, or item specifications.
- Complex or layered arrangements appear designed to conceal a party's involvement or obscure the ultimate destination — for example, layered letters of credit, front companies, or unnecessary intermediaries and brokers.
- Uncertainty exists about an item's license history (a required license was not, or would not likely be, obtained), or a request is received to service, install or upgrade an item altered after export for a more advanced end-use that would normally require a license.

6. Ownership, affiliation and sanctions-network nexus

- A new customer's senior management or technical leadership overlaps with an entity on a restricted-party list, or counterparties are physically co-located with, or share ownership with, such a party.
- A new customer requests an item or service that was originally designed or modified for a customer that is now designated, suggesting the new customer has assumed the listed entity's operations.
- A foreign party to the transaction has one or more owners on the restricted-party list, triggering an affirmative duty to determine ownership percentage.

7. Financing and payment

- Customer significantly overpays relative to known market prices, is offered unusually favorable payment terms or pays in advance, or pays cash for a very expensive item when the terms of sale would normally call for financing.
- Payment is made by a party other than the customer or stated intermediary, or from an entity in a third country not party to the transaction; or multiple smaller-value payments are made from a single end-user's foreign bank account to several similar suppliers.
- A purchase under a letter of credit is consigned to the issuing bank rather than the actual end-user, or supporting documents do not identify the true end-user; or open accounts/lines of credit are used in conjunction with known transshipment jurisdictions.

4.3. Maritime industry[69]



4.3.1. Global Risk

174. The maritime industry is exposed to WMD proliferation and proliferation financing. Proliferators use maritime transport to move sensitive goods for illicit procurement, and they also move non-sensitive cargo for fundraising (selling commodities to generate funds). High container traffic, complex logistics chains, and extensive reliance on intermediaries create "screening gaps" that proliferators and evaders of sanctions and export controls can exploit. Seaports are potentially attractive for trade-based money laundering and, by extension, proliferation financing. Illicit networks can manipulate trade flows by over- or under-invoicing, multiple invoicing, phantom shipments, and complex routing while exploiting permissive ecosystems around ports.

175. About 80% of international trade is transported by sea, meaning most illicitly obtained sensitive goods are moved by vessels. Sea containers are frequently exploited for illicit trafficking, given the volume of containerized trade and low physical-inspection rates. Documented categories include sensitive and dual-use goods such as chemical precursors, chemical, biological, radiological, and nuclear materials, and controlled advanced electronics.[70] Trafficking and other unauthorized movements of nuclear and other

[69] Any reference to this term in this document also includes the inland navigation sector, including inland ports and waterways.

[70] UNODC–WCO Container Control Programme (CCP), UNODC/World Customs Organization. The CCP was established to reduce the risk of shipping containers being exploited for illicit drug trafficking, transnational organized crime, and other forms of black-market activity, and its thematic scope has expanded to include dual-use and strategic goods, CBRNe materials, weapons and their means of

radioactive material across borders are documented and monitored at the international level.[71] Physical inspection of *all* cargo is not feasible for any seaport in the world, as it would bring international trade to a halt.[72] This places extreme importance on screening – identifying high-risk cargo through due diligence, including document checks, analysis of parties involved, vessel profiles, and so on.

176. The global structure of the maritime industry complicates efforts to manage these risks. Ships, ports, freight forwarders, and insurers are often based in different countries, making oversight difficult. The ownership and operation of vessels are often fragmented, making it difficult to identify the true beneficial owner. A vessel can be registered under one flag, owned by a company in another jurisdiction, managed elsewhere, and crewed by international personnel. Additionally, parties that control vessels, including sanctioned countries and entities, can conceal their involvement through front companies, shell companies, and nominees to hide vessel ownership or charter agreements. The use of flags of convenience — registering a vessel in a country different from the owner's — adds another layer of anonymity. For instance, vessels controlled by the DPRK often fly the flags of other jurisdictions. Other evasion tactics include changing the physical look of ships, spoofing or laundering vessel identities, or disabling automated identification systems (AIS).

177. Financial institutions are at risk of secondary exposure to proliferation financing through the processing of payments for vessel purchases, fuel, port fees, and other transactions. When financial institutions facilitate transactions for vessels engaged in sanctions evasion, they inadvertently aid the proliferation.

178. FATF specifically notes the exploitation of the maritime sector as a proliferation financing typology. In its 2025 report *Complex Proliferation Financing and Sanctions Evasion Schemes*, FATF stated: "the maritime sector has become a primary target used by illicit actors, leveraging its complexity, international reach, anonymity, and limited AML/CFT/CPF controls."[73]

179. Even jurisdictions without major production of dual-use goods and technology can be exposed to proliferation risks if they serve as major transit and transshipment hubs. Proliferators often use third jurisdictions for transit and transshipment of illicitly procured sensitive goods, especially if these hubs do not have comprehensive export control systems. Jurisdictions without export control systems have only limited checks on sensitive cargo passing through their national territories.

4.3.2. Regional Risk

180. The assessment of regional risk on the maritime front relies on data provided by jurisdictions in response to country surveys and on open-source analysis. The relevant section of the country survey

delivery, and chemical precursors to drugs and explosives. https://www.unodc.org/unodc/en/drug-trafficking/container-control-programme.html.

[71] IAEA Incident and Trafficking Database (ITDB), IAEA. The ITDB is the IAEA's information system on incidents of illicit trafficking and other unauthorized activities involving nuclear and other radioactive material outside of regulatory control, recording 4,243 incidents between 1993 and 2023, a subset of which involve confirmed or likely trafficking or malicious use, https://www.iaea.org/resources/databases/itdb.

[72] For example, in the United States, only about 3% of ocean traffic gets inspected. "The Difference Between Cargo Screening Vs. Inspection," November 22, 2019, https://www.greenworldwide.com/the-difference-between-cargo-screening-vs-inspection/.

[73] *Complex Proliferation Financing and Sanctions Evasion Schemes*, FATF, 2025, p. 46.

focused on the availability on whether jurisdictions were major transit/transshipment hubs, the availability of a Flag of Convenience ("open registry"), the number of vessels registered under the country's flag, PF/sanctions risk assessment during the licensing process, and government training and guidance on proliferation financing and sanctions evasion to the maritime industry.

181. The GAFILAT region's risk profile for the maritime industry and transit/transshipment routes is mixed. On the one hand, the region is geographically farther from key proliferant states, the DPRK and Iran. On the other hand, the region is home to some major seaports and several jurisdictions can be classified as major transit/transshipment hubs.

182. GAFILAT member jurisdictions' ports are not among the world's largest, but they serve some of the world's busiest Atlantic and Pacific maritime corridors, and significant amounts of cargo pass through them. The region's largest container ports are located in Brazil, Panama, Mexico, and Colombia. In 2024, Brazil's Santos handled 5,484,829 TEU, placing it #37 in the global port rankings.[74] Panama's Colón complex processed 5,395,134 TEU, placing it #41 in the world[75] and its Balboa complex processed 4,013,685 TEU, placing it #50 in the world.[76] Mexico's Manzanillo port handled 3,924,501 TEU, placing it #52 in the world.[77] Colombia's Cartagena port processed 3,701,044 TEU in 2024, placing it #58 in the world.[78] Importantly, most of these ports showed an upward trend in cargo volume. It is reasonable to assume that the total volume of cargo passing through the region's ports will continue to increase.

183. Several jurisdictions are major transit or transshipment hubs. Among them: Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Mexico, Panama, Paraguay, and Peru. Uruguay is a regional transit/transshipment hub. Guatemala, Honduras, El Salvador can be considered transit hubs based on the availability of land-based transit corridors. Bolivia and Nicaragua do not have significant transit throughput.

184. In total, 12 jurisdictions provided responses to all questions on the Maritime Sector in the country survey. Additionally, 2 jurisdictions provided responses to some questions.

185. One proliferation risk component for the maritime sector is the availability of the Flag of Convenience or "open registry." A flag of convenience is a situation in which a ship is registered in a country other than the one where its owner resides or holds citizenship. This is also often referred to as an "open registry." The International Transport Workers' Federation and other expert sources list Panama, Bolivia, and Honduras as having a Flag of Convenience.[79]

186. Bolivia, Dominican Republic, and Honduras responded with "Yes" to the country survey question on the Flag of Convenience. Bolivia is landlocked, which means its vessels under the Flag of Convenience operate entirely outside its territory and physical oversight. At the same time, Bolivia's fleet is relatively

[74] "37 – Santos (Brazil)," August 19, 2025, https://www.lloydslist.com/LL1154196/37-Santos-Brazil.

[75] "41 – Colón (Panama)," August 12, 2024, https://www.lloydslist.com/LL1149208/41-Coln-Panama.

[76] "50 – Balboa (Panama)," August 19, 2025, https://www.lloydslist.com/LL1153978/50-Balboa-Panama.

[77] "52 – Manzanillo (Mexico)," August 19, 2025, https://www.lloydslist.com/LL1153979/52-Manzanillo-Mexico.

[78] "58 – Cartagena (Colombia)," August 19, 2025, https://www.lloydslist.com/LL1154197/58-Cartagena-Colombia.

[79] "Current Registries Listed as FOCs," International Transport Workers' Federation, https://www.itfseafarers.org/en/issues/flags-of-convenience/current-registries-listed-focs.

small, and no confirmed cases of misuse of the Bolivian flag for sanctions evasion were reported. A Honduras-flagged FT Island (HQAI6) crude oil tanker was included on an autonomous designations list for violation of unilateral sanctions on Iran.[80]

187. Panama's open registry is known as the "Panama International Ship Registry." With 8,602 registered vessels,[81] this jurisdiction is a major player in the global maritime system. In the past, Panamanian-flagged vessels were used to evade sanctions. To give one example, among the DPRK sanctions-evasion cases, the UN Panel of Experts documented the case of *Dong Thanh*, a Panama-flagged vessel used to illicitly transfer DPRK coal.[82] Panama has made significant efforts in protecting its flag. In 2006, the General Directorate of Merchant Marine of the Panama Maritime Authority adopted *Resolution No. 106-36-DGMM* (dated 16 November 2006), mandating full compliance with United Nations Security Council Resolution 1718 (2006). As part of this measure, a policy was established to reject any application to register vessels originating from the DPRK or vessels flying its flag; this was one of the first measures Panama adopted to prevent its maritime registry from being used to facilitate activities linked to the DPRK. Since 2019, it has canceled the registration of hundreds of vessels.[83]

188. It is important to highlight that the aforementioned jurisdictions—with the exception of Bolivia—also host numerous FTZs. The combination of the relative maritime anonymity offered by open registries (or "flags of convenience") and the relative opacity provided by FTZs—when not duly regulated and supervised—exacerbates the overall risk. Goods can be transported under a flag with poor oversight, transshipped through an FTZ with limited controls, and re-exported with falsified documentation regarding their origin and destination.

189. Answering a question on whether maritime authorities conduct proliferation financing and sanctions risk assessment before granting relevant licenses, only 4 jurisdictions – Panama, Bolivia, Honduras, and the Dominican Republic - responded "Yes," with Bolivia clarifying that the training offered is on cargo classification and port handling, not specific to proliferation financing. Out of 4, only Panama provided substantial detail on how such risk assessment works in practice. Panama described sophisticated due diligence procedures for the efficient review of the backgrounds of all vessels (including their owners, operators, and/or managers) that are registered or in the process of registration, and to identify those linked to illicit activities, including vessels about to arrive at ports or waters under Panama's jurisdiction. The verification considers, among other aspects, flag transfers, the operational history of the companies, the vessel's areas of operation, whether it is on international sanctions lists from various organizations (including the United Nations Security Council), port call records, and reports from the Flag State.

190. In addition to 4 jurisdictions that answered "Yes" to maritime authorities conducting PF/sanctions checks, Mexico reported that its maritime authority - The National Maritime Authority Unit – participates

[80] "Iran-Related Designations," U.S. OFAC, December 3, 2024, https://ofac.treasury.gov/recent-actions/20241203.

[81] The number is reported by Panama in its country survey.

[82] UN Panel of Experts report, S/2019/691, p.18.

[83] Elida Moreno, "Panama Removes Over 650 Ships from Registry Amid Sanctions, Stricter Rules," *Reuters*, June 2, 2025, https://www.reuters.com/world/americas/panama-removes-over-650-ships-registry-amid-sanctions-stricter-rules-2025-06-02/.

in CANDESTI as a member, where PF/sanctions-related situations are addressed, but it does not conduct assessments on its own because it is not empowered to do so.

191. The maritime industry in the GAFILAT region is the weakest link in government-led guidance or training on proliferation financing and sanctions. Only 3 jurisdictions – Panama, the Dominican Republic, and Honduras – responded "Yes" to the question of whether their governments provide training on proliferation financing and sanctions to the maritime industry. Additionally, Bolivia reported offering training on cargo classification and port handling, not specific to proliferation financing. The remaining 13 jurisdictions did not provide responses or responded "No." Even countries with meaningful maritime sectors provide no industry-level guidance or training.

192. Regarding whether maritime supervisors monitor or supervise compliance with the implementation of targeted financial sanctions, only Mexico and Panama answered "Yes," while 12 jurisdictions reported "No," and the remaining jurisdictions did not provide an answer.

193. In total, 12 GAFILAT jurisdictions reported the total number of vessels under their flags. El Salvador reported the smallest number of vessels at 11; Panama reported the largest international merchant registry at 8,602.[84] The wide range in the number of vessels registered under a national flag reflects a broad spectrum of potential exposure to maritime-related risk. Additionally, consideration must also be given to the volume and nature of the cargo; the jurisdiction's participation in transit, transshipment, or re-export corridors; the presence of maritime or river ports; the size of the merchant or river fleet; the use of vessels registered in third countries; and the degree of integration with international logistics chains. However, the residual risk depends on the effectiveness of the mitigation measures, applied controls and the supervisory capacity of each jurisdiction.

194. The maritime sector is among the most vulnerable industries in the GAFILAT region, and the data indicate it should be a priority for national and sector-specific PF risk assessments in line with FATF guidances,[85] as well as a priority for government outreach.

Summary

195. The GAFILAT region presents a mixed maritime risk profile. Geographically, it sits far from the principal proliferant states—the DPRK and Iran—which lowers its direct exposure; at the same time, it hosts several of the busiest Atlantic and Pacific maritime corridors and a number of major transit and transshipment hubs. While the region's ports are not among the world's largest, significant cargo volumes pass through them — the largest for container count being Brazil's Santos, Panama's Colón and Balboa, Mexico's Manzanillo, and Colombia's Cartagena — and most are on an upward trajectory, so total throughput is expected to keep rising. Brazil, Panama, Colombia, Argentina, Chile, Mexico, Peru, and Paraguay are major transit or transshipment hubs; Ecuador is a regional hub; Guatemala, Honduras, and El Salvador serve as land-based transit corridors; and Bolivia and Nicaragua have minimal throughput.

[84] Argentina and Mexico reported larger totals of vessels that include small/non-merchant craft.

[85] In the context of Recommendation 1, "proliferation financing risk" refers strictly and exclusively to the potential non-compliance, failure to implement, or evasion of obligations regarding the targeted financial sanctions referred to in Recommendation 7. However, FATF guidance—such as the 2025 report on *Complex Proliferation and Sanctions Evasion Schemes*—notes that the misuse of the maritime and shipping sectors to circumvent sanctions constitutes one of the primary threats regarding proliferation financing. See paragraph 18, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

196. A central risk component is the availability of Flags of Convenience ("open registries"), which the International Transport Workers' Federation attributes to 3 jurisdictions in the region. Compounding the exposure, these 3 jurisdictions also host numerous FTZs, so the relative anonymity of an open registry can combine with the relative opacity of an FTZ to let goods be shipped, transshipped, and re-exported with laundered origin and destination documentation.

197. Governance and controls across the region are uneven and, in key respects, thin. Only 4 jurisdictions —Bolivia, the Dominican Republic, Honduras, and Panama— reported conducting PF and sanctions risk assessments during vessel licensing, and only Panama described substantial due diligence procedures in practice, covering flag transfers, operational history, areas of operation, sanctions-list screening, and port-call records; Mexico participates in the interagency CANDESTI but is not empowered to assess on its own.

198. Government-led training and guidance to the maritime industry is the weakest link, provided only by the Dominican Republic, Honduras, and Panama, while the remaining 13 jurisdictions did not respond or answered "No." Supervision of targeted financial sanctions compliance is similarly limited, according to survey results, and was reported only by Mexico and Panama. However, the 4th round of MERs shows progress in implementing targeted financial sanctions, in accordance with FATF Recommendations, in other jurisdictions, including Bolivia, Brazil, Costa Rica, Cuba, the Dominican Republic, Nicaragua, Paraguay, Peru, and Uruguay, with ratings ranging from Compliant to Largely Compliant.

199. On balance, the maritime sector is among the most vulnerable industries in the GAFILAT region and should be a priority for national and sector-specific PF risk assessments in line with FATF guidances,[86] as well as a priority for government outreach.

4.3.3. Key Red Flags for the Maritime Sector [87]



1. AIS/Location Data

- **Automatic Identification System (AIS) "going dark":** vessels conducting illicit ship-to-ship transfers disable AIS to evade detection; extended periods without AIS transmission. These specific anomalies serve as Red Flags that unilateral sanctions regimes typically highlight to insurers, urging them to be on the lookout for such activity.
- **AIS spoofing/manipulation:** manipulating AIS signals to make a vessel appear somewhere it is not (e.g., appearing to be in Dubai while loading oil in Iran).
- **Maritime Mobile Service Identity (MMSI) manipulation and abnormal patterns:** MMSI manipulation to disguise the ship's name or location, abnormal traffic or voyage patterns, and dark activity concentrated in known hotspots and maritime chokepoints.

[86] In addition to other relevant documents such as *Complex Proliferation Financing and Sanctions Evasion Schemes*, FATF, 2025.

[87] The Consolidated List of Red Flags for the maritime sector with a list of references is available in Annex II (c). The list of key Red Flags—including the one in Annex II (c)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

2. Vessel Identity and Flag

- **Physically altering vessel identification:** painting over vessel names and IMO numbers to pose as different vessels — the IMO number is permanent regardless of name or ownership changes.
- **False flags and flag hopping:** falsifying flags to mask illicit trade, or repeatedly registering vessels with new flag states to avoid detection; using a country's flag after deregistration, or claiming a flag without proper authorization.
- **Frequent name and identity changes:** a common shadow-fleet tactic alongside ownership changes, flags of convenience, and going dark; false-flagged ships often lack valid insurance and certificates of seaworthiness.

3. Ownership and Management

- **Complex or opaque ownership and management:** one of the core deceptive shipping practices.
- **Front and shell companies:** layered across jurisdictions, with single-vessel ownership structures and frequent changes of registered owner, manager, or operator shortly before or after sanctions designations.
- **Shadow/dark fleet characteristics:** older vessels that do not meet standard maritime regulations and rely on flag registries with lower due diligence standards; unclear or unverifiable P&I insurance.

4. Voyage / Routing

- **Ship-to-ship (STS) transfers:** used to conceal the origin or destination of surreptitiously transferred petroleum, coal, and other materials - especially in waters known for transfers of sanctioned cargo, or with a counterparty vessel not broadcasting AIS.
- **Voyage irregularities:** indirect routing, unscheduled detours, or transit/transshipment of cargo through third countries to disguise the ultimate destination or origin.
- **Sanctioned-jurisdiction calls and loitering:** port calls to sanctioned jurisdictions followed by attempts to obscure them; loitering in known STS zones without a declared commercial purpose.

5. Cargo and Documentation

- **Falsified cargo and vessel documents:** bills of lading, certificates of origin, invoices, packing lists, proof of insurance, and lists of last ports of call; irregularities may provide a basis to hold a shipment until contents are validated.
- **Origin/destination mismatch:** documentation that does not accurately reflect the origin and destination of cargo, particularly involving jurisdictions commonly listed on falsified documentation or waters known for ship-to-ship transfers of sanctioned oil; mismatched bills of lading, invoices, and packing lists.
- **Dual-use cargo descriptions:** vague or generic descriptions ("machine parts," "electronic equipment") inconsistent with the consignee's line of business, and freight forwarders listed as final destination.

6. Financial/Payment

- **Shadow payment channels:** used to obscure financial routes, including intermediaries in jurisdictions with less stringent financial regulations.
- **Third-party and off-market payments:** payments from a third party not identified on the original letter of credit or trade documentation, located in an intermediary or known transshipment jurisdiction; freight, demurrage, or charter payments routed through unrelated third parties or exchange houses, or inconsistent with prevailing market rates.

- **Insurance Red Flags:** requests for cover with incomplete vessel history, refusal to provide voyage details, or cancellation of cover requests once questions are asked.

4.4. Free Trade Zones (FTZs)



4.4.1. Global Risk

200. Free Trade Zones or similar arrangements, such as free economic zones, free zones, and special economic zones, pose a high risk of evading export controls and sanctions and, relatedly, of proliferation financing. There is less oversight of goods entering and exiting these zones. Exemptions from foreign business ownership regulations, separate company formation services, and less rigorous beneficial ownership checks create a more lenient oversight regime. Fewer restrictions on trade involving FTZs make them appealing for both legitimate businesses and illicit activities, including sanctions evasion.[88] High volumes of goods passing through the zones further complicate due diligence.

201. FATF explicitly assessed that FTZs are vulnerable to proliferation financing and sanctions evasion because they can reduce visibility into goods, counterparties, and trade documentation. FATF's report *Complex Proliferation Financing and Sanctions Evasion Schemes* describes how procurement networks route goods through FTZs that "often have less stringent oversight" and may allow "repackaging and re-exporting under new labels", alongside falsified shipping and trade documents intended to disguise the true origin, final destination, final end-user, or nature of the cargo.[89] "Light manufacturing" activities typically allowed in FTZs may include assembly, packaging, labeling, and the creation of new final products from components imported into the free trade zone. This can obscure product identities before the product leaves the zone. FTZs often feature in cases of illicit procurement of sensitive goods. For example, a company based in the UAE's free zone attempted to re-export dual-use inverters to Iran.[90]

[88] Kenji Omi, "'Extraterritoriality' of Free Zones: The Necessity for Enhanced Customs Involvement," 2019, WCO Research Paper No. 47, 8; *Complex Proliferation Financing and Sanctions Evasion Schemes*, p. 24-25.

[89] *Complex Proliferation Financing and Sanctions Evasion Schemes*, p. 26.

[90] Ibid, p. 52.

4.4.2. Regional Risk

202. In the GAFILAT region, FTZs (free economic zones, special economic zones) often operate on high-throughput trade corridors (ports, airports, land borders). They are designed to minimize logistical barriers for trade and are key to the countries' economies. The same characteristics that make region's FTZs attractive to legitimate businesses make them vulnerable to actors pursuing illicit activities. As discussed earlier, proliferators can use FTZs to move goods because the likelihood of detection is lower.

203. To assess regional FTZ-related risk, the country survey included questions on the number of FTZs, regulatory oversight, sanctions-evasion or illicit transit/transshipment cases linked to FTZs, and trade turnover.

204. All 16 GAFILAT jurisdictions that participated in the survey have FTZs, and 2 non-participating jurisdictions also have FTZs. In total, 15 jurisdictions – Argentina, Bolivia, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panama, Paraguay, Peru, Uruguay – provided full or partial responses to the questions on FTZs.

205. It is worth noting that, answering the question "Is regulatory supervision reduced in FTZs compared with other national territories?" all except 1 jurisdiction (El Salvador) answered "No" or left the answer blank. The fact that the majority of GAFILAT jurisdictions perceive regulatory supervision as equivalent to that in other national territories does not align with the reality that there is usually less regulatory oversight in FTZs. As mentioned earlier, FATF specifically warns that FTZs "often have less stringent oversight."[91]

206. The country survey also included a question on transparency requirements for company formation within an FTZ. Proliferators and sanctions evaders often use front companies and other legal entities to conceal their involvement. Company formation is usually easier in FTZs. Hence, it was important to understand what transparency requirements GAFILAT jurisdictions have in place. In total, 11 jurisdictions – Bolivia, Chile, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Panama, Paraguay, Peru, Uruguay - provided substantive answers. However, some of the region's major users of dual-use goods and technology did not respond.

207. Two approaches became apparent from the data provided. In the first group, the same rules that govern company incorporation in the rest of the national territory apply to FTZs, with no FTZ-specific regimes: Bolivia and Uruguay state that requirements are the same as in the rest of the national territory; Panama notes that companies are not incorporated "in" the zone but through Panama's Public Registry, and additionally, they are subject to supervision by a competent regulatory body which, upon verifying compliance with applicable legal requirements and formalities, issues the resolution authorizing them to operate; and Peru reports no specific regulation. In the second group, companies must obtain authorization from a designated public body before operating in a zone with specific documents. The following jurisdictions belong to the group: the Dominican Republic, Guatemala, Honduras, El Salvador, and Paraguay.

208. Only 2 participating GAFILAT jurisdictions expressly connected FTZ incorporation to beneficial ownership and AML/CFT obligations in their responses on transparency requirements for company

[91] *Complex Proliferation Financing and Sanctions Evasion Schemes*, p. 26.

formation in FTZs. Paraguay cited *Law 5895/17*[92] as amended by *Law 6399/19,*[93] which introduced specific obligations to ensure the identification of the beneficial owner of all legal persons incorporated or registered in Paraguay, prohibiting the use of bearer shares and ensuring shareholder traceability through registered shares. In addition, *Law 6446/19 on Creating the Administrative Registry of Legal Persons and Structures and Beneficial Owners*[94] establishes the obligations to register and keep updated information related to the ownership structure and beneficial owner of legal persons and legal structures incorporated or registered in the country.

209. The Dominican Republic noted that, under *Law No. 155-17 on Anti-Money Laundering and Countering the Financing of Terrorism*, competent authorities may require companies operating in the FTZ to provide information on shareholders and ultimate beneficial owners, as well as documentation necessary to identify the ultimate ownership of capital—in line with international standards—for the purpose of strengthening the transparency of corporate structures and preventing the misuse of these entities for illicit purposes.

210. Ecuador cited the *Organic Law on Transparency and Access to Public Information* (2023),[95] which appears to be more of a freedom-of-information statute governing how the government discloses information and how the public can request it, rather than a corporate transparency framework.

211. Chile delegates the requirements to the FTZ management companies' own regulations, meaning the rules are set by private zone operators.

212. The country survey asked GAFILAT jurisdictions if there were any reported cases of sanction evasion or illicit dual-use transit/transshipment linked to FTZs. GAFILAT-participating jurisdictions either answered "None" or left their answers blank. The lack of reported cases (or detected cases) must be read in the context of the confirmed vulnerability of regional FTZs to other illicit activity. Researchers and international bodies regularly document how FTZs have been used for arms transshipment, commodity-based trade laundering, and other illicit activity.

213. The country survey requested trade volume data for FTZs in GAFILAT region, which can be consulted in individual country matrices in Annex I.

Summary

214. Free trade zones must be seen as a priority area for the GAFILAT region in minimizing the risks of proliferation financing and sanctions evasion. Although no cases of sanctions evasion or export control

[92] *Law 5895/17*, 2017, https://www.bacn.gov.py/leyes-paraguayas/9118/ley-n-5895-establece-reglas-de-transparencia-en-el-regimen-de-las-sociedades-constituidas-por-acciones.

[93] *Law 6399/19*, 2019, https://www.bacn.gov.py/leyes-paraguayas/9358/ley-n-6399--modifica-los-artculos-3-y-4-de-la-ley-n-58952017-que-establece-reglas-de-transparencia-en-el-rgimen-de-las-sociedades-constituidas-por-acciones-y-establece-medidas-transitorias.

[94] *Law 6446/19*, 2019, https://www.bacn.gov.py/leyes-paraguayas/9116/ley-n-6446-crea-el-registro-administrativo-de-personas-y-estructuras-juridicas-y-el-registro-administrativo-de-beneficiarios-finales-del-paraguay.

[95] *Organic Law on Transparency and Access to Public Information*, 2023, https://www.gob.ec/regulaciones/ley-organica-transparencia-acceso-informacion-publica-2.

violations involving sensitive goods were detected, this does not necessarily indicate a lack of risk. First, the majority of GAFILAT jurisdictions lack comprehensive export control systems for dual-use goods and technology, making it less likely to detect illicit activity involving such goods. Second, the documented cases of illicit activities in the region's FTZs or similar areas with a low-tax free-commerce border in the Tri-Border Area confirm general exposure to risk.

215. GAFILAT jurisdictions employ two distinct methods regarding transparency requirements for incorporating companies in FTZs. Some jurisdictions use the same rules as in the rest of the national territory, and some apply FTZ-specific regimes. Beneficial ownership requirements are also relevant in this context and will be discussed in detail in Section 4.5.2. Importantly, two jurisdictions – Paraguay and the Dominican Republic – specifically mentioned beneficial ownership and AML/CFT obligations in their responses on transparency requirements for company formation in FTZs.

216. Overall, there seems to be a lower risk perception of FTZs than they deserve, with all but 1 jurisdiction suggesting that regulatory oversight is the same as in the rest of the national territories.

4.4.3. Key Red Flags for FTZs[96]



1. Zone Oversight and Structure

- **Weak zone oversight:** goods are routed through, or warehoused in, an FTZ known for limited physical cargo inspection, weak supervision, or inadequate AML/CFT/CPF safeguards.
- **Zone–customs oversight gap:** the FTZ authority and national customs lack effective coordination or information-sharing, creating an oversight gap between the zone and the wider customs territory.
- **Exploitation of zone openness:** the zone's openness, fiscal and customs exemptions, and reduced reporting are exploited to structure cross-border transactions with limited transparency.

2. Goods, Documentation, and Origin

- **Repackaging and relabeling:** goods are repackaged, relabeled, re-marked, re-invoiced, blended, or assembled within the zone in ways that change their apparent description, classification, value, or origin before re-export.
- **Altered certificates of origin:** certificates of origin are issued or altered within the zone in a manner that disguises the true country of origin of the goods.
- **Value inflation through transit:** the declared value of goods rises substantially as they transit the zone, consistent with value-inflation or trade-based money laundering through transshipment.

3. Entities and Ownership

- **Pass-through or minimal-substance entities:** an FTZ-registered entity has minimal physical presence, a warehousing-only or 'pass-through' profile, or operations inconsistent with its stated trade volumes.
- **Shell and front company concentration:** there is a concentration of shell or front companies registered within, or transacting through, the zone, or repeated re-registration of similar entities.

[96] The Consolidated List of Red Flags for FTZs with a list of references is available in Annex II (d). The list of key Red Flags —induding the one in Annex II (d)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

4. Geography and Logistics

- **Proximity to sanctioned jurisdictions:** the FTZ is in close geographic proximity to, or maintains trade links with, a sanctioned jurisdiction or a recognized diversion/transshipment point.
- **Altered shipping instructions:** an item's shipping instructions are changed on entry to a freight forwarder or FTZ, without the exporter's knowledge.
- **Consolidation of small shipments:** small, frequent shipments are consolidated at an FTZ warehouse before onward movement.

4.5. Relevant DNFBPs: Trust and Company Service Providers; Legal Professionals (Lawyers), Notaries, Accountants.



217. For the purpose of this report, several categories of DNFPs were selected as most relevant to proliferation financing: Trust and Company Service Providers; Legal Professionals (Lawyers), Notaries, Accountants; Dealers in Precious Metals and Stones.

Overview of DNFBP-related Risks

218. To understand the regional risk when it comes to DNFBPs and areas for potential improvement, the survey posed three questions: (1) Is there a requirement for DNFBPs to implement targeted financial sanctions? (2) Is there a requirement for DNFBPs to apply customer due diligence (CDD) controls? (3) Are there sectors to which reporting obligations do not apply?

219. Regarding the requirement for DNFBPs to implement targeted financial sanctions, of the 16 jurisdictions that participated in the survey, 13– Argentina, Bolivia, Brazil, Chile, the Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Paraguay, and Peru – reported that such a requirement exists; 2 jurisdictions – Colombia and Honduras – reported no requirement for DNFBPs to implement targeted financial sanctions. Uruguay did not respond to the question; however, in its 4th round mutual evaluation MER, it was rated as Largely Compliant with Recommendation 7, and no specific deficiencies related no specific deficiencies related to the implementation of targeted financial sanctions by DNFBPs were identified.

220. Answering the question on the requirement for DNFBPs to apply CDD controls, in accordance with FATF Recommendation 22, out of 16 jurisdictions that participated in the survey, 13 jurisdictions – Argentina, Bolivia, Chile, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru – responded that such a requirement exists.

221. The first category of DNFBPs relevant to our analysis consists of so-called "gatekeepers." These professionals help control access to the financial system by facilitating corporate, legal, and commercial transactions. Their strategic position makes them the first line of defense in blocking illicit funds, including those derived from PF. These DNFBPs include TCSPs, as well as lawyers, notaries, and accountants.

4.5.1. Global Risk

222. The main objective of proliferators is to obscure the end-use, end-user, and final destination of sensitive goods. To do it, they use all available methods to hide that information. With that objective in mind, proliferators use front companies, shell companies, joint ventures, and complex opaque ownership structures. TCSPs, as well as lawyers, notaries, and accountants, can serve as enablers, giving illicit corporate structures surface-level legitimacy.

223. TCSPs create and administer legal entities, trusts, nominee arrangements, and corporate structures. In some jurisdictions, TCSPs offer "shelf companies" – companies already created and registered but left dormant. TCSPs can provide nominee shareholders and directors, making it easier to camouflage real beneficial owners. The obfuscation of beneficial ownership is one of the main typologies used in proliferation financing and sanctions evasion. Proliferators and sanctions evaders can set up front companies, including shell companies, in third countries with the help of local businesses.[97]

224. Proliferators, including sanctioned entities and individuals, can use TCSPs to create shell and front companies for use in illicit activities. As reflected in FATF's report *Complex Proliferation Financing and Sanctions Evasion Schemes*:

> *"Front companies are a common vehicle to obscure the path of dual-use goods with an application in military weaponry or the defence sector. Illicit actors employ these types of complex vehicles to slow the momentum of investigations to uncover the potential evasion of sanctions or circumvention of export controls involving sensitive goods."*[98]

225. There are plenty of cases of proliferation financing and sanctions evasion involving the DPRK and Iran that confirm this is not a theoretical threat but a practical risk. DPRK and Iran frequently use front companies, shell companies, joint ventures, and complex ownership structures for sanctions evasion. For example, Foreign Trade Bank, a DPRK bank sanctioned by the US since 2013 and by the UN since 2017, relied on more than 250 front companies. The bank's executives set up branches in different countries around the world and engaged in illicit transactions totaling at least $2.5 billion.[99]

---

[97] *Complex Proliferation Financing and Sanctions Evasion Schemes*, p. 21.

[98] Ibid, p. 23.

[99] "US Charges North Korean Bank Officials in Sanctions Case," Voice of America, Associated Press, May 28, 2020. https://www.voanews.com/a/usa_us-charges-north-korean-bank-officials-sanctions-case/6190090.html.

226. TCSPs can be used to grant sanctioned entities and individuals access to the global financial system that they would otherwise lack. TCSPs, including holding companies, foundations, and trusts, can open bank accounts, enter into commercial contracts, engage in trade finance, and conduct wire transfers on behalf of sanctioned entities and individuals.

227. FATF recognizes TCSPs' inherent vulnerability and specifically mentions TCSPs among private sector institutions for conducting proliferation financing risk assessment.[100] Based on FATF Recommendations, TCSPs must screen all clients, both at onboarding and on an ongoing basis, against applicable UNSC sanctions lists, to freeze assets immediately upon a positive match, and report any match to the financial intelligence unit.

228. Lawyers, notaries, and accountants are also indispensable for creating corporate structures for commercial operations, including illicit ones. Illicit actors seek the services of legal professionals because their services are required in certain categories of transactions.

229. FATF and Egmont Group recognize the vulnerabilities posed by legal professionals.[101] The involvement of legal professionals offers illicit actors a veneer of respectability and legitimacy that might dissuade financial institutions from questioning or raising suspicions. Similarly, the attorney-client privilege and secrecy protected by law can be used to shield illicit dealings from inquiries by financial institutions.

230. While there are no detailed publications tracing the link between legal professions and proliferation financing, available data and guidance from FATF and select governments on adjacent topics help in understanding the risks. For example, Canada's FIU – FINTRAC – issued specific guidance to its private sector on the use of the legal profession in money laundering and sanctions evasion.[102] Sanctions evasion is directly relevant to proliferation financing. Moreover, FINTRAC specifically highlights the role of legal professionals in the creation, management, and use of companies and trusts. This is directly relevant to proliferation financing as proliferators extensively hide behind front and shell companies.

231. FinCEN 2026 alert on Iran's IRGC mentions that oil and shadow banking networks use trust and service providers to evade U.S. sanctions.[103]

4.5.2. Regional Risk

[100] *Guidance on Proliferation Financing Risk Assessment and Mitigation*, p. 12.

[101] "Concealment of Beneficial Ownership," FATF and Egmont Group, July 2018, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf; "Guidance for a Risk-Based Approach: Legal Professionals," July 2019, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.inline.pdf; "Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals," June 2013, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Mltf-vulnerabilities-legal-professionals.html.

[102] "Special Bulletin on the Use of the Legal Profession in Money Laundering and Sanctions Evasion," FINTRAC-2024-SB0003, October 2024, https://fintrac-canafe.canada.ca/intel/bulletins/legal-juridique-eng.

[103] "FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds," FinCEN, May 11, 2026, https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf, p. 4.

232. The broader environment of corporate opacity in which TCSPs operate is important for our discussion. To get a sense of the context, the country survey included a request to report on the following: (1) whether shell companies are permitted; (2) if there are beneficial ownership transparency requirements; (3) if a beneficial ownership registry exists. Out of 16 participating jurisdictions, 12 answered "No" to whether shell companies are permitted; 4 jurisdictions did not provide answers. In total, 12 jurisdictions – Argentina, Bolivia, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Nicaragua, Panama, Paraguay, Peru – reported the existence of beneficial ownership transparency requirements; 4 jurisdictions did not answer; 11 jurisdictions – Argentina, Bolivia, Colombia, Dominican Republic, Ecuador, El Salvador, Nicaragua, Panama, Paraguay, Peru, Uruguay – reported having beneficial ownership registries.

233. Mexico noted that, while the country does not have a beneficial ownership registry, it has mechanisms that enable competent national authorities to access timely, accurate, and up-to-date information on the beneficial ownership of legal persons and arrangements. Brazil reported that the creation of the beneficial ownership registry was underway. Open-source information suggests that the Brazilian tax authority collects beneficial ownership data, and that, as recently as 2026, Brazil further enhanced beneficial ownership requirements.[104] Guatemala reported that draft law on beneficial ownership is pending. Chile and Honduras reported no beneficial ownership registries.

234. To capture the regional risk profile specific to TCSPs, two TCSP-specific questions were included in the country survey.

235. The first question was framed as follows: "Do supervisors provide guidance on proliferation financing to TCSPs?" Of the 16 jurisdictions that participated in the survey, 9 – Bolivia, Colombia, Dominican Republic, Mexico, Nicaragua, Panama, Paraguay, Peru, and Uruguay – responded "Yes."

236. The second question was framed as follows: "Do supervisors of [TCSPs] monitor or supervise compliance by reporting entities with the implementation of targeted financial sanctions?" Out of 16 jurisdictions that participated in the survey, 10 – Bolivia, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Nicaragua, Panama, Peru, and Uruguay responded "Yes." Six - Argentina, Brazil, El Salvador, Honduras, Mexico, and Paraguay – responded "No."

237. The answers provided demonstrate an uneven oversight of TCSPs in the region. Noting the inherent vulnerability of TCSPs, stronger monitoring and supervision requirements on TCSPs will increase jurisdictions' ability to minimize exposure to proliferation financing.

4.5.3. Key Red Flags for TCSPs, Legal Professionals (Lawyers), Accountants, and Notaries[105]



[104] "Brazil Enhances Beneficial Ownership (UBO) Reporting Requirements," Martinelli Advogados, March 10, 2026, https://www.martinelli.adv.br/en/brazil-enhances-beneficial-ownership-ubo-reporting-requirements/.

[105] The Consolidated List of Red Flags for professional intermediaries with a list of references is available in Annex II (e). The list of key Red Flags—including the one in Annex II (e)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

1. Concealed ownership and nominees

- **Nominees and proxies:** formal, informal, "mass," or family/associate nominees, or instructions routed through proxies, used to distance the real owner from the asset
- **Control retained despite "divestment":** a deed of trust or similar arrangement lets a designated person appear to divest while keeping indirect control or benefit
- **Sanctions-timed restructuring:** ownership transferred to non-sanctioned associates around a designation date, or arranged to keep a stake below the 50% control threshold
- **Unjustified complexity:** complex or circular multi-jurisdiction ownership structures with no commercial sense

2. Shell and front companies

- **No substance:** no real presence, employees, or web footprint despite significant activity — often the intermediary's registered office or mailbox is the only presence
- **Mass-produced vehicles:** off-the-shelf or throughput companies, and clusters of entities incorporated by the same agent at a single address
- **Front for sensitive goods:** a shell or front company trades in dual-use or proliferation-sensitive items unrelated to its stated business

3. Client behavior and gatekeeping

- **Opacity:** the client cannot or will not explain its business, beneficial owner, or source of funds
- **Secrecy and shortcuts:** emphasis on secrecy, no rationale for the structure, or pressure for unusual speed
- **Payment without purpose:** willingness to pay fees for little or no genuine professional work

4. Transactions and asset movement

- **Account as a shield:** funds moved through the intermediary's client or pooled account so counterparties see only the intermediary, not the underlying party
- **Value flight:** assets sold or transferred at a loss, or moved out and accounts closed, around a sanctions designation
- **Opaque routing:** payments routed through weak-enforcement jurisdictions, or via virtual assets or hawala, to obscure the parties

5. Proliferation and sanctions nexus

- **Designated or concern nexus:** the client or counterparty is linked to a sanctioned jurisdiction or a diversion/proliferation jurisdiction
- **WMD-list and military markers:** a name or address resembling a proliferation-listed party, or co-located with a military facility in a country of concern
- **Layered procurement:** shipments, communications, and finances routed through multiple brokers and intermediaries — including DPRK or Iranian networks — to conceal the end-user
- **Post-designation set-up:** a company formed shortly after a sanctions date, dealing in defense or dual-use goods

6. Profession-specific markers

- **Lawyers:** client-account misuse with no genuine legal work, sham litigation, or privilege/legal opinions used to shield ownership or source of funds
- **Notaries:** powers of attorney handing control to nominees, non-market property transfers, or the notarial seal lending unwarranted legitimacy
- **Accountants:** false or "shadow" financials that manufacture substance, or engagement chiefly to lend legitimacy
- **TCSPs:** nominee, registered-office, or trustee services — or shelf-company supply — provided without understanding the client or purpose.

4.6. Relevant DNFBPs: dealers in precious metals and stones



4.6.1. Global Risk

238. Currently, most payments for procuring dual-use goods and technology go through formal financial institutions. Nonetheless, precious metals and stones are relevant to proliferation financing as tools for transferring value across borders. Dealers in precious metals and stones can be exploited in proliferation financing, especially through sanctions-evasion schemes. Precious metals and stones are high-value, easily transportable assets that provide a rapid, discreet means of conducting large international transactions.

239. Gold, especially, is attractive because it is liquid, priced globally, and easy to use as a payment instrument. It can help settle trade outside of the banking system, be moved physically, or be monetized through intermediaries in regional bullion hubs.

240. DPRK diplomats have smuggled gold across borders.[106] In one especially impressive case, a DPRK diplomat was caught carrying $1.7 million in gold at Dhaka International Airport in Bangladesh.[107]

241. Iran has used gold to mitigate the constraints imposed by the UN and unilateral (autonomous) sanctions regimes, such as limited access to correspondent banking, U.S. dollars, and Euros, and limitations on routine cross-border transfers. The best illustrative example of Iran's use of gold is the Halkbank scheme. According to U.S. law enforcement, a conspiracy scheme involving Halkbank managers helped convert Iran's revenue from oil and gas into gold, using front companies and falsified information.[108]

242. Under FATF Recommendations, dealers in precious metals and stones are designated DNFBPs, required to conduct customer due diligence and report suspicious and above-threshold cash transactions.

4.6.2 Regional Risk

243. Of the 18 GAFILAT jurisdictions, in 17 – Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, and Uruguay – dealers in precious metals and stones are reporting entities. There are two approaches in the region: (1) outright inclusion of dealers of precious metals and stones as DNFBP reporting entities; (2) inclusion based on reaching certain thresholds for transactions.

244. The main vulnerability in the GAFILAT region regarding precious metals and stones stems from the scale of illegal gold mining and its comingling with criminal activities. Illegal gold mining is one of the easiest and most profitable ways to land criminal proceedings, including from the drug trade.

245. Dealers in precious metals and stones serve as vehicles for converting illicitly mined gold into "clean" metal. In one landmark enforcement example from 2018, three traders at NTR Metals, the Miami subsidiary of Dallas-based refiner Elemetal, pleaded guilty to a money-laundering scheme built on illegally mined and smuggled gold from the region. Elemetal pleaded guilty to failure to maintaining an adequate AML program.[109] For years, Elemetal was importing illegally mined gold from Peru in staggering quantities.[110] As part of the plea and forfeiture deal, Elemetal agreed to forfeit $15,000,000 to the United

[106] Chad O'Carroll, "North Korean Diplomats Regularly Flew on Emirates to Smuggle Gold and Cash," NK Pro, April 13, 2021.

[107] "Bangladesh Seizes Gold from North Korean Diplomat," BBC, March 6, 2015, https://www.bbc.com/news/world-asia-31768756

[108] "Turkish Bank Charged In Manhattan Federal Court For Its Participation In A Multibillion-Dollar Iranian Sanctions Evasion Scheme," U.S. Attorney's Office, Southern District of New York, Press Release, October 15, 2019, https://www.justice.gov/usao-sdny/pr/turkish-bank-charged-manhattan-federal-court-its-participation-multibillion-dollar.

[109] Seth Robbins, "Peru Targets Multinationals Linked to Sale of Illegal Gold," InSight Crime, April 10, 2019, https://insightcrime.org/news/peru-targets-multinationals-illegal-gold/.

[110] Leonardo Goi, "Peru-US Gold Case Shows How Importer Shifted Gears," May 22, 2017, https://insightcrime.org/news/analysis/peru-us-gold-case-shows-how-importer-shifted-gears/.

States and be subject to a 5-year probation with no purchase of foreign gold.[111] Peru and other countries in the region have intensified the fight against illegal mining and smuggling. In the most recent example from April 2026, which shows both the vulnerability and efforts to combat illicit operations, Brazilian highway police seized 13 kilograms of illegal gold worth at least US$2 million.[112]

246. Dealers of precious metals and stones must be treated as a high-risk category, especially in gold-producing states of Peru, Colombia, Bolivia, Ecuador, and Brazil, and more broadly in the region.

4.6.3. Summary of Red Flags for Dealers of Precious Metals and Stones [113]



1. Customer identity and behavior

- **Identity evasion:** the customer cannot be properly identified, refuses or gives vague, false, or conflicting identity or beneficial-ownership information, uses aliases or name variations, or alters the transaction when asked for ID
- **Secrecy and source-of-funds opacity:** reluctance to explain the source of funds, requests that normal business records not be kept, or a defensive stance to routine questioning
- **Profile mismatch:** a purchase or sale inconsistent with the customer's known occupation, income, or financial profile, or a sudden change in their pattern of activity
- **Indiscriminate buying:** the customer buys merchandise without regard to value, size, or color, or does not haggle or ask for the usual discount on high-value items

2. Cash and payment

- **Large or unusual cash:** high-value jewelry or bullion paid for in cash only, or cash that is musty, dirty, or packed and transported in an uncommon way
- **Structuring:** transactions split across amounts, days, locations, or staff to stay below identification or reporting thresholds, or a customer who displays knowledge of those thresholds
- **Atypical instruments or third-party payment:** sequentially numbered money orders, traveler's or cashier's cheques, third-party cheques or credit cards, or payment from unrelated parties
- **Refund or cancellation laundering:** an order paid in cash then cancelled for a large refund, or goods returned for a cheque, especially one payable to a third party

[111] "U.S. Gold Refinery Pleads Guilty to Charge of Failure to Maintain Adequate Anti-Money Launderung Program," U.S. Attorney's Office, Southern District of Florida, Press Release, March 16, 2018, https://www.justice.gov/usao-sdfl/pr/us-gold-refinery-pleads-guilty-charge-failure-maintain-adequate-anti-money-laundering.
https://storage.courtlistener.com/recap/gov.uscourts.flsd.523146/gov.uscourts.flsd.523146.3.0.pdf

[112] "Operation Leads to Major Gold Seizure in the Amazon Region," UNODC, May 25, 2026, https://www.unodc.org/unodc/en/frontpage/2026/June/operation-leads-to-major-gold-seizure-in-the-brazilian-amazon.html.

[113] The Consolidated List of Red Flags for dealer of precious metals and stones with a list of references is available in Annex II (f). The list of key Red Flags—including the one in Annex II(f)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

3. Transaction and product

- **No economic sense:** the transaction lacks a business or economic purpose, is unnecessarily complex, or is not in conformity with standard industry practice
- **Rapid resale and value transfer:** precious metals or stones bought and rapidly resold, or bullion and jewelry used as an easily transportable store of value
- **Trade does not fit the business:** an entity whose core business is unrelated (for example, a car dealer trading in precious metals), or volumes well outside its normal line

4. Valuation and trade documentation

- **Over- or under-invoicing:** jewelry or stones invoiced above or below true value to move value or disguise proceeds, or repeated and multiple invoice requests
- **Misdescription and smuggling forms:** goods declared at a false value, or moved in bullion, scrap, jewelry, or artefact forms to disguise their origin

5. Parties, structure, and intermediaries

- **Shell entities and shared identifiers:** a suspected shell company with no economic purpose, common addresses or phone numbers used by multiple unrelated customers, or multiple entities at one address with the same directors
- **Third parties and gatekeepers:** a customer acting on behalf of or directed by an unrelated party, or a gatekeeper (lawyer or accountant) who conceals the client or rushes the deal
- **Informal dealers and intermediary chains:** chains of intermediaries or informal dealers that make the source and ownership of goods and funds hard to trace

6. Geography, sanctions, and proliferation

- **High-risk jurisdictions:** funds, supply, or counterparties tied to jurisdictions of concern — conflict zones, weak-AML or secrecy jurisdictions, or FATF-listed countries
- **Illicit-origin gold:** gold of unclear or illegal-mining origin, or supply chains used to launder proceeds or fund conflict and sanctioned actors
- **Sanctions and PF nexus:** counterparties, suppliers, or branches in sanctioned jurisdictions, or precious metals (notably gold) used as value transfer to evade sanctions.

4.7. Virtual Asset Service Providers (VASPs)



4.7.1. Global Risk

247. Most payments for dual-use goods and technology currently rely on transactions through formal financial institutions. Nonetheless, cryptocurrency's role in proliferation financing and sanctions evasion has grown exponentially. Proliferators increasingly turn to crypto domain to generate, launder, and transfer funds. Virtual assets enable rapid fund transfers, including cross-border transfers. Sophisticated obfuscation methods – such as mixers, DeFi protocols, chain-hopping, and rapid transfers through numerous one-time-use wallets – enable malicious actors to use virtual assets for illegal activities without detection.

248. Theft, cryptocurrency mining, and cryptocurrency laundering are among the DPRK's most profitable sources of revenue. Funds generated within the virtual domain directly support the DPRK's regime and its nuclear and missile programs. DPRK hackers have been stealing funds from cryptocurrency exchanges and other blockchain platforms. According to Chainalysis, DPRK agents stole up to $1.1 billion in virtual assets in 2022, $660.5 million in 2023, and $1.34 billion in 2024.[114] The 2024 UN Panel of Experts report noted that, between 2017 and 2023, the DPRK carried out 58 cyberattacks, resulting in the theft

[114] "$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July," Chainalysis, December 19, 2024.

of approximately $3 billion in cryptocurrency.[115] In 2025, DPRK stole $2.02 billion in crypto.[116] DPRK also generates additional funds through crypto mining, which involves verifying transactions in exchange for cryptocurrency, and cryptojacking, in which the computing power of unsuspecting victims is used to mine cryptocurrency. DPRK hackers also raise funds by installing ransomware — malicious software that encrypts victims' data — and demanding payment in cryptocurrency for the decryption key.

249. Cryptocurrency also plays an important part in Iran's payment ecosystem. Iran's main cryptocurrency exchange Nobitex has 11 million users and is used by Islamic Revolutionary Guard Corp (IRGC) to move millions in dollars.[117] Iran uses cryptocurrency to bypass sanctions and procure sensitive goods. Entities and individuals directly involved with Iran's nuclear and missile programs use cryptocurrency. At a minimum, some suppliers are willing to sell goods to Iran in exchange for cryptocurrency. According to TRM, a company specializing in technology solutions to combat financial crime, Chinese companies supply Iran with drone parts, AI hardware, and other electronic components paid for with cryptocurrency.[118]

250. Among the vulnerabilities of VASPs is that they are either unregulated or in the early stages of regulation in many jurisdictions worldwide. A typical cryptocurrency exchange does not follow the same KYC procedures as a regular bank.

251. FATF recognizes the inherent risks in virtual assets and, through Recommendation 15, sets the relevant standard (as discussed in Section 3.3.). FATF asks jurisdictions to assess the money laundering, terrorist financing, and proliferation financing risks of the VASP sector and require VASPs to be registered and supervised. Where permitted, VASPs should be subject to the same preventive measures as financial institutions regarding CDD, record-keeping, and STRs. An important obligation is the "Travel Rule" under FATF Recommendation 16. VASPs must obtain, hold, and securely transmit originator and beneficiary information when making transfers above a threshold of USD/EUR 1,000.[119]

252. Over the past few years, FATF has encouraged governments to regulate VASPs more effectively, stressing that regulatory failures in one jurisdiction can have global consequences.[120]

---

[115] UN Panel of Experts, *Final Report S/2024/215*, p. 557–558.

[116] "North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion," Chainalysis, December 18, 2025, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

[117] Gavin Finch, Allison Martell, Denise Ajiri, James Pearson and Elizabeth Howcroft, "One of Iran's Most Powerful Families Founded Its Largest Crypto Exchange. It's Used by IRGC to Move Millions," Reuters, May 1, 2026, https://www.reuters.com/investigations/one-irans-most-powerful-families-founded-its-largest-crypto-exchange-its-used-by-2026-05-01/.

[118] "Iran's Crypto Economy in 2025: Declining Volumes, Rising Tensions, and Shifting Trust," TRM Blog, August 26, 2025.

[119] Recommendation 16, The FATF Recommendations, as amended June 2026, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/fatf-recommendations-2012.pdf; "Changes to FATF Standards," FATF, June 18, 2025, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html ; "Explanatory Note for Revised R.16," FATF, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Explanatory%20Note%20for%20Revised%20R.16.pdf.coredownload.pdf.

[120] "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Provides," FATF, June 2025.

4.7.2. Regional Risk

253. Recognizing the growing importance of VASPs in the proliferation financing and sanctions evasion landscape, the country survey included several VASP-specific components: regulation, supervision, the number of VASPs, KYC and STR obligations, and PF and sanctions training. The survey also asked jurisdictions if any cyberattacks on VASPs were reported.

254. For a comprehensive and up-to-date (2025) overview of the money laundering and terrorist financing risk assessment regarding virtual assets and VASPs in the region, see the GAFILAT regional risk assessment document.[121] Additionally, paragraph 65 of this document outlines the level of regional compliance with Recommendation 15 during GAFILAT's 4th Round of Mutual Evaluations.

255. The data from participating jurisdictions revealed the following regional trends. There has been significant progress in developing a legal-regulatory framework for VASPs over the past five years, 2020-2025. This trend suggests that jurisdictions are following FATF's Recommendations and recognizing the importance of regulating virtual assets. At the same time, relatively recent legal and regulatory systems for VASPs are not always fully operational. For example, in several jurisdictions, the primary legislation has been adopted, but the secondary legislation (implementing regulations) is still being developed. Importantly, even during the period of this project, there have been substantive positive developments with new legislation coming into force between the time when jurisdictions participated in country surveys and the final report.

256. Of 16 jurisdictions participating in the survey, 11 – Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, El Salvador, Mexico, Nicaragua, Paraguay, Peru – regulate VASPs. In Mexico, VASPs are regulated at the level of DNFBPs, not financial institutions.

257. Uruguay has adopted *Law No. 20,345* (on virtual assets), which grants the Central Bank of Uruguay (BCU) the authority to regulate entities that provide certain services related to virtual assets and extends securities market legislation to decentralized-managed securities that are issued, stored, transferred, and traded electronically using distributed ledger technologies. The implementing regulations are currently in progress.

258. Brazil is the jurisdiction with the most recent legislative changes. Brazil, which already had a foundational law in place – *Law No. 14,478/2022* (on virtual assets) – adopted new implementation resolutions to complete a legal-regulatory framework for VASPs. In November 2025, the Central Bank of Brazil published *Resolutions 519, 520*, and *521* under which VASPs must obtain authorization from the Central Bank to conduct their activities. Consequently, they became subject to Central Bank supervision, just like other institutions authorized to operate by the Central Bank.

259. The Dominican Republic currently lacks a legal basis to regulate VASPs but reported that an assessment of the virtual assets sector is underway. The Central Bank of the Dominican Republic does not endorse virtual assets. Guatemala, Honduras, and Panama also reported the absence of a

[121] *Evaluación sectorial de riesgos de lavado de activos y financiamiento del terrorismo de los activos virtuales y los proveedores de servicios de activos virtuales de los países del GAFILAT,* GAFILAT, 2025, https://biblioteca.gafilat.org/wp-content/uploads/2025/08/EvaluacionsectorialderiesgosdeAVyPSAVregionaldelGAFILAT.pdf.

comprehensive legal basis to regulate VASPs. The absence of VASP regulation could have consequences, especially for the Dominican Republic and Panama, as they are among the region's principal financial centers.

260. The number of registered VASPs in GAFILAT jurisdictions with regulating legislation in force as of 2025 ranges from zero to hundreds (exact numbers for each jurisdiction are available in Annex I).[122]

261. It is important to note that the number of registered VASPs does not reflect the full scope of virtual assets activity. For example, Brazil, where VASP-related regulations went into effect only this year, is the 5th largest country in the world in terms of grassroots adoption of cryptocurrency and in year to June 2025 received $318.8 billion in crypto value.[123] Mexico, where VASPs are treated as DNFBPs, in the year to June 2025 recorded about $71.2 billion in crypto transaction volume, third in Latin America behind Brazil and Argentina.[124] Bolivia, which only recently adopted relevant legislation and where implementing regulations are still being drafted, saw cryptocurrency transaction volume surging approximately 630% in six months after a ban on virtual assets was lifted (*Resolution No. 082/2024*).[125] Even jurisdictions reporting zero registered VASPs may still have significant virtual-asset activity within their territory, as the population can use foreign and offshore providers. In fact, the offshore-/unlicensed VASP activity is a concern for FATF due to an oversight gap. In March 2026, FATF published a report highlighting the gap and recommending best practices.[126]

262. To assess whether jurisdictions have already followed FATF Recommendations to subject VASPs to the same preventive measures as financial institutions, the country surveys asked: "Do the same KYC regulations apply to VASPs as to financial institutions?" Of the 16 jurisdictions participating in the survey, 9 responded "Yes"; 4 responded "No" or "N/A" due to a lack of regulation; and 3 were considered "in progress," with relevant implementing regulations pending. Due to the progress that has happened since the time of data collection and taking into consideration Brazil's adoption of regulatory resolutions, the revised numbers should read: 10 jurisdictions - "Yes" (Argentina, Brazil, Chile, Colombia, Ecuador, El Salvador, Mexico at the level of DNFBPs, Nicaragua, Paraguay, Peru); 4 - "No" (Dominican Republic, Guatemala, Honduras, Panama), and 2 - "in progress" (Bolivia and Uruguay). In Bolivia, the adoption of implementing regulations is in progress. In Uruguay, draft regulations stipulate that VASPs operating with financial virtual assets and VASPs that buy and sell non-financial virtual assets will be subject to the same rules as other supervised entities in this area.

263. Another FATF Recommendation concerns a requirement for VASPs to submit STRs. Out of 16 participating jurisdictions, 10 stated that they require VASPs to submit STRs or other reports related to proliferation financing. It can be assumed that the total number is now 11, following Brazil's recently adopted regulations. In Uruguay, the draft regulations implementing *Law 20,345* provide that VASPs,

[122] Confidential Annex available exclusively to GAFILAT National Coordinators.

[123] "The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption," Chainalysis, September 2, 2025, https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/

[124] "Latin America Emerges as a Crypto Powerhouse Amid Volatile Growth," Chainalysis, https://www.chainalysis.com/blog/latin-america-crypto-adoption-2025/

[125] "En un año las operaciones en activos virtuales crecieron en más del 630% y llegaron a $us430 millones," Banco Central do Bolivia, June 25, 2025, https://www.bcb.gob.bo/webdocs/files_noticias/CP-24_Un%20año%20AV%20FINAL%2027jun25.pdf.

[126] "Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers," FATF, March 2026, https://www.fatf-gafi.org/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html.

within the framework of due diligence policies and procedures, will report STRs to the Financial Information and Analysis Unit.

264. The areas that require the most improvement are proliferation financing-related training and supervision. Of 16 jurisdictions, only 8 reported that their governments provide training on sanctions implementation and proliferation financing to VASPs. Of the 16 jurisdictions, only 8 reported that supervisors assess VASPs for compliance with sanctions implementation; Brazil, as a jurisdiction with newly adopted regulatory legislation, can be considered "in progress" in this area. This data reconfirms the assessment in the 2025 GAFILAT Regional Risk Assessment on VASPs for money laundering and terrorist financing, which identified the lack of effective VASP supervision in the region as one of the main vulnerabilities of the sector.[127]

Summary

265. Taken together, the regional picture of the virtual assets sector is one of rapid but uneven and still-maturing regulation. Over 2020–2025, the majority of GAFILAT jurisdictions moved to bring VASPs within their AML/CFT/CPF frameworks in line with FATF Recommendation 15, and several strengthened those frameworks further during the life of this project, most notably Brazil, which aligned VASP obligations regarding "Know Your Customer" (KYC) and Suspicious Transaction Reports with those of financial institutions, effective 2026. Yet the adoption of primary legislation has consistently outpaced the implementing regulations needed to make it operational, and registration has outpaced supervision. Coverage remains incomplete: the Dominican Republic, Honduras, and Panama still lack a comprehensive legal basis to regulate the sector, a gap that could be consequential, especially for the Dominican Republic and Panama given their weight as regional financial centers. Guatemala recently approved *Decree Number 15-2026—the Comprehensive Law on the Prevention and Suppression of Money Laundering or Other Assets and the Financing of Terrorism*—which includes VASPs among obliged entities within the prevention framework.

266. Compounding these challenges is the fact that the number of registered VASPs materially understates the region's true exposure, because residents of jurisdictions with few or no licensed providers continue to transact through foreign and offshore platforms that fall outside national oversight, precisely the supervisory gap the FATF underscored in its 2026 report.

267. These regional weaknesses translate into a concrete vulnerability for proliferation financing and sanctions evasion, as there is consistent evidence that the DPRK and Iran use virtual assets for illicit activities. The most acute deficiencies lie not in whether rules exist, but in whether they are enforced: training and supervision on proliferation financing and sanctions implementation remain the weakest elements of the regional regime, with only half of the participating jurisdictions providing such training or assessing VASP compliance with sanctions implementation. The overall assessment, therefore, is that the region's principal VASP-related risk is no longer the absence of regulation but the absence of effective, risk-based supervision, together with the persistence of unlicensed, offshore activity beyond the reach of that supervision.

268. Among all the high-risk sectors analyzed in this report, the virtual asset sector is the fastest-growing and hardest to regulate, while also becoming increasingly important for preventing the proliferation of financing and sanctions evasion. Operationalizing recently enacted legal-regulatory

[127] *Evaluación Sectorial de Riesgos de LA/FT de los Activos Virtuales y los PSAV de los países del GAFILAT,* GAFILAT, July 2025, p. 8.

frameworks, introducing legislation in jurisdictions that lack it, and investing in supervisory and training should be the region's priority.

269. Beyond the proliferation financing and sanctions evasion risks the report focuses on, virtual assets can also be used for other financial crimes and illicit activities, such as money laundering, terrorism financing, human trafficking, and other crimes.

4.7.3. Summary of Red Flags for VASPs [128]



1. Customer and onboarding

- **Identity evasion:** false, inconsistent, or stolen KYC data, forged documents, or onboarding through borrowed identities and fabricated personas
- **Profile mismatch:** high-value or high-volume activity inconsistent with the customer's stated occupation, income, or profile
- **Sanctioned or concern nexus:** the customer or counterparty is in, or linked to, a sanctioned jurisdiction (e.g., DPRK, Iran) or a proliferation/diversion-concern jurisdiction

2. Anonymity and obfuscation

- **Anonymity tools:** use of mixers or tumblers (including sanctioned ones), privacy coins, or unhosted wallets and P2P platforms with weak AML controls
- **Chain-hopping and layering:** rapid movement across multiple blockchains or bridges, or funds passed through numerous one-time-use wallets, with no business rationale
- **Nested services:** use of nested exchanges or instant exchangers operating within larger platforms to evade controls

3. Transactions and structuring

- **Structuring:** transactions split into small amounts, or amounts just below record-keeping, reporting, or "Travel Rule" thresholds
- **Rapid in-and-out:** immediate transfer out of deposited assets with no holding period, then cross-border movement to foreign VASPs
- **Event-timed activity:** transactions timed to a heist or a sanctions designation, or a willingness to transact at a loss to move quickly

4. On-chain exposure and source of funds

- **Illicit-address exposure:** direct or indirect exposure to DPRK-attributed addresses, sanctioned mixers, darknet markets, ransomware, or theft incidents
- **List-address screening:** sending or receiving exposure to addresses on sanctions lists, including a historic look-back after a new address is listed

[128] The Consolidated List of Red Flags for VASPs with a list of references is available in Annex II (g). The list of key Red Flags—including the one in Annex II (g)—is indicative and non-exhaustive, given that typologies and methods are constantly evolving.

- **Cyber-theft proceeds:** funds traceable to exchange hacks, DeFi exploits, or bridge attacks

5. Sanctions-evasion-specific

- **Sanctioned or unregulated exchanges:** dealings with designated or sanctions-serving exchanges, or use of unregulated platforms to cash out
- **Evasion tokens and nominees:** bespoke tokens built for cross-border evasion, or accounts held via nominees and front companies to hide a sanctioned owner
- **Shadow-banking and commodity nexus:** virtual assets used in hawala/shadow-banking networks to settle oil or commodity sales for sanctioned actors (e.g., the IRGC)

6. Proliferation-financing-specific

- **DPRK revenue streams:** funds linked to Lazarus-type heists, IT-worker earnings converted to crypto, or state-linked mining and ransomware that fund WMD and missile programs
- **Procurement of sensitive goods:** virtual-asset payments to suppliers of dual-use or proliferation-sensitive items (e.g., drone parts, AI hardware, electronics) for Iranian or DPRK programs
- **Designated-program nexus:** counterparties connected to entities or individuals in nuclear, missile, or military programs transacting in virtual assets

7. VASP-level vulnerabilities

- **Weak or absent KYC:** the VASP applies customer due diligence weaker than that of a financial institution, or none, and permits unverified accounts
- **Unregulated or offshore counterparties:** counterparty VASPs that are unlicensed, not enforcing the "Travel Rule," or offshore and outside any supervision
- **Operational compromise:** social-engineering or phishing of VASP staff, or unexpected changes to wallet-signing infrastructure — indicators of a state-actor intrusion.



CHAPTER 5

Overall WMD Proliferation and Proliferation Financing Risk Profile of the GAFILAT Region

5. Overall WMD Proliferation and Proliferation Financing Risk Profile of the GAFILAT Region



270. GAFILAT region's overall exposure to WMD proliferation is low to moderate compared with major procurement and manufacturing supplier countries and major transit and transshipment hubs. The U.S., Europe, and Asia remain the main targets for illicit procurement of sensitive goods due to the concentration of advanced high-tech industries there. When it comes to the DPRK and Iran-related proliferation efforts, Asia, the Middle East, and the Gulf region are the main transit and transshipment points. Compared with the regions mentioned above, the GAFILAT region is not a primary concern for WMD proliferation. It is, nonetheless, far from being insulated from proliferation risks. The assessment of high-risk sectors conducted for this report allows to draw a regional picture.

271. The region remains exposed to risks from transit, transshipment, re-export, diversion, and brokering of sensitive goods and technology. While most countries in the region lack advanced dual-use industries of their own, all rely on dual-use goods and technologies across sectors, including in agriculture and medicine.

272. Several countries have successfully built indigenous high-tech industries and advanced peaceful nuclear programs. Argentina has an advanced peaceful nuclear program, including technology for nuclear reactor production, as well as a satellite industry. Brazil has an advanced peaceful nuclear program, an advanced aerospace and defense industry, and space-launch infrastructure. Mexico has aerospace manufacturing clusters. Brazil has an established and growing semiconductor industry, while Mexico's semiconductor sector — concentrated in assembly, testing, packaging, and design — is also expanding rapidly.

273. Several GAFILAT countries have emerging dual-use industries, a sign of industrial development and technological progress, as analyzed in section 4.2.2. of this document. It is worth noting that the

existence of these industries does not imply they are illicit; however, in the absence of adequate controls and oversight mechanisms, the risk of WMD proliferation and its financing could increase. For example, Chile has been working on a satellite program. Colombia is developing aerospace industrial capability, focusing on UAVs. Costa Rica is an emerging player in the semiconductor industry. There are areas of sensitive technological development in the region that could expand as national economies advance toward high-tech models. Peru produces nuclear radioisotopes for medical, industrial, and research applications. Uruguay is emerging as a regional hub for biotech and genomics. Cuba has an established biopharma and vaccine sector. The Dominican Republic has been manufacturing medical devices, pharmaceuticals, and chemical components. Bolivia has undertaken measures to industrialize its lithium sector. Sensitive goods and technology are therefore present throughout the region, and that footprint is expected to grow as national economies advance towards high-tech economies. This warrants monitoring of potential risks associated with WMD proliferation and its financing.

274. The physical movement of goods compounds the risk. The region is vulnerable as a potential transit and transshipment point for illicitly acquired goods owing to major seaports and air logistics hubs. The region's free trade zones, key to its economic profile and trade, also expose it to additional vulnerabilities, as they enable storage, consolidation, "light manufacturing," and onward shipment with varying levels of oversight. Brokering and intermediary services offered by trading companies and agents can facilitate the sale or shipment of sensitive goods without them being handled locally. Another source of exposure stems from the market for used industrial equipment or surplus goods – for example, a local company in the region might sell sensitive, imported equipment to a third party abroad without seeking a re-export permit (license). There is also a risk of diversion of regulated hazardous materials, such as radiological sources used for industrial and medical purposes or controlled chemicals, through theft or loss. While some GAFILAT states have developed robust, comprehensive, and effective control systems for the export of sensitive and dual-use materials, the majority of GAFILAT countries lack comprehensive export control systems to control sensitive goods, thereby increasing their vulnerability.

275. When it comes to relations with the DPRK and Iran, the following picture arises. In total, 8 jurisdictions – Brazil, Chile, Colombia, Cuba, Dominican Republic,[129] Guatemala, Mexico, Nicaragua – have diplomatic relations with the DPRK. When it comes to Iran, the situation is different. More jurisdictions, 13 in total – Argentina,[130] Bolivia, Brazil, Chile, Colombia, Cuba, the Dominican Republic,[131] Guatemala, Mexico, Nicaragua, Paraguay, Peru, Uruguay – maintain diplomatic relations with Iran.[132] It is important to remember that the sanctions regimes imposed by the United Nations Security Council on these 2 jurisdictions do not amount to a prohibition on maintaining diplomatic relations with those states; however, FATF Recommendation 19 regarding high-risk countries requires enhanced measures or countermeasures against certain states, including DPRK and Iran.

276. The country surveys contained questions on trade volumes with the DPRK and Iran. Only few jurisdictions provided trade data, and the full picture is not available. It is safe to make a general conclusion that trade with the DPRK is either non-existent or negligible, judging by the data submitted by some jurisdictions. Meanwhile, trade with Iran, a country more integrated in the world economy than the heavily sanctioned DPRK, is more present in the region. While Brazil did not report its trade with Iran,

[129] The diplomatic relations of this delegation are of a "non-resident" nature, according to the information provided.

[130] Diplomatic relations between Argentina and Iran are not significant and are conducted at the level of a chargé d'affaires.

[131] The diplomatic relations of this delegation are of a "non-resident" nature, according to the information provided.

[132] This list is based on jurisdictions' self-reporting supplemented with external verification.

open-source information suggests that the bulk of exports from the region to Iran comes from Brazil (around 88% of all exports from Latin America, at about US$3 billion) and consists mainly of corn, soybeans, coffee, sugar, beef, and poultry.[133] In 2025, Iran was the top buyer of Brazilian corn.[134] Brazil mainly imports fertilizers from Iran, but the volume of imports is significantly lower than that of exports. Brazil and Iran are both members of BRICS.

277. Argentina reported its trade with Iran as "low." Peru reported imports from Iran during 2021-2025 totaling US$4.7 million and exports to Iran during the same period totaling US$3.2 million. Uruguay reported exports to Iran, with the export volume falling from US$2.1 million in 2020 to US$29,311 in 2025.

Uneven regional picture

278. Jurisdictions vary both in their exposure to risk and in their capacity to mitigate it. Risk in the region is sector- and jurisdiction-specific, not evenly spread. For example, one category of exposure involves the presence of higher-capability, higher-exposure economies, such as Argentina, Brazil, Chile, and Mexico, which combine dual-use industries, major ports, and significant trade volumes. A second category of exposure centers on the region's financial and logistical hubs, notably Panama and the Dominican Republic. A third category of exposure comes from non-currency flows of value and funds, such as gold and crypto. Illicit mining of gold is directly tied with illicit activities, such as drugs, and the same networks can be used for using gold in sanctions evasion schemes. This exposure is especially relevant to gold-producing jurisdictions – Peru, Colombia, Bolivia, Ecuador, and Brazil. The vulnerabilities inherent in virtual assets are an exponentially growing risk vector as proliferators and sanctions evaders are leaning more and more on the crypto domain to support their illicit activities.

279. The ability to mitigate the risk is also uneven. In most cases, there is a correlation between the size of the economy, the share of the dual-use sector, and other types of high exposure (such as to maritime industry-related risks) and the national response. For example, jurisdictions with a greater share of the dual-use sector tend to have more comprehensive export controls (e.g., Brazil, Argentina, and Mexico). Similarly, Panama – a jurisdiction with the greatest exposure to maritime industry-related risk due to its leading role as a transit/transshipment hub – has invested heavily in recent years in measures to mitigate this risk.

280. At the same time, this correlation is not always in place, and, as sector-by-sector analysis shows, the national response is sometimes not commensurate with the level of risk exposure (one of the best examples for that is the virtual assets sector).

281. This unevenness leads to two observations. First, no single approach will be applicable to all jurisdictions in the region, as they face unique combinations of risks; therefore, national proliferation risk assessments are paramount. Second, the region will only be as secure as its weakest link, so it is in the region's interests for all jurisdictions to make reasonable progress and amplify their capacity to mitigate proliferation financing risk.

[133] Chase Harrison, "Explainer: Iran's Relationship with Latin America," April 1, 2026, https://www.as-coa.org/articles/explainer-irans-relationship-latin-america.

[134] "From Soybeans to Coffee: Brazil Accounts for Most of Latin America's Trade With Iran," Datamar News, March 12, 2026, https://datamarnews.com/noticias/from-soybeans-to-coffee-brazil-accounts-for-most-of-latin-americas-trade-with-iran/.

The central role of financial institutions

282. Financial institutions are at the intersection of every channel examined in this report – the procurement of sensitive goods, fundraising, and the servicing of other high-risk sectors. This puts them in a position of greatest exposure, and at the same time, makes them an additional line of defense against proliferation financing and sanctions evasion. As the analysis in this report showed, the financial sector is ahead of other sectors in terms of its measures to detect and disrupt proliferation financing and sanctions evasion. The financial sector has more comprehensive KYC measures, stronger supervision and monitoring, and more training opportunities than other sectors. At the same time, there are some serious gaps present and discrepancies among jurisdictions.

283. Operationally, financial institutions must be cognizant of the limitations of list screening as the main KYC tool, as proliferators and sanctions evaders rely on deceit tactics and, in the majority of cases, will not be picked up by list-scanning alone. The majority of jurisdictions reported using KYC tools in addition to list scanning, and it is important to reiterate the value of these additional tools.

A false sense of security and a lack of inter-agency coordination for on-the-ground implementation

284. One recurring theme is the mismatch between perceived and actual risk. Nearly every jurisdiction reported that regulatory oversight within its free trade zones is no lighter than in the rest of its territory, which warrants further examination, as it is commonly accepted that such zones typically operate under less stringent supervision and have more permissive trade regimes. Similarly, the discrepancy between registered VASPs and the overall significant activity involving virtual assets via offshore VASPs is another example of when formal data does not correspond to the actual situation on the ground. In general, most jurisdictions perceive their exposure to proliferation financing as low. The majority of jurisdictions have neither registered PF STRs nor launched PF-related investigations, which may indicate genuine low exposure, low detection capacity, or a combination of both. Regardless, it is prudent for the region not to have a false sense of security.

285. While jurisdictions have, in most cases, demonstrated sufficient grounds for inter-agency cooperation and coordination on policy development, cooperation and coordination at the operational level on proliferation financing controls appear insufficient. The region lacks procedures, platforms, and tools to share proliferation-financing information effectively and in real time, especially to integrate export controls and proliferation-financing controls as tools against a shared problem (proliferation).

From laws on paper to implementation in real life and the outlook for the future

286. The region shows an overall positive trend toward advancing PF legal-regulatory frameworks. Legislation for implementing TFS is generally strong across the region, but the track record of implementation is more challenging. As mentioned earlier, only a handful of PF-related STRs and PF-related investigations may indicate weak detection capacity. The supervision of vulnerable sectors – TCSPs, VASPs, and dealers in precious metals and stones – is uneven, with roughly half of the jurisdictions monitoring compliance with TFS implementation in any given sector. In some jurisdictions where primary export control laws were passed, the implementation has not begun due to a lack of implementation frameworks.

287. The region's dual-use sectors are growing, cargo volumes through its ports are rising, and the adoption of virtual assets is expanding. Exposure to proliferation financing will increase, not diminish, in

the coming years. Adopting measures and building systems to minimize risks without delay is critical to regional and international security. The next section proposes some recommendations for the next steps.



CHAPTER 6

Policy Recommendations

6. Policy Recommendations[135]



(1) Complete and operationalize national proliferation financing risk assessments

288. One of the region's immediate needs is to start, continue developing, or complete national PF risk assessments in jurisdictions that have yet to do so. As a minimum, national risk assessments should assess risk as far as the implementation of TFS is concerned. While not required by FATF, a broader risk PF risk assessment that goes beyond TFS implementation will be of great value to the region.[136] Governments should also encourage financial institutions with conducting institutional PF risk assessments.

(2) Close remaining legal gaps

289. This study has revealed some remaining legal gaps that must be closed. Priority areas include, but are not limited to:

[135] For a more detailed discussion of relevant policy recommendations, see also Togzhan Kassenova, Bryan R. Early, *Countering the Challenges of Proliferation Financing*, Center for Policy Research, University at Albany (SUNY), 2023, https://www.albany.edu/rockefeller/news/2023-countering-challenges-proliferation-financing; Togzhan Kassenova and Bryan R. Early, *Banks and the Bomb: Understanding Proliferation Financing*, Stanford University Press, forthcoming, 2027.

[136] For reference consult *Guidance on Proliferation Financing Risk Assessment and Mitigation*, FATF, 2021; Aaron Arnold, David Salisbury, *Guide to Conducting National Proliferation Financing Risk Assessment: 2024*, RUSI, https://www.rusi.org/explore-our-research/publications/special-resources/guide-conducting-national-proliferation-financing-risk-assessment-2024.

- requirement for DNFBPs to implement TFS and conduct PF/sanctions KYC;
- requirement for the maritime sector to implement TFS and conduct PF/sanctions KYC;
- comprehensive legal-regulatory frameworks for VASPs;
  legal basis for inter-agency information sharing on proliferation financing and sanctions evasion at the implementation (not only policy) level.

(3) Strengthen detection capacity

290. The near-total absence of PF STRs and PF investigations reflects limited detection capacity as much as low underlying activity. Strengthened detection capability will depend on introducing PF-specific STR reporting paths (for example, in some jurisdictions, this involves requiring reporting entities to add PF-specific codes to reports to prioritize review), structured feedback loops to reporting entities, and FIU analytical capability. On the latter, FIU's analytical capacity depends on access to Customs/trade/export controls data. Competent authorities should provide awareness-raising training, disseminate PF typologies and lists of Red Flags. As the next step, jurisdictions should invest in developing prosecutorial capacity, ensuring that prosecutors have sufficient expertise to handle PF cases (the lack of PF-specific prosecutorial capacity is a universal problem for many jurisdictions worldwide).

(4) Strengthen export controls on dual-use goods and technology and minimize siloing between financial crime prevention and export control actors

291. Jurisdictions without comprehensive export control regimes should aim to develop, to the extent possible, licensing (permit) regimes, national control lists, and end-use and end-user verification. Noting the region's risk profile, special attention should be paid to the transit, transshipment, re-export, and brokering risks.

292. Jurisdictions should treat export controls and proliferation financing controls as mutually reinforcing tools to deal with proliferation. In practical terms, it means developing platforms and procedures for information-sharing and training opportunities that involve both export control and financial crime prevention authorities.

(5) Encourage PF-focused risk management by all financial institutions

293. Jurisdictions should encourage all financial institutions to move from just list-scanning to trade-based and behavioral PF detection, which relies on additional risk management tools. While larger financial institutions already employ additional tools, it is safe to assume that smaller institutions with less capacity rely mostly on list scanning. Financial institutions will also benefit from building up dual-use goods screening capability. While financial institutions cannot be expected to develop deep technical expertise on dual-use goods and technology, they should understand what they are, what to look for, and where to seek technical expertise if needed.

(6) Deconflicting national priorities and the private sector objectives

294. Some financial institutions overcomply and de-risk due to concerns about secondary sanctions. In some circumstances, it can create tension between national policy and the private sector's behavior on the ground. Jurisdictions will benefit from recognizing this tension and taking appropriate policy decisions if deemed necessary.

(7) Strengthen oversight over FTZs and offer training to companies operating in FTZs

295. Jurisdictions should ensure that supervision, beneficial ownership transparency, and company formation requirements align with the risk profiles of FTZs, especially those with high throughput. Competent authorities should offer training and guidance to companies operating in FTZs on the risks of PF and sanctions evasion, as FTZs are commonly used by proliferators and sanctions evaders.

(8) Strengthen oversight and offer training to the maritime sector

296. Jurisdictions should reinforce due diligence in their vessel registries and incorporate PF and sanctions screening into the registration and licensing process, with the particular attention to open registries and to the high-throughput ports. Panama's example of recently implemented measures can serve as the region's Best Practices.

297. Competent authorities should offer PF and sanctions training and guidance to the maritime sector which appears to be the least covered.

(9) Strengthen oversight and offer training to high-risk DNFBPs

298. Jurisdictions in which supervisors do not monitor/supervise compliance with TFS by TCSPs and dealers of precious metals and stones should consider strengthening their efforts. The illegal gold mining should be seen as a relevant and adjacent vulnerability when it comes to use of gold in proliferation financing and sanctions evasion.

299. High-risk DNFBPs will also benefit from guidance and training on PF and sanctions evasion.

(10) Strengthen oversight and offer training to VASPs

300. Jurisdictions should operationalize recently adopted or soon-to-be-adopted legal and regulatory frameworks and strengthen supervisory oversight of VASPs. Imposing the same KYC and STR requirements on VASPs as on financial institutions in line with FATF Recommendation 15, and ensuring they are met, is critical, given the growing reliance of proliferators and sanctions evaders on virtual assets for illicit activities.

301. Jurisdictions should also address the supervisor gap created by residents' reliance on foreign and offshore VASPs.

302. Competent authorities should offer PF and sanctions training and guidance to VASPs.

(11) Learn from regional peers

303. While one jurisdiction's approach cannot be applied directly to another, there is now a growing wealth of experience across the region in different components of PF-related measures. Jurisdictions can share their experience (both the positive outcomes and the challenges they encountered) with their peers, contributing to overall progress in the region. Even within the constraints of this report, jurisdictions have access to a wealth of information. For example, they can consult the examples of training and guidance provided by the peers (see Table "Select Examples of Guidance on Proliferation Financing" in Section 4.1.2.) or analyze examples of legislation (see Country Matrices in Annex I).



CHAPTER 7

Annexes

7. Annexes

(see in separate documents)

Annex I. Country matrices of CPF regional situation (confidential)

- Country matrix template
- Country matrices

Annex II. Detailed Red Flags for High-Risk Sectors

- Annex II (a) Consolidated list of Red Flags for financial institutions
- Annex II (b) Consolidated list of Red Flags for the dual-use sector
- Annex II (c) Consolidated list of Red Flags for the maritime industry
- Annex II (d) Consolidated list of Red Flags for Free Trade Zones
- Annex II (e) Consolidated list of Red Flags for professional intermediaries (TCSPs; legal professionals (lawyers), accountants, notaries)
- Annex II (f) Consolidated list of Red Flags for dealers in precious metals and stones
- Annex II (g) Consolidated list of Red Flags for VASPs

Annex III. Sample interactive exercise for training purposes

Annex IV. List of relevant resources