Guidance Note on Proliferation and Proliferation Financing

Version 2.0

September 2024

Table of Contents

ACRONYMS

AML/CFT/ CPF	Anti-Money Laundering/Combating Terrorist Financing and Countering Proliferation Financing
CBA	Centrale Bank van Aruba
DNFBPs	Designation Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
EU	European Union
FATF	Financial Action Task Force
FIU-Aruba	Financial Intelligence Unit-Aruba
KYC	Know Your Customer
ML	Money Laundering
OFAC	Office of Foreign Assets Control
PF	Proliferation Financing
SDN List	Specially Designated Nationals List
TF	Terrorist Financing
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction
TFS	Targeted Financial Sanctions
VASP	Virtual Asset Service Provider

GLOSSARY

In the context of proliferation and proliferation financing, it is important to have the following common understanding of certain terms and concepts used throughout this Guidance Note.

Dual-use Goods	Dual-use goods are items that have both commercial and military or proliferation applications. These goods could be components of a weapon or items used in the manufacturing of a weapon (e.g. specific machine tools for repairing automobiles which could also be used to manufacture a missile). These items are generally controlled by governments via export controls, which prevent the export of certain items depending on the end user and end use of the item.
Hawala	Hawala is an informal value transfer system common in the Middle East, North Africa, and the Indian subcontinent. It involves an international transfer of value outside the legitimate banking system and is based on a trusted network of individuals. In a basic form, a customer contacts a hawaladar (a hawala broker) and gives him/her money to be transferred to another person. The hawaladar contacts his/her counterparts where the beneficiary lives, who remits the funds to that person. A running tally is kept between the hawaladars of whom owes the other a net sum.
Non-state actors	The United Nations Security Council Resolution (UNSCR) 1540 (S/RES/1540, April 28, 2004) defines "non-state actors" in proliferation as individuals or entities not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution. Non-state actors in proliferation include organizations and individuals that are not affiliated with, directed by, or funded through the government (e.g. corporations, private financial institutions, terrorist groups, paramilitary and armed resistance groups, etc.).
Proliferation	Proliferation involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical, or biological weapon-related programs, including delivery systems.
Proliferation Financing (PF)	PF is the act of providing funds or financial services which are used in whole or in part for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Proliferator	A proliferator is an individual or group of individuals that abuses both the formal and informal sectors of the international financial system or resorts to cash in order to trade in proliferated goods. (FATF Report: "Combating Proliferation Financing", 2010).
State proliferation actor	A state proliferation actor is one who acts as a proliferator of nuclear, chemical, or biological weapons and their means of delivery and related materials.
Targeting jurisdiction	A targeting jurisdiction is one that has been specifically identified due to its involvement in proliferation of weapons of mass destruction (nuclear, chemical, or biological weapons).
Weapons of Mass Destruction (WMD)	WMD are atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above (1977 United National General Assembly Resolution A/RES/32/84-B).
End-use	The ultimate purpose of use for the exported goods.
End-user	The ultimate intended user of the goods. Not necessarily the person or organization to whom the goods are exported.
Means of delivery	The part of a weapon system that serves to deliver a weapon to a target (i.e. missiles, rockets, and other unmanned systems capable of delivering nuclear, chemical, or biological weapons for mass destruction).
Proliferation-sensitive goods	Nuclear, chemical, or biological equipment, material, or technology used in the research, design, development, testing, or production of nuclear, chemical, or biological weapons.
Related materials	Materials, equipment, and technology which could be used for the design, development, production or use of nuclear, chemical, and biological weapons and their means of delivery.
Sanctions list	A list of person and entity names who are subject to sanctions which may include restricting or prohibiting trade, financial transactions or other economic activity between a country and the target state, as well as the seizure or freezing of property.
Targeted financial sanctions	Financial measures imposed on designated persons, groups, and entities to impede their access to funds and resources. The term means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons, groups, and entities on sanctions list.

Trade finance	The financing of the movement of goods and services, both within the country's boundaries as well as cross border. Trade finance activities entail money transmissions, default undertakings, performance undertakings and the provision of credit facilities.
Transshipment	The shipment of goods which are not destined for end-use in a country but are passing through it en route to another country.
Letter of credit	A binding document that a buyer can request from a bank to guarantee that the payment for goods will be transferred to the seller. It is a letter issued by a bank to another bank to serve as a guarantee for the payment of goods to a specific person under particular circumstances..

I. INTRODUCTION

Proliferation and its financing is a less understood challenge than money laundering (ML) and terrorist financing (TF). The proliferation of weapons of mass destruction (WMD), including their means of delivery, poses a significant threat to global security. Proliferation financing (PF) is quickly evolving as a threat as actors find innovative ways to disguise funds using financial transactions that include shell or front companies, bearer shares, and offshore secrecy havens. Countering the flow of funds to proliferation actors and preventing the procurement of illicit goods and technology necessary for the development of WMD play a key role in combating the risks posed by the proliferation of WMD.

IF A 10-KILOTON NUCLEAR BOMB IS DETONATED IN A POPULATED AREA IN, FOR EXAMPLE, THE USA, ESTIMATED FATALITIES WILL EXCEED 54,000 PEOPLE, AND INJURIES WILL EXCEED 86,000 PEOPLE. THE NUCLEAR FIREBALL WILL REACH 650 FEET INTO THE SKY, AND ANYTHING WITHIN IT WILL VAPORIZE. RADIATION, THERMAL, AND LIGHT BLAST DAMAGE WILL COVER MILES. SUCH A NUCLEAR DENOTATION IN ANY PART OF THE WORLD WILL BRING DEVASTATION OF AN UNIMAGINABLE SCALE.

'Countering the Challenges of Proliferation Financing' by
Dr. Togzhan Kassenova and Dr. Bryan R. Early

Aruba is not considered a weapons manufacturing jurisdiction or an international trade center or a market of proliferation goods.[1] Whilst there may be no direct PF links due to its geographical location, Aruba can be targeted as a transshipment center[2] for dual-use goods, proliferation-sensitive items, or military goods. Furthermore, Aruba is also likely to be exposed to proliferation and its financing as a result of its cross-border business in the international financial market, as well as financial transactions and activities in or from Aruba. In this context, financial institutions and designated non-financial businesses and professions (DNFBPs) should consider the PF risks carefully in view of their potential severe impact. Proliferators utilize diverse and constantly evolving methods to disguise their illicit activities and the networks they control to deliberately spread their operations across multiple jurisdictions. Involvement in proliferation or its financing, even if inadvertent, carries the risk of severe reputational damage to institutions, including designating individuals and entities on sanctions list, or being denied access to banking and other services.

II. PURPOSE, SCOPE, AND APPLICABILITY

This Guidance Note applies to all financial institutions and DNFBPs. It has been issued in an effort to raise awareness among the institutions supervised by the Central Bank of Aruba (CBA) of the risks and vulnerabilities posed by proliferation and its financing, and the effects to the reputation of Aruba if a supervised institution, intentionally or unintentionally, becomes involved in PF. It aims to help the supervised financial institutions and DNFBPs understand the risks of PF and comply with existing national laws and regulations, and international standards (i.e. targeted financial sanctions related to PF).

Having reviewed this revised guidance note, supervised financial institutions and DNFBPs may wish to revisit the following areas to consider whether they have adequately addressed PF:

- Provision of staff training;
- Implementation of policies, procedures and measures;
- Conduct of risk assessments of customers and products with emphasis on, inter alia, trade finance;

[1] Press release, *Aruba Completes its Terrorist Financing and Proliferation Financing National Risk Assessment,* July 7, 2021, available at: https://www.government.aw/news/news_47033/item/aruba-completes-its-terrorist-financing-and-proliferation-financing-national-risk-assessment_56936.html.

[2] A "transshipment center" is defined as a port where merchandise can be imported and then exported without paying import duties.

- Application of enhanced due diligence on higher risk transactions and customers.

III. LEGAL NATURE

This guidance note is intended for use as a general guide and does not carry the force of law. Reference for that purpose shall be made to the relevant statutory requirements cited in the references at the end of this document. The guidance note is subject to periodic review and amendments in view of emerging PF risks and developments. It should be read in conjunction with the AML/CFT State Ordinance and the AML/CFT/CPF Handbook.

IV. OVERVIEW OF PF

1. What is Proliferation?

The Financial Action Task Force (FATF)'s 2008 Typologies and Proliferation Financing Report[3] defines "proliferation" as follows:

> "Proliferation involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programs, including delivery systems."

2. What is PF?

PF has no internationally accepted definition. The FATF provided a working definition of PF in 2010 which is based on UNSCR 1540 (2004).[4] However, in 2021, the FATF updated the definition of PF, which refers to:

> "Financing of proliferation is (…) raising, moving or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)."

[3]FATF, *Proliferation Financing Report*, June 18, 2008, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf.

[4]UNSCR 1540, S/RES/1540 (April 28, 2004), available at: https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004). The resolution requires all States to adopt and enforce appropriate laws and undertake effective measures to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery to non-State actors, in particular, for terrorist purposes. Subsequently, the UNSC issued successor resolutions with regard to nuclear-related activities of the Democratic People's Republic of Korea (DPRK) (UNSCR 1718) and the Islamic Republic of Iran (UNSCR 2231).

In June 2021, the FATF provided an explanation to its working definition, which delineate that PF refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (entailing both dual use technologies and dual-use goods for non-legitimate purposes).[5] Access to the financial system and financial services is central to proliferation efforts. As such, disrupting the financing of such activities is key to countering the spread of WMDs. PF facilitates the movement and development of proliferation-sensitive items, and subsequently, it can contribute to global instability and potentially catastrophic loss of life if WMD are developed and deployed.

3. Types of PF

PF can be divided into two types:

Terrorism financing – where it provides financial support to terrorist organizations that would want to acquire and/or use a WMD.

+

Financing from a state, or **a state-controlled or state-sponsored entity** with the aim of providing a state with a WMD, or to enhance, improve or replace an existing one.

4. Three stages of PF

The financial elements of a WMD program can be divided into three stages:[6]

Stage 1*: *FUND RAISING – the proliferator raises funds for the program through its domestic budget, which can be also supplemented with funds raised by networks overseas or by criminal activity.

Stage 2*: *DISGUISING THE FUNDS – the proliferator transfers the funds into the international financial system, often involving a foreign exchange transaction, for trade purposes.

Stage 3*: *PROCUREMENT OF MATERIALS AND TECHNOLOGY – the proliferator uses these funds in the international financial system to pay for goods, materials, technology, and logistics necessary for its WMD program, either directly to manufacturers or more likely via brokers or trading companies.

The process is significantly more challenging during the second stage for countries subject to comprehensive sanctions such as the Democratic People's Republic of Korea (DPRK). Proliferators often depend on extensive network of businesses, including front companies and middlemen to disguise any link to sanctioned countries. Typically, during the third stage, the international financial system becomes involved in processing PF related transactions. PF activities may resemble legitimate trading transactions.

[5] FATF, *Guidance on PF Risk Assessment and Mitigation*, June 2021, available at: https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html.
[6] Dr Jonahan Brewer, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation*, CNAS, January 2018.

It is noteworthy to mention that modern proliferation does not merely involve the purchase of a complete WMD system. Instead, many proliferators seek individual goods and elementary component parts that can be utilized to develop WMD and missile programmes. This complicates the detection of proliferation activities and the determination of whether the goods will be used for illicit purposes. For this reason, it is crucial to understand the entire payment chain and consider how any trade may facilitate illicit activity.

In complex structures, PF may not be directly connected to the physical flow of goods. As such. PF may include, among other things, the following:

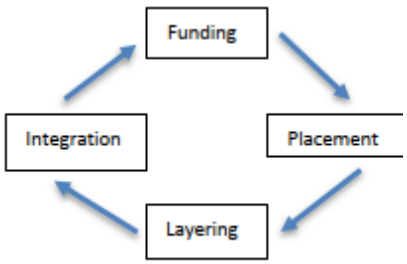
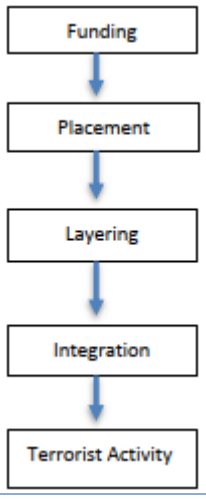
- Financial transfers
- Provision of loans
- Ship mortgages and registration fees
- Insurance and re-insurance services
- Credit lines for shipment of illicit sensitive goods
- Trust and corporate services
- Acting as an agent for, to, or on behalf of someone else
- Facilitation of any of the above.

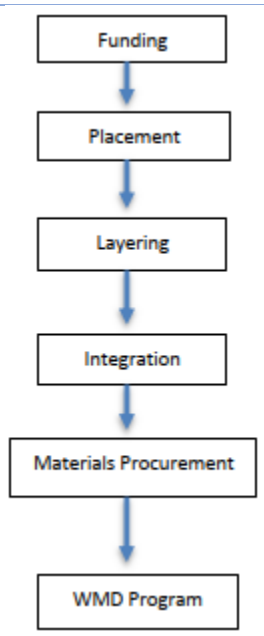
5. Comparison of PF with ML and TF

The following table provides an overview of the differences and similarities between ML, TF, and PF.[7]

	ML	TF	PF
Motivation	Profit-seeking	Religious, political and/or psychological ideology Publicity for the cause and political influence	Either due to ideology (e.g. to support a sanctioned state) or for power/recognition and/or profit
Intention	To make ill-gotten proceeds appear to be legitimate	To intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence	Acquire goods that can contribute to WMD programs without detection
Source of Funding	Internally from within criminal organizations (unlawful sources – e.g. extortion, kidnapping, narcotics, smuggling, fraud, theft, robbery, identity theft, tax evasion, improper use of charitable or relief funds and other forms of criminal activity)	Internally from self-funding cells (unlawful sources – e.g. smuggling, fraud, theft, robbery, identity theft, improper use of charitable or relief funds and donors may have no knowledge that their donations have been diverted to	Often state-sponsored programs, but also through fundraising activities by non-state actors (e.g. charitable donations, foreign government sponsors, business ownership and personal employment)

[7] Jonathan Brewer, *Study of Typologies of Financing of WMD Proliferation* (October 13, 2017), available at: https://menafccg.com/wp-content/uploads/2017/11/Study-of-typologies-of-FoP-October-2016_-002.pdf.

		support terrorist causes) Externally from benefactors and fundraisers (lawful sources – e.g. charitable donations, foreign government sponsors, business ownership and personal employment)	
Conduits	Favors formal financial system	Favors cash couriers or informal financial systems such as Hawala and currency exchange companies	Favors formal financial system
Stages	Funding – Placement – Layering - Integration	Fund raising- Moving- Use of Funds or Other Assets	Fund raising – Disguising the funds – Procurement of Materials and/or Technology
Transaction Amounts	Large amounts often structured to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts which may possibly be above the reporting threshold
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens	Various methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables	Transactions look like ordinary commercial activity, structured to hide origin of funding and connection to proliferator or proliferation activities
Money Trail	Circular – money eventually ends up with the person who generated it 	Linear – money generated is used to promote terrorist groups and activities 	Linear – money generated is used to purchase goods and materials from brokers or manufacturer for the development of WMD

			
Detection Focus	Identify a suspicious activity (e.g. transactions and/or behaviors, such as deposits not in line with customer's wealth or the expected activity)	Identify suspicious relationships, such as wire transfers between seemingly unrelated parties and/or to high-risk or blacklisted countries	Identify suspicious individuals, entities, States, goods, materials, and activities
Cross-border activities	Yes, likely to involve nationals or legal entities associated with jurisdictions of proliferation and/or diversion concern, as well as countries with weak export control laws or weak enforcement thereof. Make use of organized or transnational crime networks, particularly their transport corridors and intermediaries in their networks for goods and/or funds	Yes, likely to involve use of smaller correspondent banks located in countries with weak AML laws	Yes, likely to involve the use of organized or transnational crime networks, specifically their transport corridors and intermediaries in their networks

6. International Standards and Obligations to Counter Proliferation and PF Risks

The international framework to counter proliferation and its financing relies on two interrelated sets of obligations: (i) international legal obligations imposed by the UNSC, and (ii) the FATF Recommendations. Aruba has implemented laws and regulations to comply with these international standards (see section 6 below).

6.1 *UNSC Resolutions*

International obligations to combat the financing of proliferation are contained primarily in a number of UNSC Resolutions (UNSCRs). There are two UNSCRs which oblige countries, including Aruba, to implement the relevant PF obligations.

a) **UNSCR 1540 (2004)** entails the implementation of broad-based provisions to prevent non-state actors and targeted jurisdictions from acquiring WMD, their means of delivery of WMD,[8] and other related materials.[9] It prohibits the financing of proliferation-related activities by non-state actors and requires countries to establish, develop, review, and maintain appropriate controls on providing funds and service, such as financing, related to the export and transshipment of items that would contribute to WMD proliferation.
b) **UNSCR 1718 (2006)**[10] was adopted in response to the DPRK's nuclear test program. The scope and nature of DPRK-related sanctions have been expanded following the country's repeated violations of UN Resolutions.

Note that as of October 18, 2023, the targeted financial sanctions on 23 individuals and 61 entities designated on the list established pursuant to the UNSCR 2231 (2015) endorsing the Joint Comprehensive Plan of Action (JCPoA) on the Islamic Republic of Iran (Iran) have ceased to apply.[11] The UNSCR 2231 List has since been removed from the UNSC website and corresponding changes were made to the UNSC Consolidated List.

6.2 *FATF*

Similar to the approach taken by the UNSC, the FATF sets standards implementing targeted financial sanctions related to the prevention, suppression and disruption of proliferation of WMD and PF. These standards are laid down in the FATF Recommendations, interpretative notes, and methodology.

[8] Means of delivery involve missiles, rockets, and other unmanned systems capable of delivering nuclear, chemical, or biological weapons that are specially designed for such use.
[9] Related materials involve materials, equipment, and technology covered by relevant multilateral treaties and arrangements or included on national control lists, which could be used for the design, development, production, or use of nuclear, chemical, and biological weapons and their means of delivery.
[10] The successor resolutions, as of February 15, 2024, to UNSCR 1718 (2006) are: 1874 (2009), 1887 (2009), 1928 (2010), 1985 (2011), 2050 (2012), 2087 (2013), 2094 (2013), 2141 (2014), 2207 (2015), 2270 (2016), 2276 (2016), 2321 (2016), 2345 (2017), 2356 (2017), 2371 (2017), 2375 (2017), 2397 (2017), 2407 (2018), 2464 (2019), 2515 (2020), 2569 (2021), 2627 (2022), and 2680 (2023).
[11] The JCPoA is an agreement reached in 2015 between Iran and its negotiation partners (the UK, China, France, Germany, Russia, and the USA) to impose restrictions on Iran's nuclear program in exchange for the removal of sanctions. This agreement was endorsed by UNSCR 2231. However, on Transition Day (October 18, 2023), all nuclear-related sanctions against Iran were lifted even though Iran did not fulfill its commitments under the JCPoA. These sanctions include restrictions on ballistic missile technologies, the proliferation of sensitive technologies, and the designation of individuals and entities associated with Iran's nuclear and ballistic missile programs.

FATF Recommendation/Immediate Outcome	Description
Recommendation 1	This recommendation was revised in October 2020. It requires countries, financial institutions, DNFBPs, virtual asset service providers (VASPs), and non-profit organisations to identify and assess the risks of potential breaches, non-implementation or evasion of targeted financial sanctions related to PF and to take action to mitigate them.
Recommendation 2	This recommendation was revised in October 2020. It calls on cooperation and coordination of the relevant authorities to combat ML, TF, and PF.
Recommendation 7	This recommendation requires countries to implement targeted financial sanctions to comply with the UNSCRs relating to the prevention, suppression, and disruption of proliferation of WMDs and its financing. The UNSCRs require countries to freeze *without delay*[12] the funds or other assets of and 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 UNSC under Chapter VII of the United Nations (UN) Charter. Recommendation 7 is **not** risk-based. The Interpretative Note to Recommendation 7[13] draws further attention to the need for financial institutions to implement preventive measures to counter the flow of funds or assets to proliferators or those who are responsible for proliferation of WMD.
Recommendation 15	This recommendation was revised in June 2021. It requires countries and financial institutions to conduct a PF risk assessment and establish mitigation in respect of virtual asset activities and service providers.
Immediate Outcome 1	It requires coordinated domestic actions to counter PF.
Immediate Outcome 11	It requires countries to demonstrate that they fully and accurately implement targeted financial sanctions "without delay".

[12] The phrase "without delay" means within a matter of hours of a designation by the UNSC or its relevant Sanctions Committee (i.e. 24 hours).
[13] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (the FATF Recommendations), adopted in 2012, updated in October 2020, Paris, France, available at www.fatf-gafi.org/recommendations.html.

It is important to note that UNSCR 2231 serves as the legal basis for certain elements of FATF Recommendations 1 and 7, and its scope has affected the requirements on PF. After October 18, 2023, FATF Recommendation 7 no longer mandates countries to apply targeted financial sanctions to individuals and entities designated under UNSCR 2231. Similarly, FATF Recommendation 1 no longer requires the assessment or mitigation of PF risks associated with such individuals and entities. Even though this change affects UN designations related to Iran and consequently part of the FATF Recommendations, such individuals and entities may continue to be subject to targeted financial sanctions under national and regional sanctions authorities. In this context, further clarification on the national laws and regulations in Aruba is provided in section 7 below. The requirements of Recommendation 7 remain applicable to entities designated under UNSCRs relating to DPRK, and the PF requirements of Recommendation 1 continue to apply to DPRK-related PF risks.

7. National Laws and Regulations

For the purpose of addressing the potential risk of PF and to comply with the mentioned international standards, Aruba has adopted and issued:

- *Sanctions State Ordinance 2006 (AB 2007 No. 24)*

This state ordinance grants the Government of Aruba the power to adopt State Decrees containing General Administrative Orders for the implementation of international obligations (article 2). Such a State Decree containing General Administrative Orders may impose a restriction, a prohibition, or a burden on the citizens of Aruba. On the basis of the sanctions state ordinance, both UN sanctions and European Union (EU) sanctions targeting financial sanctions related to the prevention, suppression, and disruption of WMD can be incorporated into Aruban legislation.

- *Sanctions State Decree North Korea (AB 2017 no.42*)

This state decree provides for a targeted financial sanctions regime in implementation of UNSCR 1718 (2006) and its successor resolutions.

- *Interim State Decree Priority Sanctions Regimes (AB 2019 no.47) (including its respective amendments)*

This state decree provides for a targeted financial sanctions regime to a number of regulations and decisions, adopted within the framework of the Common Foreign and Security Policy of the EU, to the degree that they are intended to maintain or restore international peace and security or to promote international legal order.[14] This Sanctions State Decree covers a broad country-specific targeted financial sanctions provision against, inter alia, the DPRK, together with Iran.[15]

[14] The Interim State Decree Priority Sanctions Regimes requires the freezing of all funds and other assets of persons and organizations mentioned in the annex of this State Decree.

[15] Reference is made to Annex I of the Interim State Decree Priority Sanctions Regimes under the sections DPRK and Iran for an overview of the adopted EU Resolutions and Decision with regard to these countries.

- *Sanctions State Decree Chemical Weapons (AB 2021 no.31)*

This state decree implements the EU sanctions regime concerning restrictive measures against the proliferation and use of chemical weapons aimed at the freezing of funds or other assets.[16]

- *Sanctions State Decree Iran (AB 2021 no. 141)*

On September 3, 2021, the Sanctions State Decree Iran (AB 2021 no. 141) implementing the UNSCR 2231 (2015) with regard to the targeted financial sanctions against certain persons, entities, and bodies of Iran was enacted. However, on October 18, 2023, the targeted financial sanctions on 23 individuals and 61 entities designated on the list established pursuant to the UNSCR 2231 (2015) were lifted and ceased to apply. In light of these recent changes, on March 14, 2024, this sanctions state decree was repealed and is no longer in force.[17]

Notwithstanding the aforementioned, note that the Interim State Decree on Priority Sanctions Regime (AB 2019 no. 47), which implements the restrictive measures of the EU regarding Iran s indicated above, is still in force and provides for sanctions against persons, legal entities, and bodies subject to restrictive measures mentioned in the corresponding annexes of Annex I to this state decree.

- *State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (AB 2011 no. 28)*

This state ordinance was amended in September 2021 to include PF requirements for financial institutions and DNFBPs, inter alia, establishing adequate and written policies, procedures, and measures aimed at preventing and combating PF; conducting PF business risk assessment; undergoing regular PF related training; monitoring of transactions for timely detection of potential PF or any related patterns; and reporting unusual transactions related to PF.

- *Handbook for the Prevention and Detection of Money Laundering and Financing of Terrorism for Services Providers (financial and designated non-financial) (AML/CFT Handbook)*

With respect to targeted financial sanctions related to proliferation, the CBA stipulates in its AML/CFT Handbook, dated January 1, 2020 that entities[18] that fall under the scope of the AML/CFT State Ordinance must take PF risks into consideration when carrying out their periodic evaluations of the extent to which their activities and operations expose them to the risk of PF ("business risk assessment") (paragraphs 3.3.3 and 11.1.2 of the AML/CFT Handbook).

The CBA is entrusted with overseeing compliance with the obligations under, among other laws and regulations, the Sanctions State Ordinance 2006, the Sanctions State Decree North Korea, the Interim State Decree Priority Sanctions Regimes, along with the AML/CFT Handbook.[19]

---

[16] The Sanctions State Decree Chemical Weapons implements Regulation (EU) No. 2018/1542 of the Council of the European Union of October 15, 2018, and Decision (CFSP) 2018/1544 of October 15, 2018, concerning restrictive measures against the proliferation and use of chemical weapons.

[17] Reference is made to State Decree repealing Sanctions State Decree Iran (AB 2024 no. 9) (published on March 13, 2024), available at: https://www.cbaruba.org/readBlob.do?id=16821.

[18] These entities include all financial institutions and DNFBPs that fall under the scope of supervision of the CBA.

[19] Pursuant to the Sanctions State Ordinance 2006 (AB 2007 no.24), the CBA informs the supervised financial institutions and DNFBPs, by letter of all new decrees and regulations that have been enacted by the Government of Aruba. The supervised financial institutions and DNFBPs are required to take measures to ensure that they keep abreast of the content of the freezing lists and all changes made and to otherwise ensure that they comply with the requirements and prohibitions set in sanctions regulations/decrees in a timely manner. Further, the CBA requires that all supervised institutions take adequate measures to identify possible relationships or transactions with the persons listed therein.

8. Understanding How Proliferators Operate

Several typologies[20] delineate a number of characteristics attributed to proliferators and their complex networks. These typologies include the following:

Proliferators:	Proliferation networks are composed of proliferators who:
Operate globally and exploit global commerce	Abuse both the formal/informal sectors of the international financial system by using ordinary financial transactions to pay intermediaries and suppliers outside the network
Disguise their acquisitions as legitimate trade	Use cash to trade in proliferation types of goods to bypass the system
Operate in countries with high volumes of international trade	Purchase proliferation-sensitive goods/services in the open market and make them appear legitimate to avoid suspicions of proliferation (e.g. purchase of dual-use goods)
Exploit weaknesses in global commerce controls (i.e. they operate in countries with weak export controls or utilize free-trade zones where their procurements and shipments might escape rigorous control)	Conduct financial transactions in the banking system through fake intermediaries, front companies, and illegal trade brokers
N/A	Create complex procurement networks to avoid detection of the true end-users of proliferation-sensitive goods

9. PF Red Flag Indicators & Potential PF Risks

The prime purpose of the following red flags and indicators is to illustrate common situations that may pose potential PF-related risks. This section also aims to enhance the understanding of the risks posed by the financing of proliferation, which may be affiliated with certain customers, transactions, methods, or jurisdictions. Nevertheless, these indicators are not exhaustive, but serve as a foundation for the type of measures that a supervised institution should implement for the purpose of detecting, mitigating, and deterring the risks associated with proliferation and its financing.

The red flag indicators have been categorized under a number of sections. The presence of a single red flag may not automatically make a transaction suspicious. However, a combination of the red flags below with other indicators may require a financial institution or DNFBP to conduct a deeper investigation. If there is an activity that raises a ML/TF/PF suspicion, a financial institution or DNFBP is required to report such suspicion subjectively to the FIU-Aruba.

[20]FATF, *Proliferation Financing Report*, 18 June 2008, available at https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf.

Financial institutions and DNFBPs must understand the different scenarios where customers, transactions and other account activities may indicate involvement in PF. It is imperative for financial institutions and DNFBPs to conduct enhanced customer due diligence before providing services to customers that are red flagged, as well as to perform ongoing transaction monitoring throughout the business relationship with such customers. The CDD performed and the ongoing transaction monitoring need to be adequately documented.

a. *Customer Red Flag Indicators*

- The customer is involved in the supply, sale, delivery, or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions.
- The customer is physically located in proliferation countries/diversion concern (e.g. through business or trade relations).
- The customer has ties with a foreign country of proliferation concern, or a neighboring or sympathetic country. The customer has previously had dealings with individuals or entities now designated for proliferation by the UNSC.
- The customer or counterparty, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists (e.g. OFAC, UN, EU Sanctions Lists).
- The customer is a university, military or research institution connected with a higher risk jurisdiction of proliferation concern and/or is involved in the trading of dual-use goods or goods subject to export control.
- The customer's activities do not match the business profile, or the end-user information does not match the end-user's business profile. A customer engages in a transaction that lacks business sense or strategy, or that is inconsistent with its historical pattern of trade activity.
- The customer is vague about the end user(s) and end use, provides incomplete information, or is resistant when requested to provide additional information when it is queried.
- A new customer requests a letter of a credit transaction awaiting the approval of a new account.
- A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control.
- The customer uses complicated structures to conceal involvement - for instance, use of layered letters of credit, front companies, intermediaries, and brokers.
- The customer is a person dealing with dual-use goods, goods subject to export control, or complex equipment for which he/she lacks technical background, or that is inconsistent with its stated line of activity.

b. Transaction Red Flag Indicators

- The transaction(s) concern(s) dual-use, proliferation-sensitive, or military goods, whether licensed or not.
- The transaction(s) involve(s) an individual or entity in a foreign country of proliferation concern.
- The transaction reflect(s) a link between representatives of companies (e.g. same owners or management) exchanging goods to evade scrutiny of the goods exchanged.
- The transaction(s) involve(s) the shipment of goods inconsistent with normal geographic trade patterns i.e. where the country involved does not normally export or import the types of goods concerned (e.g. goods are shipped through several countries for no apparent reason).
- The order for goods is placed by companies or individuals from countries other than the country of the stated end-user.
- A transaction involves possible shell companies.

- A trade finance transaction involves shipment route through a country with weak export control laws or weak enforcement of export control laws.
- The transaction structure (whether shipping route, financing arrangement or documentation) appears unnecessarily complex or irrational.
- The description of the goods on the trade/financial documentation is non-specific or misleading.
- Transactions involve country of diversion concern (e.g. China, Hong Kong, Singapore, and Malaysia).
- Transactions include countries that are known to trade with DPRK (including Egypt, Yemen, Iran, Syria, and the United Arab Emirates).
- Transactions involve financial institutions with known deficiencies in AML/CFT/CPF controls or located in weak export control and enforcement jurisdiction (e.g. it is known that DPRK has used correspondent accounts held with Chinese banks to facilitate its international financial transfers).
- Evidence or suspicion that documentation or other representation are fraudulent/fake.
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously undervalued in line with the shipping cost.

c. Country/Jurisdiction Red Flag Indicators

- Countries with weak financial and export safeguards, and which are actively engaged with a sanctioned country.
- The presence of an industry that produces dual-use goods, proliferation-sensitive items, or military goods.
- Countries that are neighboring or sympathetic to the interests of Iran or DPRK.
- Deliberate insertion of extra links into the supply chain (e.g. diverting shipments through a third country).
- The use of countries were their laws make it difficult to determine the beneficial ownership behind a corporate structure.
- A route of shipment of goods or transactions inconsistent with normal geographical patters or the customer's expected business activity.
- Countries which may present ongoing and/or substantial ML/TF/PF risks or have strategic deficiencies in the fight against ML/TF/PF (e.g. jurisdictions under increased monitoring identified by the FATF).
- Countries which have strong links (such as funding or other support) with terrorist activities or organized crime.
- Countries that are known to have weak import/export control laws or poor enforcement.
- Countries that do not have the required level of technical competence with regard to dual-use goods involved.

d. Other Red Flag Indicators

Trade Finance

- The final destination or end-user is unclear.
- Inconsistencies in information contained in trade documents and financial flow, e.g. names, addresses, final destination.
- The use of fraudulent documents and identities (e.g. false end-use certificates and forged export certificates or re-export certificates).

- Wire instructions or payment from or due to entities are not identified on the original letter of credit or other documentation.
- The use of facilitators to ensure that the transfer of goods avoids inspection.
- Identifying documents seems to be forged or counterfeited/tampered or modified documents with no apparent explanation, especially those related to international trade.

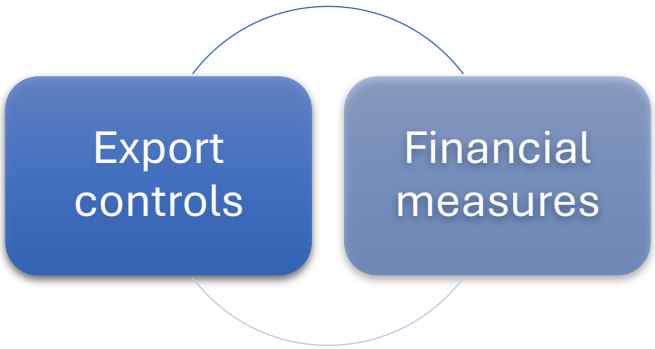
Maritime Sector

- An order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- Declared value of shipment is undervalued via-a-vis the shipping cost.
- A freight forwarding firm is listed as the product's final destination.
- Pattern of wire transfer activity demonstrates unusual patterns or has no apparent purpose.
- Transactions include wire instructions or payment details from parties not identified on the original letter of credit or other documentation.
- The destination of a shipment is different from importer's location.
- A shipment of goods is inconsistent with normal geographic trade patterns, e.g. the destination country does not normally export or import the goods listed in trade transaction documents.

10. What is required from the Supervised Financial Institutions and DNFBPs in Aruba?

Aruba is not adjacent to any of the countries identified as a threat for proliferation or its financing (e.g. the DPRK or Iran). However, due to its solid and reliable financial sector, the threat associated with PF derives predominantly from the possibility that the financial system of Aruba can be potentially misused to launder illicit money, which subsequently may be used for the financing of proliferation of WMD. Proliferation financing vulnerabilities exist in global commerce, international trade, free-trade zones, and shipping, among other areas. Countering proliferation financing is crucial for the purpose of blocking efforts of proliferating states, actors, and complex proliferation networks to procure goods and technology needed for their illicit WMD programs.

There are two recognized mechanisms for targeting proliferation and its financing, being:



Export controls serve as important counter-proliferation measures, aiming at preventing the illegal transfer of sensitive goods by proliferators who disguise their activities as legitimate trade through exploiting the global commerce. Financial measures, on the other hand, complement effective export controls by targeting the financial activity linked to proliferation. Proliferation networks leverage the international financial system to facilitate transactions and business activities.

Given the identified Medium risk of PF in Aruba, financial institutions and DNFBPs should be aware of the PF red flags indicators as listed above.[21] PF risks are more likely to be evident in cases where the source of funds is legal and the end-user of a type of goods involved is vague, making identification of such activities problematic. Identification and detection of PF presents its challenges given that most transactions occur within normal business transaction processes and can be masked along with all other legitimate transactions. Additionally, identifying PF is not limited to individuals and entities designated on sanctions lists. It may also involve other actors with no apparent connection to designated entities and individuals.

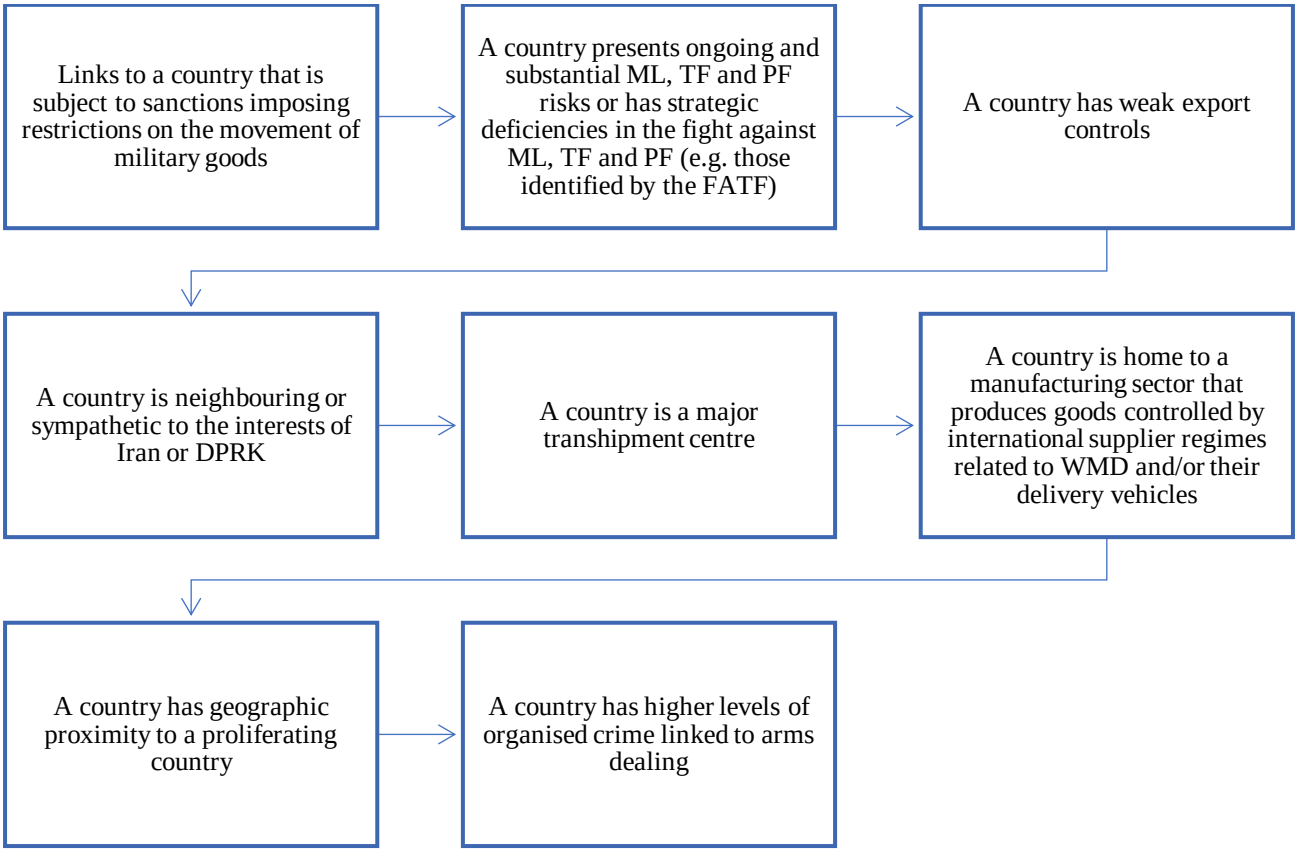
Given that proliferation networks utilize the international financial system to conduct transactions and business activities, financial institutions and DNFBPs should remain vigilant to the possibility that their customers may be involved in or facilitating proliferation activities. They must also develop a clear understanding of contextual information and sources of PF risk they are exposed to and take appropriate mitigation measures. Taking into consideration the content of this (revised) Guidance Note, financial institutions and DNFBPs should take the following actions:

I. Carry out a business risk assessment tailored to the specific business to determine their exposure to PF. The risk assessment should consider risks related to customers, vendors, suppliers, end-users, third parties involved in particular areas of the business, as well as products and services offered, geographies, transactions, and delivery channels used. It is up to the institution to determine whether the PF risk assessment is a separate document or forms a (separate) part of a document covering ML and/or TF. Generally, an institution with international operations or clientele will assess a broader range of risks, including PF risks, compared to a smaller, domestically focused institution.

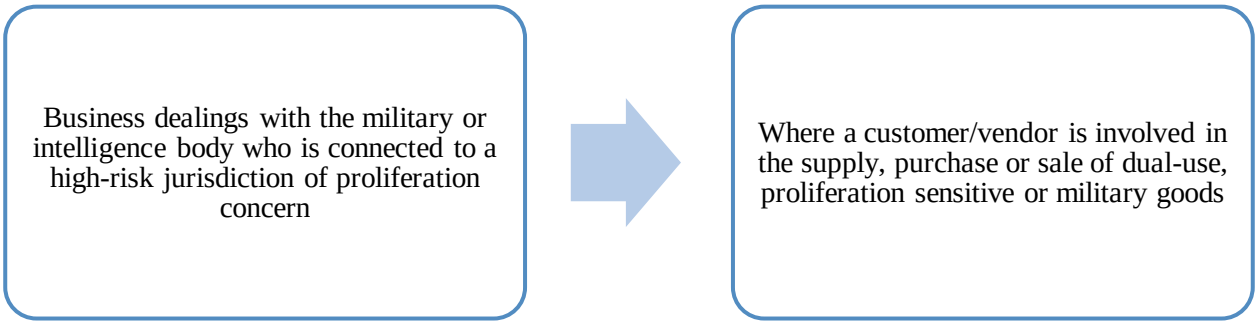
   The following activities may be relevant in developing a proliferation focused risk assessment which may indicate a higher PF risk:

[21] On June 10, 2021, the Prime Minister of Aruba, in the capacity of Chair of the AML/CFT Steering Committee, approved and adopted the TF and PF national assessment report. The national risk assessment resulted in an overall PF risk rating of Medium for Aruba. The threat level for PF in Aruba is considered Low, but the vulnerability to PF is considered High. The risk rating is mainly the result of deficiencies in Aruba's legislative framework with regard to PF, limited awareness in both the public and private sectors on PF red flag indicators, and lack of implementation of effective controls to prevent the import and export of dual-use goods, including the need for better national cooperation and coordination among competent authorities in the prevention and combating of PF.

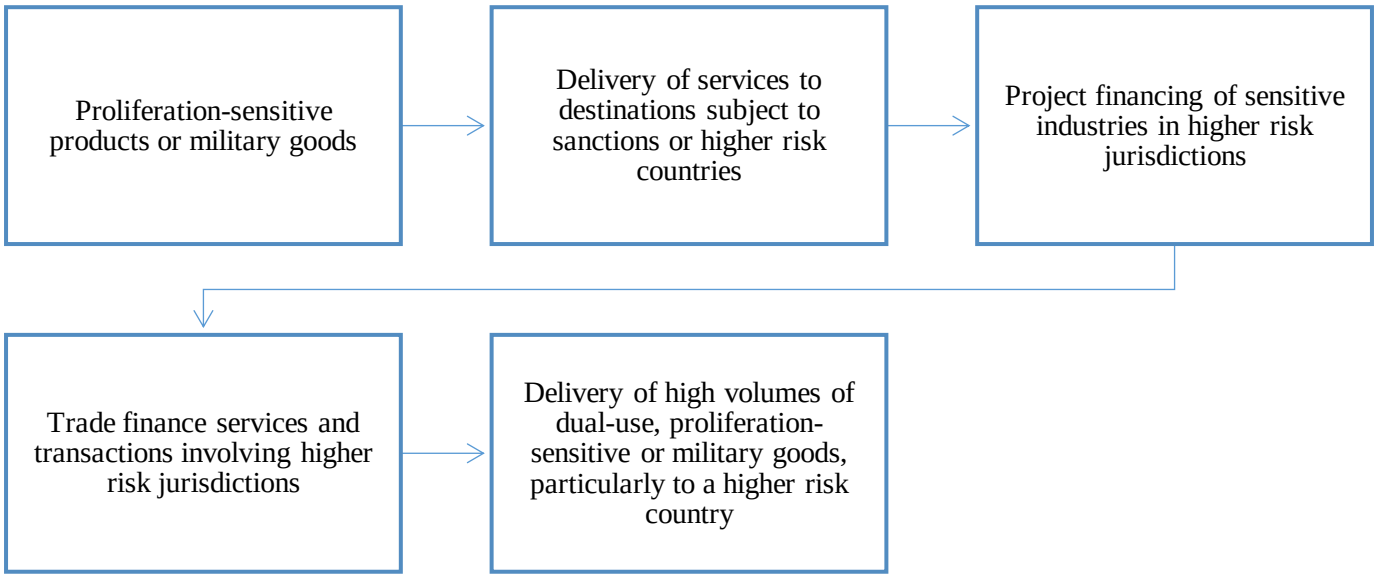
A. Country/Geographic Risks:



B. Customer Risks:



C. Product and Service Risks:



II. Conduct appropriate customer due diligence to detect PF, including screening against sanctions lists of their customers, beneficial owners, vendors/suppliers, and take the necessary actions when the screening results match against the sanctions lists (e.g. UN and EU).

III. Implement systems and controls to monitor and report PF, namely:

- Periodic review and update of the risk assessment taking into consideration any changes in products, customers, and geographical risk factors.
- Implement or adapt policies, procedures, and measures to incorporate the risks posed by PF.
- Undertake sanctions screening for all new business relationships and occasional transactions, including the customer, UBO, representative and other key principals, at the time of acceptance, during periodic reviews and when there is a trigger event generating a business relationship review. The screening should be documented.
- Employ enhanced due diligence procedures and monitoring in case a customer or a transaction by its nature may pose a higher PF risk and consider implementing, among other things, the following:
    - → Performing enhanced checks or requesting further verification of the identify or ownership of customers and/or counterparties, including their beneficial ownerships, supplemented by consulting publicly available information through the media and the Internet;
    - → Reviewing open-source databases (e.g. such as company and beneficial ownership registries to gather more information on shareholders, directors and beneficial owners of customers and/or counterparties to identify any concerns related to PF; shipping and aircraft registries, chambers of commerce, third party experts publications or media to understand the context for the movement of goods and equipment and/or the supply chains involved in a particular relationship or transaction, ensuring consistency with these contexts;

- → Requesting further explanation and/or documentation on the source of funds and/or wealth for specific transactions;
- → Conducting further supply chain analysis (for instance, by requesting further clarification and/or documentation about the nature, end-use or end-user of goods, especially when the transaction involves dual-use goods or other proliferation-sensitive goods and/or services);
- → Requesting further export control information, such as copies of export control or other licenses or authorizations issued by export control authorities, and/or end-user certification to verify the nature of the goods, proper authorization, and any changes in the volume or value of goods during transport between jurisdictions;
- → Implementing enhanced monitoring of customers engaged in transactions that deviate from their usual profile or practices.

- Understand the customer's business nature and the jurisdictions with which the customer trades or where it operates.
- Determine and understand beneficial ownership of relationships and the source of funds/wealth of relationships and transactions.
- Conduct ongoing monitoring of client accounts to ensure the account remains used for the originally stated purpose and to detect any unusual activities. This includes regular review of the risk assessment taking into consideration any changes in products, customers, and geography; incorporate PF into the full range of existing internal procedures, systems, and controls; provide training to staff regarding PF risks.
- Expand staff training by incorporating, inter alia, the risk of PF, typologies, mitigation, and circumvention techniques of PF, including the obligation to freeze and report unusual transactions or matches against sanctions lists.
- Immediately freeze funds or other assets, and subsequently report any (potential) unusual transactions related to PF, objectively[22] or subjectively, to the Financial Intelligence Unit of Aruba (FIU-Aruba) and the CBA..
- Keep information and documents obtained for the purpose of (enhanced) customer due diligence up-to-date.

11. What is the Freezing and Reporting Requirement?

The relevant sanctions laws and regulations in Aruba, as outlined in section 7 above, require financial institutions and DNFBPs to promptly take measures to freeze without delay all funds or other assets in Aruba, which directly or indirectly belong to, are owned by, are in possession of or are controlled by a natural person, a legal person, entities or bodies listed in the designated UN or EU sanctions lists referred to in the national sanctions laws and regulations. The frozen funds or other assets cannot be used, transferred, converted, relocated, or made available. Access to the frozen funds or assets can only be granted with the approval of the Minister charged with financial matters. Subsequently, the supervised institutions are also required by law to report to the CBA and the FIU-Aruba of the freezing of any funds or other assets which are in their custody.

In connection with these reporting requirements, the CBA has issued a reporting form (Annex 3) and supplementary guidance on the reporting procedure regarding freezing of funds or other assets of designated

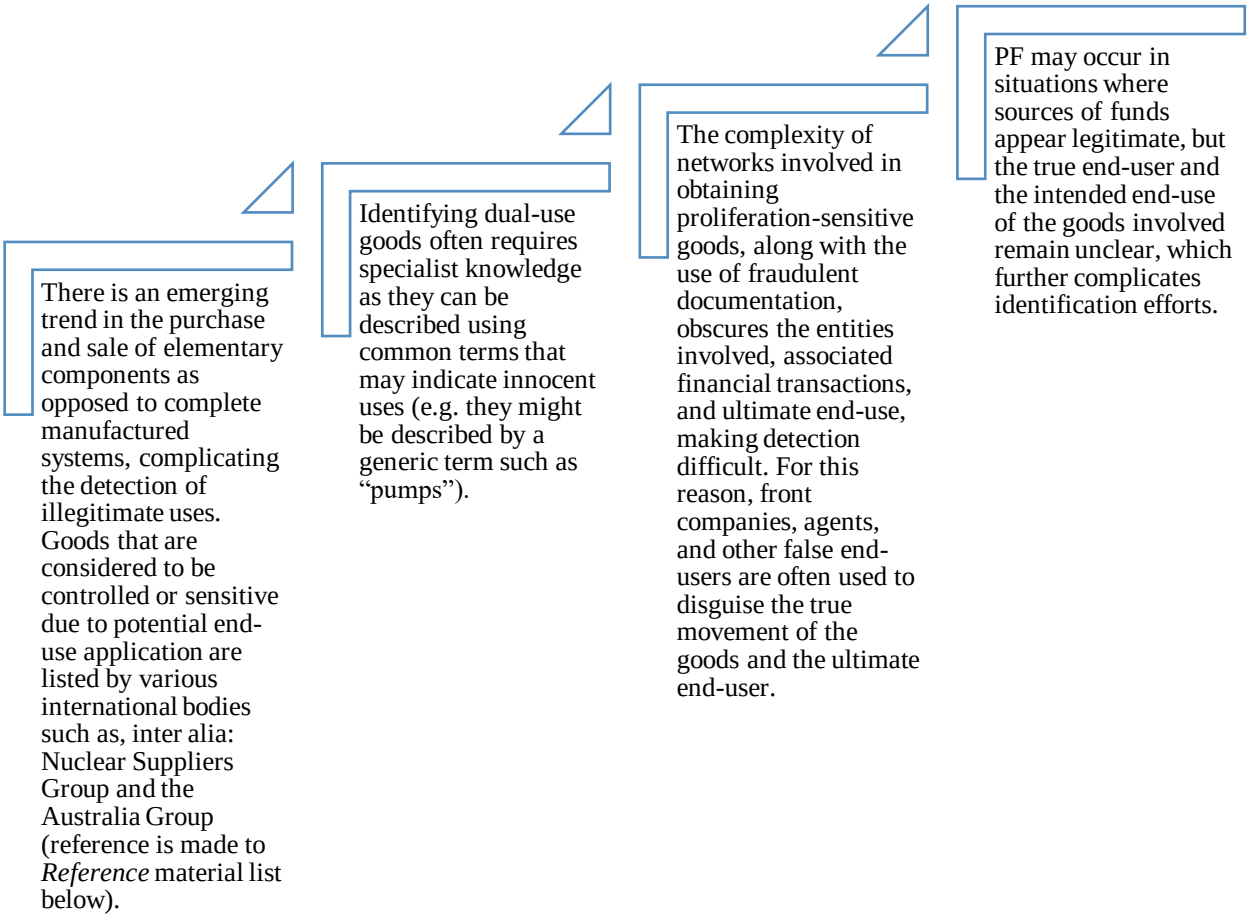
[22] Objective reporting under code 130102 in case a transaction performed by or for the benefit of a natural person, legal person, group or entity established in countries or territories which are mentioned on an accepted sanctions list pursuant to the Sanctions State Ordinance 2006.

persons or entities (Annex 4). The institutions under the supervision of the CBA are required to use this form for the reporting to the CBA notwithstanding the obligation to also report to the FIU-Aruba. The form must be accompanied with copies of identification documents, company registry extracts and any other document used to verify the identity of the reporting person or entity pursuant to the AML/CFT State Ordinance.

12. PF Cases: Examples of Trends, Tactics and Typologies

Trade finance is considered a common vehicle to financing proliferation. In this context, supervised institutions are required to apply enhanced due diligence on trade finance transactions and relationships, and special attention should also be given to insurance activities.

The identification of PF may be rather challenging for several reasons:



Annex 2 provides further examples of trends, tactics, typologies and case studies of the financing of proliferation.

ANNEX 1

Amendments to the PF Guidance Note

This PF Guidance Note was first published by the CBA in July 2021.

- → *September 2024* - This guidance note was revised to include, inter alia, additional information on PF, enhance the reader's experience, introduce new relevant trends, typologies and case studies to illustrate practical applications, as well as update reference material. These enhancements aim at supporting the efforts of financial institutions and DNFBPs in navigating the complexities of PF and staying informed about the latest developments in this area.

ANNEX 2

PF Trends, Tactics and Typologies[23]

This Annex describes several case examples of trends, tactics, and typologies related to PF.

- *Case example 1*

The Khan proliferation case involves nuclear weapon programs across several jurisdictions of proliferation concern. The proliferation process for each item to be constructed requires numerous steps to conceal the network's activities, as well as the true nature and end-use of the goods. Many individuals, companies, and countries were involved, either knowingly or unknowingly. Although some operations appear to have been settled in cash, others were completed through international transfers under established contracts. The said contracts appeared to be financed conventionally, using letters of credit or bills of exchange. Additionally, there were cash transactions within the network of customers. Funds were deposited in bank accounts of emerging or offshore countries before being transferred between banks for the final beneficiaries.

- *Case example 2*

A proliferator established front companies and used other intermediaries to purchase magnets that could be used for manufacturing centrifuge bearings. Front Company A signed documents with a manufacturing company in a foreign jurisdiction regarding the production and trade of magnets. However, it was neither declared in these documents nor detected by authorities that these components could be used to develop WMD. The magnets were then transshipped to a neighboring third jurisdiction to Front Company B. This jurisdiction serves as a "turntable" for goods, meaning that goods are imported and re-exported. The proliferator used an intermediary to arrange the import and export to the third jurisdiction. The intermediary had accounts in the third jurisdiction and used his accounts to finance the acquisition of the goods, and to launder the illegal funds used for these transactions. A combination of cash and letters of credit was used to pay for the trade of the magnets, which totaled over USD 4 million.

- *Case example 3*

Trading Company B in Country Z deals in laboratory test equipment for university and research centers, and also for the energy sector. It is known to have procured dual-use items for Country Z's WMD programs. Company B holds bank accounts in several jurisdictions, including an account with a UK bank in Country U, a known diversionary destination.

[23] Reference is made to the research trends and typologies paper provided in the "Reference" material section of this guidance paper.

Chinpo Shipping Case Study

In the late 1990s, DPRK founded Ocean Maritime Management (OMM), which provided arms shipment services that played a central role in the country's nuclear programme. Before being designated by the UNSC in 2014, OMM established a global network of front companies and facilitators to circumvent UN sanctions. This included Chinpo Shipping, a shipping company and general wholesale import/export entity, founded in 1970 by Tan Cheng Hoe, and based in Singapore.

In 2014, the UNSC added OMM to the list of Specially Designated Entities for facilitating the July 2013 shipment of conventional arms from Cuba to DPRK. The shipment was on the Chong Chon Gang vessel, where the following items were found hidden under bags of sugar: two MiG-21 aircraft and engines; six trailers of SA-2 and SA-3 surface-to-air missiles; ammunition, rifles and night-vision equipment; and a total of 240 tons of military equipment. During the trial in Singapore of Chinpo's founder, Tan Cheng Hoe, the prosecution's expert witness indicated that such military equipment could be used to protect DPRK's nuclear sites. In addition, the court confirmed that OMM had instructed Chinpo Shipping to pay the vessel's Panama Canal fees (USD 54,270 and USD 72,017 for outbound and inbound passages) on its behalf. To conceal the prior activities of Chong Chon Gang, OMM had also instructed Chinpo to falsely document the vessel name – as South Hill 2 – in wire transfer documentation.

In 2015, Singapore's District Court found Tan Cheng Hoe guilty of two offences: the violation of UN sanctions, and the provision of financial services that may reasonably be used to contribute to the DPRK's nuclear and ballistic missile programme. In the course of the trial, it was revealed that Tan Cheng Hoe had close ties with DPRK: his Chinpo office space was made available, for free, to the embassy of DPRK; he was a contact person for employment of North Korean workers in Singapore-based companies; he acted as an intermediary to resolve conflict between the North Korean and Singaporean companies; and he was a financial agent for many North Korean entities, including OMM.

The Bank of China, which provided Chinpo with banking services, failed to implement robust KYC and CDD checks. It did not identify either Chinpo's close ties with North Koreans in Singapore, or its direct ties with DPRK. This included failing to identify, for instance, that Chinpo shared its address with the North Korean embassy in Singapore. In addition, Singapore's District Court found that the bank may have failed to perform adequate transaction monitoring – which may have been a consequence of its poor KYC and CDD checks. For example, Chinpo's freight decreased from 57 to 4 vessels between 2010 and 2013. However, Chinpo's outward remittances totaled more than USD 40 million between 2009 and 2013. Such transactions are inconsistent with the profile of such a shipping agent. It is unclear whether the Bank of China's ongoing transaction monitoring generated alerts, and whether analysts investigated the transactions to establish whether they were legitimate.

Sources: James Martin Center for Nonproliferation Studies, 'Chinpo Shipping Case Study', November 2017; Colum Lynch, 'U.N. Panel: North Korea Used Chinese Bank to Evade Nuclear Sanctions', Foreign Policy, March 7, 2016.

- *Case example 4*

R. David Hughes was the president of an Olympia, Washington-based company, AMLINK. AMLINK was a medical supply company, which was involved in export of commodities that did not match its business profile. In June 1996, the U.S. Customs Service began an investigation of the exportation of nuclear power plant equipment by Mr. Hughes and AMLINK from the Port of Seattle to Cyprus. The nuclear power plant equipment was to be shipped from Cyprus to Iran via Bulgaria, in violation of the U.S. embargo on Iran. Payment was made via wire transfer from Abi-Saad into Mr. Hughes U.S. bank account; Mr. Hughes then paid for the equipment with a cashier's check. The declared value of the shipment was undervalued. Hughes was indicted and convicted of export of nuclear equipment without a license.

- *Case example 5*

A foreign national set up a trading company in another Middle East State and opened a series of accounts on behalf of the company at an international bank in that country. These accounts were denominated in local currency, euros, and other foreign currencies. Monitoring by the bank showed that the trading company's account received funds in local currency from only one source (a second company set up by another foreigner). These local currency funds were then quickly switched into foreign currencies and transferred overseas. This activity triggered investigations by the bank, which indicated that the owners of the companies involved had links to Iran. The bank suspected the funds were originating from Iran and being channeled through the trading company into the global financial system.

- *Case example 6*

A foreign national set up a trading company in another Middle East State and opened an account on behalf of the company at an international bank in that country. Monitoring by the bank showed a high turnover of funds and subsequently ML was suspected. Investigations by the bank demonstrated that the foreign national's stated employment was as a member of staff in the second company, which had the same telephone number as the trading company. Further investigation revealed that this telephone number was the same as that belonging to two other companies previously identified by the bank as having Iranian shareholders and involved in Iranian business. The bank therefore suspected that the trading company was being used as a front for Iranian business.

- *Case example 7*

The case of Shahab Ghasri: Mr. Ghasri, who based in Sweden, used his company Petroinstrument HB to procure sensitive goods from European suppliers for the benefit of Iran. Mr. Ghasri received payments from Iran via a money exchange company in Sweden and a wire transfer to a Swedish bank. Swedish authorities initially noticed Petroinstrument HB as a result of the suspicious activity reports filed by banks in late 2010 and early 2011. In 2011, Mr. Ghasri arranged to ship corrosion-resistant valves to a customer in Iran. Mr. Ghasri indicated Sharjah, United Arab Emirates, as the end-use destination for the valves, only to change the air waybill to Iran at the last minute. Swedish authorities intercepted the shipment and searched his home and office where they found documents related to previous transactions. In 2013, a Swedish court found Mr. Ghasri guilty and gave him a three-month suspended jail sentence.

Karl Lee: A Chinese national supplying Iran with sensitive goods

One of the most notorious and long-term cases of Iran-related proliferation financing involves a Chinese national known as Karl Lee. Mr. Lee operated and likely continues to operate in Dalian, China, despite having been sanctioned internationally. Mr. Lee began supplying Iran with sensitive goods in defiance of UN sanctions beginning at least in 2004 with the help of shell and front companies. Mr. Lee both procured goods from different manufacturers on behalf of Iran and sold goods manufactured at the facilities he was associated with.

The main company initially associated with Lee was LIMMT Economic and Trade, established in 1998. In 2006, the U.S. government added LIMMT to its Specially Designated Nationals List (SDN) list; in 2009, it added Karl Lee himself. Since LIMMT was sanctioned, no U.S. financial institution was allowed to provide financial services to the company. But since most of its financial transactions were processed in U.S. dollars and involved the U.S. financial system, Mr. Lee needed to find ways to deceive the system. Mr. Lee directly instructed his customers to use alias names and new account numbers for LIMMT to avoid having transactions blocked. Unsuspecting non-Iranian importers of Mr. Lee's products also received similar instructions to use various alias names instead of LIMMT and ever-changing account numbers. In 2008, the U.S. government indicted LIMMT on 118 counts, including the provision of false business information to financial institutions.

Mr. Lee established a new set of front companies in response to U.S. sanctions and the Chinese government's clampdown on setting up companies in his own name. He then used the names of his family members and close associates to open multiple accounts to transfer funds.. Many of these companies used LIMMT's address or a close variant. Between 2006 and 2014, Mr. Lee carried out more than 165 separate transactions worth USD 8.5 million in violation of U.S. sanctions. It is worth mentioning that proliferation-related transactions often involve modest amounts and might not trigger the attention of financial institutions, but over time they can add up to substantial amounts that benefit proliferation. According to press reports, between 2009 and 2013, Mr. Lee earned $10 million. Undeterred, Mr. Lee continued setting up new companies that he used for his illicit activities. As with the previous networks, Mr. Lee tried to evade sanctions by using the companies' names, owners' names, and addresses, which were often the same.

Sources:Dr. Togzhan Kassenova and Dr. Bryan R. Early, 'Countering the Challenges of Proliferation Financing', July 2023

ANNEX 3

CBA Reporting Form Sanctions Regulations

Lastly updated in September 2024

This reporting form is applicable to all financial service providers (banks, credit unions, finance companies, pension funds, insurance companies, insurance brokers, money transfer companies, money exchange offices, and pawn shops) and designated non-financial businesses and professions (accountants, casinos, car and vessels dealers, lawyers, jewelers, civil-law notaries, real estate companies, tax advisors, trust service providers and virtual asset service providers) for the reporting to the Centrale Bank van Aruba in accordance with the sanctions regulations.

REPORTING ENTITY			
1.	Name		
2.	Address		
3.	Place of business		
4.	Contact person		
5.	Reporting requirement	☐ article 4 of the Sanction Decree Combat Terrorism and Financing Terrorism ☐ article 8 of the Sanction Decree Combat Terrorism and Financing Terrorism ☐ article 12 of the Sanction Decree Combat Terrorism and Financing Terrorism ☐ article 5, paragraph 2, of the Interim State Decree on Priority Sanctions Regimes ☐ article 3, paragraph 2, of the Sanctions State Decree Libya ☐ article 4, paragraph 2, of the Sanctions State Decree Ukraine ☐ article 5, paragraph 2, of the Sanctions State Decree Sudan ☐ article 5, paragraph 2, of the Sanctions State Decree South Sudan ☐ article 5, paragraph 2, of the Sanctions State Decree Syria ☐ article 5, paragraph 2, of the Sanctions State Decree Central African Republic ☐ article 5, paragraph 2, of the Sanctions State Decree Yemen ☐ article 5, paragraph 2, of the Sanctions State Decree on North Korea ☐ article 5, paragraph 2, of the Sanctions State Decree Cyber-Attacks ☐ article 5, paragraph 2, of the Sanctions State Decree Human Rights Violations ☐ article 5, paragraph 2, of the Sanctions State Decree Chemical Weapons	
6.	Relevant UN/EU freezing list(s)		
REPORTABLE PERSON OR ENTITY		**DATA INCLUDED IN SANCTIONS REGULATION OR FREEZING LIST**	**DATA IN ADMINISTRATION OF REPORTING ENTITY**
7.	Name		
8.	Alias		
9.	Address		
10.	Home address or place of business		
11.	Place of birth (if applicable)		
12.	Date of birth (if applicable)		
13.	Description of the service rendered or requested, including (a) the identity of the person or entity who requested the service or on behalf of whom the service was requested; and (b) the identity of the person or entity for or to the benefit of whom the service was requested		
14.	Actions undertaken by reporting entity	☐ Funds or other assets are frozen. ☐ Other, namely _____.	
15.	*Amount* and *origin* of the funds or other assets that are frozen		
Signature: Date: Name: Position:			

This form must be accompanied with copies of identification documents, company registry extracts and any other documents used to verify the identity of the reportable person or entity pursuant to the State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (AB 2011 no.28). The completed and signed reporting form must be submitted to the Integrity Supervision Department of the Centrale Bank van Aruba via e-mail: **integritysupervision@cbaruba.org**. For completeness sake, a report must also be filed immediately to the Financial Intelligence Unit of Aruba (FIU-Aruba) in case of a positive match.

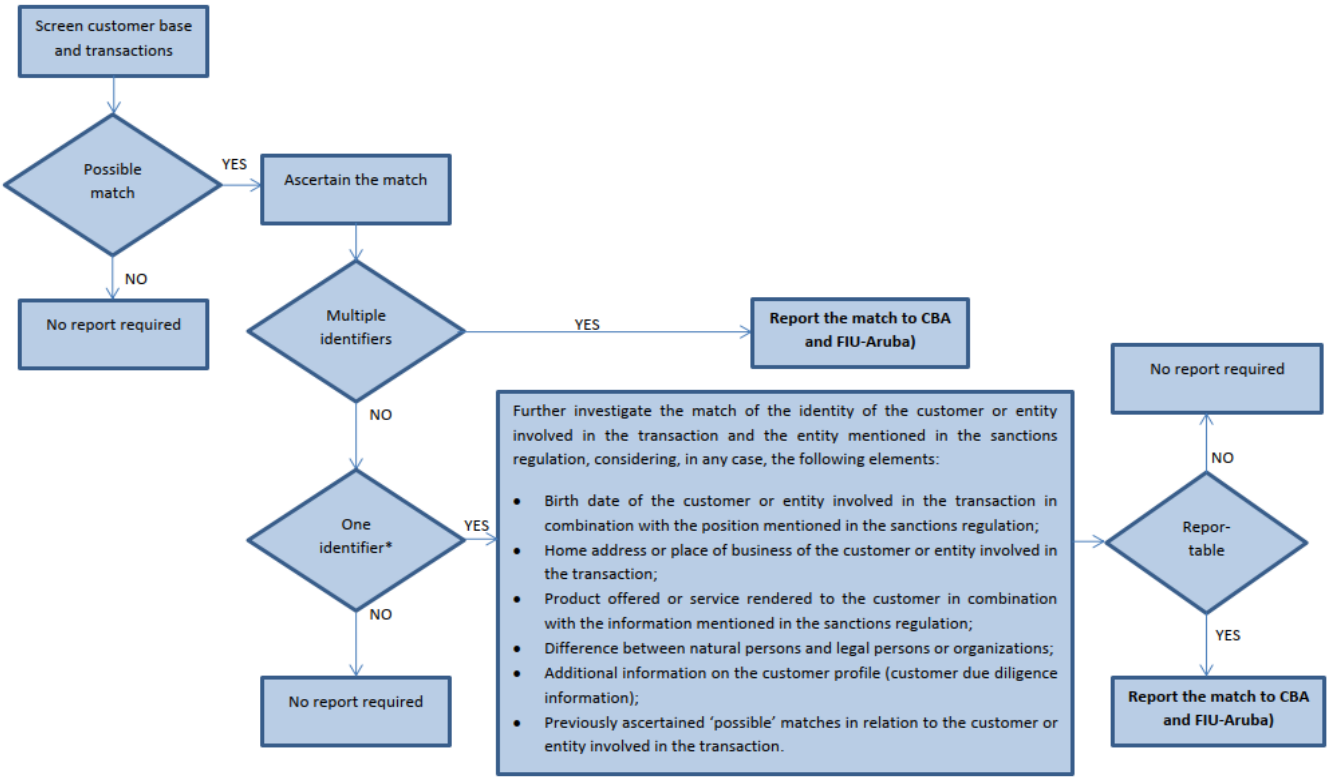
ANNEX 4

Reporting Procedure Sanctions Regulations

Centrale Bank van Aruba

The Reporting Procedure Sanctions Regulations is **applicable to** all financial service providers (banks, credit unions, finance companies, pension funds, insurance companies, insurance brokers, money transaction companies, money exchange offices, and pawn shops) and designated non-financial businesses and professions (DNFBPs) (accountants, casinos, car and vessels dealers, lawyers, jewelers, (junior) civil-law notaries, real estate companies, tax advisors, trust service providers and virtual asset service providers). In case of a positive match with any of the names of the natural/legal persons, bodies or entities designated on the UN/EU sanctions lists, the service provider is required to immediately inform the CBA of such, including any blocked funds/assets in its custody via the reporting form designed for this purpose. The transactions intended or carried out by or on behalf of designated natural/legal persons, bodies or entities must also be immediately reported to the Financial Intelligence Unit-Aruba (FIU-Aruba).

This reporting procedure concerns the following Sanctions State Decrees, which are currently in force: Sanctions Decree Combat Terrorism and Terrorist Financing (AB 2010 no.27), the Interim State Decree on Priority Sanctions Regimes (AB 2019 no. 47), Sanctions State Decree Libya (AB 2011 no.25), Sanctions State Decree Ukraine (AB 2014 no.26), Sanctions State Decree Sudan (AB 2014 no. 46), Sanctions State Decree South Sudan (AB 2015 no. 47), Sanctions State Decree Syria (AB 2016 no. 2), Sanctions State Decree on Central African Republic (AB 2016 no. 55), Sanctions State Decree on Yemen (AB 2017 no. 10), Sanctions State Decree on North Korea (AB 2017 no.42), Sanctions State Decree Cyber-Attacks (AB 2020 no. 125), Sanctions State Decree Human Rights Violations (AB 2021 no.30), Sanctions State Decree Chemical Weapons (AB 2021 no. 31). All financial institutions and DNFBPs are required to have updated lists of the sanctions decrees in time.



*such as name, alias, home address or place of business.

REFERENCES

FATF DOCUMENTS

- FATF Best Practices Paper: Sharing Among Domestic Competent Authorities Information Related to the Financing of Proliferation, February 2012.
- FATF Guidance on Countering Proliferation Financing: The implementation of financial provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction February 2018.
- FATF Guidance, The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, June 2013.
- FATF Report, Combating Proliferation Financing: A Status Report on Policy Development and Consultation, February 2010.
- FATF, Typologies Report on Proliferation Financing, June 18, 2008.
- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations – last amended November 2023.[24]
- FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures, June 2007.
- FATF Guidance on Proliferation Financing Risk Assessment and Mitigation, June 2021.

UNITED NATIONS DOCUMENTS

- United National Security Council Resolution 1540 adopted by the Security Council at its 4946th Meeting on April 28, 2004.
- United National Security Council Resolution 1718 adopted by the Security Council at its 5551st Meeting on October 14, 2006.
- United National Security Council Resolution 2231 adopted by the Security Council at its 7488th Meeting on July 20, 2015.[25]

NATIONAL LAWS AND REGULATIONS

- State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (AB 2011 no. 28).
- Handbook for the Prevention and Detection of Money Laundering and Financing of Terrorism for Service Providers (financial and designated non-financial), the Centrale Bank van Aruba, Version 1.1, January 1, 2020.
- Sanctions State Decree North Korea (AB 2017 no.42).
- Sanctions State Decree Iran (AB 2021 no. 141).
- State Decree repealing Sanctions State Decree Iran (AB 2024 no. 9).
- The Interim State Decree Priority Sanctions Regimes (AB 2019 no.47) and its subsequent amendments in 2022 (AB 2022 no. 39), 2023 (AB 2023 no. 63) and 2024 (AB 2024 no. 17 & AB 2024 no. 19).

[24] Note that the FATF Recommendations are subject to frequent periodical updates.
[25] The targeted financial sanctions on 23 individuals and 61 entities on the list established pursuant to UNSCR 2231 on Iran ceased to apply after 18 October 2023. The UNSCR 2231 List has since been removed from the UNSC website and corresponding changes were made to the UNSC Consolidated List.

SANCTIONS LISTS

- UN Sanctions List.
- EU Sanctions Map.
- US Treasury Office of Foreign Assets Controls (OFAC) list.
- Domestic sanctions list.[26]

PF TYPOLOGIES AND CASE STUDIES

- United Nations Panel of Experts Reports related to North Korea.
- Jonathan Brewer, Final Report on the Study of Typologies of Financing of WMD Proliferation, King's College, London, October 13, 2017.
- FATF, Proliferation Financing Report, June 2008
- Project Alpha – Centre for Science and Security Studies at King's College London (comprehensive database of open-source PF case studies).
- James Martin Center for Nonproliferation Studies (non-proliferation research).

MULTILATERAL EXPORT CONTROL REGIMES (LISTS OF DUAL-USE GOODS)

- FATF, Proliferation Financing Report, June 2008.
- Nuclear Suppliers Group Control Lists.
- Australia Group Common Control Lists.
- Missile Technology Control Regime Guidelines and the Equipment, Software and Technology Annex.
- Wassenaar Arrangement Control Lists.
- Zangger Committee Trigger List.
- EU dual-use control regime pursuant to Regulation (EU) 2021/821 of the European Parliament and of the Council of May 20, 2021 (see Annex IV of the Regulation).

INDEPENDENT BODIES DOCUMENTS

- Anagha Joshi, Emil Dall, and Darya Dolzikova, Guide to Conducting a National Proliferation Financing Risk Assessment, RUSI Occasional Papers, May 13, 2019.
- Anagha Joshi, RUSI Supplementary Material for Guidance Paper, Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction, Second Edition, July 2018.
- Anagha Joshi, Supplementary Material for Guidance Paper: Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction, RUSI, Second Edition, July 2018.
- Berger, Joshi, Countering Proliferation Finance: Implementation Guide and Model Law for Governments, RUSI Guidance Paper, July 2017.
- Dr Jonathan Brewer, The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation, CNAS, January 2018.
- Emil Dall and Tom Keatinge, RUSI Occasional Paper, Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry, July 2018.
- Emil Dall, Tom Keatinge, and Andrea Berger, Countering Proliferation Finance: An Introductory Guide for Financial Institutions, RUSI Guidance Paper, April 2017.

[26] The domestic list of Aruba, which has been established by Ministerial Decision dated November 20, 2013, consists of individuals, legal persons and other entities to which Council Regulation (EU) No. 2580/2001 of the EU applies.

- Jonathan Brewer, Study of Typologies of Financing of WMD Proliferation , October 13, 2017.
- Jonathan Brewer, The Financing of WMD Proliferation: Conducting Risk Assessments, CNAS, November 2018.
- Togzhan Kassenova, Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help, World ECR: The Journal of Export Controls and Sanctions, May 30, 2018.
- Noémi També, RUSI Paper, Institutional Proliferation Finance Risk Assessment Guide, June 2023.
- Emil Dall and Tom Keatinge, RUSI Occasional Paper, Assessing the Global Response to Proliferation Financing: An Analysis of FATF Mutual Evaluation Data, November 2021.
- Dr. Togzhan Kassenova and Dr. Bryan R. Early, Countering the Challenges of Proliferation Financing, July 2023.