FATF

GUIDANCE ON PROLIFERATION FINANCING RISK ASSESSMENT AND MITIGATION

JUNE 2021

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2021), *Guidance on Proliferation Financing Risk Assessment and Mitigation,* FATF, Paris, France, https://www.fatf-gafi.org/publications/financingofproliferation/documents/proliferation-financing-risk-assessment-mitigation.html

Table of contents

Acronyms

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CDD	Customer Due Diligence
CPF	Counter Proliferation Financing
DNFBP	Designated Non-financial Business and Profession
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
INR.	Interpretive Note to Recommendation
ML/TF	Money Laundering/Terrorist Financing
MVTS	Money or Value Transfer Service
NRA	National Risk Assessment
OPs	Operative Paragraphs
PF	Proliferation Financing
PoE	Panel of Experts
SRB	Self-Regulatory Body
TCSP	Trust and Company Service Provider
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
VASP	Virtual Asset Service Provider
WMD	Weapons of Mass Destruction

Background and context

1. In October 2020, the FATF revised Recommendation 1 and its Interpretive Note (R.1 and INR.1) to require countries[1] and private sector entities[2] to identify, assess, understand and mitigate their proliferation financing risks (PF risk). In the context of R.1 and of this Guidance, proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions (TFS) obligations referred to in Recommendation 7.[3]

2. In addition to obligations for countries, the revised FATF Standards require private sector entities to have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks. Private sector entities may do so within the framework of their existing targeted financial sanctions and/or compliance programmes, and are not expected to establish duplicative processes for proliferation financing risk assessment or mitigation.

3. This Guidance seeks to develop a common understanding about the impact of the amendments to R.1 and INR.1, in particular, on how countries and private sector entities could implement the new requirements to assess and mitigate proliferation financing risks given the rule-based nature of the targeted financial sanctions under Recommendation 7.

4. The source of proliferation financing risks would depend upon a number of factors as follows:

    a. **Risk of a potential breach or non-implementation of targeted financial sanctions:** This risk may materialise when designated entities and individuals[4] access financial services, and/or funds or other assets, as a result, for example, of delay in communication of designations at the national level, lack of clear obligations on private sector entities, failure on the part of private sector entities to adopt adequate policies and procedures to address their proliferation financing risks (e.g. weak customer onboarding procedures and ongoing monitoring processes, lack of staff training, ineffective risk management procedures, lack of a proper sanctions screening system or irregular or inflexible screening procedures, and a general lack of compliance culture);

---

1 All references to country or countries apply equally to territories or jurisdictions or member states as referred in UNSCRs.

2 All references to "private sector entities", "private sector(s)" or "private sector firms" refer to financial institutions, designated non-financial businesses and professions (DNFBPs), and virtual asset service providers (VASPs). References to "financial institutions and/or DNBFPs" are also relevant to VASPs.

3 Paragraphs 1 and 2 of the Interpretive Note to Recommendation 7, and the related footnotes, set out the scope of Recommendation 7 obligations; including that, it is limited to the implementation of targeted financial sanctions and does not cover other requirements of the UNSCRs (including UNSCR 1540 (2004)). The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15 only. The requirements under Recommendation 1 for PF risk assessment and mitigation, therefore, do not expand the scope of other requirements under other Recommendations.

4 All references to "individuals" apply equally to "persons" as referred in UNSCRs. In the DPRK UNSCRs, obligations also refer to those "persons" or "individuals" acting on these designated persons/individuals' behalf.

b. **Risk of evasion of targeted financial sanctions:** This risk may materialise due to concerted efforts of designated persons and entities to circumvent targeted financial sanctions (e.g. by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries).

Objectives and scope

5. This non-binding Guidance draws on the experiences of countries and of the private sector, and may assist competent authorities and private sector entities to effectively implement the new obligations. The purpose of this Guidance is:

   a. to provide guidance to assist public and private sectors in implementing the new requirements to identify, assess and understand their proliferation financing risk as defined in R.1;

   b. to provide guidance to assist public and private sectors in implementing the requirement to mitigate the proliferation financing risks, which they identify; and

   c. to provide additional guidance to supervisors/self-regulatory bodies (SRBs) on supervision or monitoring of proliferation financing risk assessment and mitigation.

6. Recommendation 1 requires countries and private sector entities to identify, assess, and understand "*proliferation financing risks*". 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 obligations referred to in Recommendation 7. These R.7 obligations apply to two country-specific regimes for the Democratic People's Republic of Korea (DPRK) and Iran, 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 (a) any person or entity designated by the United Nations (UN), (b) persons and entities acting on their behalf or at their direction, (c) those owned or controlled by them. The full text of Recommendations 1 and 7 is set out at Annex A.

7. This Guidance is intended to assist countries and private sector entities in implementing these specific obligations under R.1. Nevertheless, it also notes, where relevant, information which is not required under R.1 but relates to broader issues of counter proliferation (e.g. where it is not clear whether or not there is a link to DPRK or Iran designated entities), or activity-based prohibitions or other measures (which apply to DPRK and Iran and impose mandatory obligations for UN Member States, but are not included in R.7), are out of the scope of the FATF Recommendations. This information – indicated in footnotes – is not required under R.1, and is not assessed in the FATF mutual evaluation or assessment process, but awareness of it could be helpful for countries and private sector entities to implement relevant FATF obligations, and to avoid conflict or duplication with obligations imposed by UNSCRs or national laws, but not included under the FATF Standards. The amendments to R.1 and INR.1 also do not change or extend the existing obligations on private sector entities with respect to Recommendation 7 and to combating money laundering and terrorist financing (ML/TF) set out in Recommendations 9 to 23.

8. This Guidance is non-binding and does not restrict the freedom of national authorities and private sector entities in the conduct of their proliferation financing risk assessments and to take action as appropriate to address the risks identified. The Guidance recognises that there is no one-size-fits-all approach when assessing or mitigating proliferation financing risks. Countries and private sector entities should implement measures, having regard to the context, risk profile and materiality of different sectors and institutions within a sector. This approach would ensure the implementation of obligations in a manner that is proportionate to the risks faced by relevant entities, and be consistent with other complementary objectives such as financial inclusion.

9. The FATF Standards provide flexibility to countries to exempt a particular type of financial institution, DNFBP or VASP from the requirements to identify, assess, monitor, manage and mitigate proliferation financing risks, provided there is a proven low risk of proliferation financing relating to such private sector entities. Countries should consider using this flexibility in a timely and responsive manner to take into account financial exclusion concerns. As risk profiles can change over time, countries should monitor such exemptions. Nevertheless, full application of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

10. This Guidance does not supersede or replace the *2018 FATF Guidance on Counter Proliferation Financing*. The contents of the *2018 Guidance* remain relevant, save for the new obligations relating to proliferation financing risk assessment and mitigation introduced in R.1 and INR.1 for countries and private sector entities.

11. This Guidance also acknowledges that some countries and private sector entities may choose to assess their exposure to proliferation financing risks in a wider context, i.e. not limited to the potential breach, non-implementation or evasion of targeted financial sanctions. While it is outside the scope of FATF requirements and thus not going to be covered under the FATF assessment process, countries and private sector entities may continue to conduct such wider risk assessments, and take action to mitigate the identified risks, in accordance with their frameworks and policies.

Target audience, status, and contents

12. The Guidance is aimed at the following audience:

    a. Countries and their competent authorities, including supervisors;

    b. Financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs); and

    c. Virtual Asset Service Providers (VASPs) if they are not classified as financial institutions or DNFBPs.

13. The Guidance is focused on new obligations under R.1 and INR.1 on proliferation financing risk assessment and mitigation introduced in October 2020. It consists of the following three sections:

    a. Section 1: Assessment of proliferation financing risks;

    b. Section 2: Mitigation of proliferation financing risks; and

c. Section 3: Supervision of proliferation financing risk assessment and mitigation.

14. The FATF adopted the present Guidance in June 2021.

SECTION ONE: ASSESSMENT OF PROLIFERATION FINANCING RISKS

Introduction

15. Identifying, assessing, and understanding proliferation financing risks on a regular basis is essential in strengthening a country's or private sector's ability to prevent designated persons and entities[5] involved in Weapons of Mass Destruction (WMD) proliferation from raising, storing, moving, and using funds, and thus other financial assets. The implementation of TFS related to proliferation and its financing is essential for a stronger Counter Proliferation Financing (CPF) regime.

16. The FATF Standards, under Recommendation 1, require countries to designate an authority or mechanism to co-ordinate actions to assess risks, and apply resources to ensure the risks are mitigated effectively, as part of the ML and TF risk assessments. In October 2020, the FATF updated its Standards (R.1) to require countries and private sector entities to identify, assess, and understand the proliferation financing risks for the country and respective private sector, and to take action to mitigate these risks. This section provides guidance and highlights salient issues distinctive to a proliferation financing risk assessment for both public and private sectors.[6]

17. The FATF Standards provide flexibility in how jurisdictions and private sector entities assess their risks, and do not prescribe a risk assessment methodology. There should not be a one-size-fits-all approach in assessing risks of breach, non-implementation or evasion of PF-TFS as per the definition in Recommendation 1.

---

5 As included in the operative paragraphs (OPs) of relevant UNSCRs, it is the obligation of member states to impose targeted financial sanctions on designated persons and entities, as well as persons and entities acting on their behalf, at their direction, or owned or controlled by them. This guidance document uses "designated persons and entities" as a shorthand.

6 This section builds on the FATF's previous work on risk assessments and counter proliferation financing: *2018 FATF Guidance on Counter Proliferation Financing*, *2013 FATF Guidance on National Money Laundering (ML),Terrorist Financing (TF) Risk Assessment*, *2019 FATF Guidance on Terrorist Financing Risk Assessment*, *2008 FATF Proliferation Financing Report*, and *2010 FATF Combating Proliferation Financing: A Status Report on Policy Development and Consultation*; as well as reports from United Nations Security Council (UNSC) Panel of Experts (PoE) and other UN counter-proliferation bodies. See bibliography.

An effective approach for one jurisdiction or one private sector firm will not necessarily be effective for others.

18. The scope of this Guidance covers the risk assessment of the potential breach, non-implementation or evasion of TFS referred to in Recommendation 7. These assessments may be conducted as part of broader National Risk Assessments (NRAs), or more specific stand-alone assessments. However, the FATF Standards do not require a risk assessment of broader PF risks.[7] It should also be noted that a risk assessment to understand the potential risk of breach, non-implementation or evasion of PF-TFS, which is a process to be determined by the relevant country and private sector firms, may not necessarily require an entirely distinct or new methodological process, compared to how they have undertaken ML or TF risk assessments. It needs not require a stand-alone risk assessment if pre-existing risk assessment methodologies are adequate to incorporate PF risks.

Key Concepts relevant to Assessing and Understanding Proliferation Financing Risks

19. Similar to an ML/TF risk assessment, countries and private sector should have a common understanding of key concepts before conducting a proliferation financing risk assessment. This section sets out some key concepts relevant to assessing proliferation financing risks as set out in Recommendation 1, drawing from the definitions provided in the *2013 FATF Guidance on National ML and TF Risk Assessments* (hereafter "NRA Guidance") and the *2019* FATF *Guidance on Terrorist Financing Risk Assessment* (hereafter "TFRA Guidance"), as well as the *2018 FATF Guidance on Counter Proliferation Financing*.

Risk

20. A **proliferation financing risk**, similar to an ML/TF risk, can be seen as **a function of three factors: threat, vulnerability, and consequence**. In the context of Recommendation 1 and this *Guidance*, it refers to the obligations to identify, assess, and understand the risks of potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

21. Another concept relevant for any risk assessment process is the understanding of **inherent risk** and **residual risk**, and applying those concepts specifically to PF

---

[7] The broader PF risks, which are not covered in the updated Recommendation 1, refer to the risk of WMD proliferation and the risk of financing of proliferation. **WMD proliferation** refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual use goods used for non-legitimate purposes). **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 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. An **understanding of the risk of WMD proliferation and its underlying financing**, **which is not required under the FATF Standards,** may have a positive contribution to the **understanding of the risk of the breach, non-implementation or evasion of PF-TFS (i.e. the narrow definition of PF risks covered in the FATF Standards)**, and assist the implementation of risk-based measures and targeted financial sanctions.

risks, in a similar way that countries and private sector firms have already done so for ML and TF risks.

a. **Inherent risk** refers to the natural level of risk, prior to introducing any measures to mitigate or reduce the likelihood of an actor exploiting that risk – those measures are often referred to as controls or control measures. Understanding inherent risk, though not required and specified in the Standards, is important and beneficial as it can facilitate the corresponding understanding and assessment of whether the control measures are effective, and in the case where no control measures are to be introduced, the impact of such risk to the country or to the private sector firm. For a country, inherent risk may refer to various factors, for example close links with designated persons and entities under the DPRK and Iran PF-TFS regimes, or level of production of dual use goods or goods subject to export controls in the country, and trade patterns of such products, as well as loopholes in regulations aimed at the implementation of the relevant United Nations Security Council Resolutions (UNSCRs). For a private sector firm, it may refer to the nature, types, and complexity of services provided by the private sector firm, or its customer types, geographical distribution of its customers and/or beneficial owners, and channels of distribution.

b. As for **residual risk**, it refers to the level of risk, which remain after the risk mitigation process. An understanding of residual risk allows countries and private sector firms to determine if they are effectively managing proliferation financing risk within their jurisdiction or business operations. A high degree of residual risk may suggest that control measures are inadequate and that a country or a private sector firm should take remedial action to address that risk. An example of residual risk is that the financial institutions, DNFBPs or VASPs cannot identify the sanctioned individuals/entities even after introducing enhanced screening measures.

Threat, Vulnerability, and Consequence

22. The *2013 FATF NRA Guidance* and the *2019 FATF TFRA Guidance* set out other concepts, namely threat, vulnerability, and consequence relevant to a risk assessment. Below are elements specific to a PF risk assessment:

a. **Threat** refers to designated persons and entities that have previously caused or with the potential to evade, breach or exploit a failure to implement PF-TFS in the past, present or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities.[8] It can be an actual or a potential threat. Not all threats present the same risk level to all countries and private sector firms.

b. **Vulnerability** refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion

[8] DPRK PF-TFS, i.e. UNSCR 1718 (2006) OP8(d), covers persons or entities acting on behalf or at the direction of designated persons and entities.

of PF-TFS. For a country, these vulnerabilities may include weaknesses in the laws or regulations that comprise a country's national counter proliferation financing regime, or contextual features of a country that may provide opportunities for designated persons and entities to raise or move funds or other assets. For example, a jurisdiction with weak AML/CFT controls or that does not collect information about the beneficial owners of entities incorporated under its laws, or a jurisdiction with a high level of crime, smuggling, fraud or other illicit activities. For private sector firms, vulnerabilities may include features of a particular sector, a financial product or type of service that make them attractive for a person or entity engaged in the breach, non-implementation or evasion of PF-TFS.

c. **Consequence** refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for proliferation financing. A breach, non-implementation or evasion of PF-TFS may also cause reputational damages to the country, relevant sector(s) or private sector firms, and punitive measures such as sanction designations by the UN and/or national authorities. Ultimately, the consequence of proliferation financing, i.e. the threat of use or the use of a weapon of mass destruction, is more severe than that of ML or other financial crimes, and is more similar to the potential loss of life associated with the consequences of TF. It is likely to differ between countries, channels or sources.

Stages of PF Risk Assessment

23. A **proliferation financing risk assessment** is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse, and understand PF risks, with a view to developing appropriate measures to mitigate or reduce an assessed level of risk to a lower or acceptable level. Similar to process of an ML/TF risk assessment, it should make informed judgments about threats, vulnerabilities, and consequences, based on thorough review of information available to governments and the private sector. For a national PF risk assessment, it should be comprehensive enough to inform national counter proliferation financing strategies, and to assist in the effective implementation of risk-based measures supporting PF-TFS. It should also help countries and private sector firms to determine and prioritise the amount of resources necessary to mitigate the different risks. The ultimate goal of conducing a proliferation financing risk assessment is to ensure full implementation of PF-TFS requirements under relevant UNSCRs, effectively preventing the breach, non-implementation or evasion of PF-TFS under the FATF Standards. In terms of scope, a PF risk assessment may likely to be more targeted than an ML/TF risk assessment (e.g. because the scope of the risk to be assessed is more narrow than that of ML/TF), depending on the context of different countries and private sector firms.

24. The FATF Standards provide flexibility in how countries and private sector assess their PF risks and do not prescribe a particular risk assessment methodology. As the

risk assessment process involves a number of agencies and stakeholders, and often stretches over a period of time, it would generally be beneficial to organise the process into different stages and follow a structured approach. A PF risk assessment may follow the same six key stages as an ML/TF risk assessment. They are: (1) preliminary scoping; (2) planning and organisation; (3) identification of threats and vulnerabilities; (4) analysis; (5) evaluation and follow-up; and (6) update, which are elaborated in both the *2013 FATF NRA Guidance* and 2*019 FATF TFRA Guidance* in great detail. This section will focus on salient issues distinctive to the PF risk assessment process.[9]

Preliminary Scoping

25. Prior to the amendments of the FATF Standards in October 2020, only a limited number of countries and private sector firms have completed a national or private sector PF risk assessment.[10] As with an ML/TF risk assessment, countries, and private sector firms are strongly encouraged to conduct a scoping exercise first to determine the **objectives, scope, and focus of the assessment** before commencement. This exercise may consider issues such as potential methodologies and their applicability in the national or private sector context. At this stage, both public[11] and private sectors may take into account their domestic circumstances, including the unique national threat profile and vulnerabilities, national counter proliferation context and wider counter proliferation and counter proliferation financing activities and strategies, as well as sector, company, and customer profiles.

26. Given the limited literature on typologies of the breach, non-implementation or evasion of PF-TFS, conducting a **contextual analysis** as part of scoping may be beneficial for both public and private sectors.[12] Governments and private sector firms may focus their analysis on reviewing various recent methods, trends, and typologies of the breach, non-implementation or evasion of PF-TFS identified in the UNSC Panels of Experts (PoE) on DPRK and Iran's reports, existing available PF risk assessments prepared by other jurisdictions, other typologies common to TFS breaching, circumvention or evasion, and where relevant recent case examples and, where relevant, illustrated examples published by tertiary institutes, and apply the information therein to the national or business context. Countries and private sector firms should also identify information and data gaps that they should attempt to address while going through the risk assessment process. A PF risk assessment may

---

9 Countries and private sector are encouraged to refer to Part 2 of the *2013 FATF NRA Guidance* and Part 1 of *the 2019 FATF TFRA Guidance* concerning stages 1 and 2 for guidance on preliminary scoping and objectives setting, and planning and organisation; and Parts 4 and 5 of the *NRA Guidance* for more generic discussion on stages 3 to 5 on identification, analysis, and outcome.

10 The following jurisdictions have publicly released a PF risk assessment as of the publication of this Guidance. They are Cayman Islands, Gibraltar, Latvia, Portugal and the United States. These PF risk assessments have not been assessed in the FATF Mutual Evaluations and assessment processes.

11 For a national risk assessment, it may include considerations and decision of whether the PF risk is to be assessed standalone, or as part of a broader NRA that includes an ML and a TF risk assessment.

12 Based on review of FATF MERs published to date.

also include a mapping of the UNSCR PF-TFS obligations[13] applicable to financial institutions, DNFBPs and VASPs and their products or services, allowing the authorities to identify relevant agency and sector stakeholders to participate in the process. In addition, it may consider the unique national and regional PF threat profile, and the importance and materiality of different sectors.

Planning and Organisation

27. A systematic and consistent process is crucial to a meaningful PF risk assessment. Prior to the commencement of a PF risk assessment, countries and private sector firms may wish to prepare a project plan and identify the relevant personnel from different agencies/departments and stakeholders.[14] Within the private sector, stakeholder firms may include, but are not limited to: banks, money or value transfer service (MVTS) institutions,[15] insurance companies, trust and company service providers and lawyers. At the firm level, a PF risk assessment may include, in addition to compliance staff, senior executive leadership, members of the board of directors, heads of relevant business lines, and representatives of customer-facing personnel (for example, relationship managers at a bank). Countries and private sector firms may also devise a mechanism for data collection and subsequent analysis and update; and for documenting the findings. This would facilitate the refinement of the methodology, and comparison of findings over time. Considering that countries and private sector firms may be preparing their first PF risk assessments, and some of the information and findings may be of sensitive nature, countries may consider developing a mechanism for sharing the methodology, analysis, and results of the risk assessment among agencies and with financial institutions, DNFBPs and VASPs where appropriate. For example, through closed-door briefings to discuss outcomes of the assessment.[16] In addition, countries may consider making available the results of their PF risk assessment in the public domain (or a sanitised version of the results) where possible,[17] as well as developing a secured platform to allow ongoing engagement, consultations, and information sharing with financial institutions, DNFBPs and VASPs, where appropriate, to the extent possible. The publication and sharing of such information

---

13 The *2018 FATF* Guidance *on Counter Proliferation Financing* provides a list of requirements of UNSCR TFS of proliferation financing. See Annex C of the *2018 Guidance* for details.

14 The *2018 FATF Guidance on Counter Proliferation Financing* provides a list of agencies or authorities commonly involved in the implementation of UNSCRs on proliferation financing. The leading agency of a national PF risk assessment should involve these agencies or authorities in the risk assessment processes in terms of data/statistics collection, and providing feedback on draft analysis. These agencies or authorities would also be helpful in engaging their respective industry stakeholders throughout the risk assessment process. See paragraph 56 for details.

15 Trading companies might, sometimes in practice, operate as MVTS institutions and rely upon their bank accounts to transmit funds on behalf of their trading partners.

16 The *2019 FATF TFRA Guidance* provides content on approaches taken to overcome information sharing challenges considering the necessary confidential nature of terrorism and TF related information. See paragraph 26 for details.

17 Risk assessments with classified components may be redacted or summarised for dissemination to financial institutions, DNFBPs and VASPs, and that further adaptation may need to be made for such assessments to be made available for broader, public consumption.

will promote the understanding of PF risks and compliance with CPF requirements. For countries conducting their first PF risk assessments, they may also consider liaising or engaging with other similar jurisdictions that have experiences in PF risks assessments, or jurisdictions that share similar PF risk exposure to leverage of their experiences, lessons-learnt, good practices to help refine their assessment methodology.

Identification

a) Threats

28. A good foundation of the identification process, for both national and private sector firm PF risk assessments, is to begin by **compiling a list of major known or suspected threats**; key sectors, products, or services that have been exploited; types and activities that designated individuals/entities engaged in; and the primary reasons why designated persons and entities are not deprived of their assets or identified. This is especially useful as the R.7 and DPRK-related UNSCR PF-TFS requirements focus not only on the designated persons and entities, but also persons and entities acting on their behalf.

29. While the **methodology** of identifying PF threats could be similar to that of ML/TF,[18] countries and private sector firms should note that the **nature of PF threats** is significantly different from ML/TF threats. Unlike ML and TF threats, PF threats can be posed by persons and entities designated pursuant to relevant UNSCRs (i.e. DPRK and Iran) and the international networks they have created to disguise their activities; and can also be indirectly related to designated persons and entities.[19] As a result, the financing needs and methods of designated persons and entities may not necessarily be the same as those of money launderers and terrorists. In the context of potential breach, non-implementation or evasion of PF-TFS, countries and private sector firms should note that the financing can be sourced from both legitimate and illegitimate activities for raising funds or for obtaining foreign exchange, and may not necessarily involve laundering of proceeds. Possible examples of exploitation of legitimate activities may include procuring or trading of dual-use goods or goods subject to export control [20] or the

---

18 The *2013 FATF NRA Guidance* explains two different approaches that can be used at the identification stage. See paragraphs 47 to 49 for details.

19 For example, the DPRK PF-TFS (e.g. UNSCR 1718 (2006)) stipulates that funds, other financial assets and economic resources that are owned or controlled, directly **or indirectly**, by designated persons and entities are covered. The FATF Standards (R.7.2(b)), applicable to both the DPRK and Iran regimes, specify that the freezing obligations should extend to, among other things, "(ii) those funds or other assets that are wholly or jointly owned or controlled, directly or **indirectly**, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or **indirectly** by designated persons or entities, as well as (iv) funds or other assets of persons and entities **acting on behalf of, or at the direction of** designated persons or entities."

20 Examples of dual-use goods or goods subject to export control can be found in the *2008 FATF Typologies Report of Proliferation Financing* (page 7), or other international bodies such as Nuclear Suppliers Group Control Lists, the Australia Group Common Control Lists, Missile Technology Control Regime Guidelines and the Equipment, Software and Technology Annex.

trade in natural resources in contravention of relevant UNSCRs.[21] As for illegitimate activities, possible examples may include smuggling of cash,[22] gold, and other high-value goods,[23] cyberattacks,[24] drugs trafficking,[25] export of arms and natural resources such as sand,[26] etc. These activities can occur across multiple jurisdictions. Frequently, designated persons and entities use front and shell companies to conduct such businesses. Doing so is a deliberate strategy to obscure the fact that economic resources, assets, and funds are being ultimately made available to designated persons or entities.

30. Countries and the private sector should note that different countries and private sector firms would have its own different risk profiles and would face different types and extent of proliferation financing threats. They are therefore encouraged to take a holistic approach when gathering threat information,[27] and to draw on available information sources relating to domestic, regional, and international proliferation financing threats.

---

21 UNSCR 1718 PoE Report provides example, amongst others, sale of high-end electrical/electronic apparatus for recording and reproducing sound and images.

22 UNSCR 1718 PoE Report.

23 UNSCR 1718 PoE Report provides example, amongst others, sale of luxury yachts.

24 UNSCR 1718 PoE Report identifies that the DPRK had been using cyberattacks to illegally force the transfer of funds from financial institutions and VASPs (exchanges), as a means to evade financial sanctions and to gain foreign currency. Such attacks have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016.

25 UNSCR 1718 PoE Report.

26 UNSCR 1718 PoE Report. For example, the March 2020 report provides examples, among other things, of how the DPRK has continued to evade UNSCRs through illicit maritime export of commodities, notably coal and sand, and that "such sales provide a revenue stream that has historically contributed to the country's nuclear and ballistic missile programmes".

27 The *2019 FATF TFRA Guidance* gives examples of information gathered by authorities when identifying TF threats, which could be adapted for PF purposes. See paragraphs 31 and 32 for details.

Why is a proliferation financing risk assessment relevant in countries with little to no known or suspected breach, non-implementation or evasion of PF-TFS?

The absence of cases involving known or suspected breaches, non-implementation or evasion of PF-TFS in a particular country does not necessarily mean that a country or a private sector firm faces low or any proliferation financing risk. Designated persons and entities have made use of diverse and constantly evolving methods to disguise their illicit activities, and the networks they control deliberately spread their operations across multiple jurisdictions. Consequently, countries and private sector firms should still consider the likelihood of funds being made available directly or indirectly to these persons or entities in their jurisdictions or through customer relationships or use of their products. To better understand this potential risk exposure, countries and private sector firms may also make use of techniques such as scenario building, or focus groups with domestic or regional operational experts, to assess their proliferation financing risks despite the lack of local case studies. Reports of the Panels of Experts (PoE) (e.g. PoEs carrying out the mandate specified in UNSCR 1718 (2006) and UNSCR 1874 (2009) and relevant resolutions) also highlight the methods which may expose a country or a firm to PF risks. Below is an example illustrated in UNSC PoE Report.

The activities of DPRK state-owned Foreign Trade Bank (FTB) highlights this risk. FTB, despite its designated status, has operated multiple cover branches in several jurisdictions and was the centrepiece of efforts to launder money through the United States (U.S.) financial system in order to acquire components for the DPRK's weapons programmes. FTB maintained correspondent bank accounts and representative offices abroad that created and staffed front companies to conduct transactions. In June 2020, U.S. authorities seized millions of dollars held in correspondent accounts in the names of front companies that were ultimately controlled by FTB. The companies involved operated in Asia, Middle East, and Europe.

Remarks: See Section 2 for guidance on risk mitigation measures in case of low risks (paragraphs 66-67). The *2019 FATF TFRA Guidance* has separately provided guidance on considerations for jurisdictions with no or very few known (or suspected) terrorism or TF cases (paragraphs 34-35).

31. **Potential information sources** may include actual or known typologies; summaries of case types, schemes, or circumstances involved in the breach, non-implementation or evasion of PF-TFS; and designated persons and entities targeted by relevant UNSCR PF-TFS. [28] The table of indicators below, built on the *2018 FATF Guidance on Counter Proliferation Financing*, sets out situations indicating possible activities of the potential breach, non-implementation or evasion of PF-TFS.

    a. For a **national PF risk assessment**, authorities are also encouraged to make use of available financial intelligence and law enforcement data. Important to the understanding of PF threats, customs documents (e.g. customs declaration) would provide additional information on how the breach, non-implementation or evasion of PF-TFS activities could occur. Another important source, where available, is domestic and foreign intelligence on (i) global, regional, and national proliferation threats; (ii) source, movement, and use of funds by designated persons and entities, as well as those acting on their behalf or at their direction, and with close connections to countries of proliferation concerns (i.e. DPRK and Iran); and (iii) intelligence on potential PF activities (including those from foreign intelligence agencies, where available). This information may not immediately reveal apparent PF-related activity, but may be relevant to building an overall picture of threats and vulnerabilities. Information gathered from the private sector is also important, as private sector firms may have information on the breach of TFS or relevant typologies.

    b. For a **PF risk assessment by a private sector firm**, firm and group-wide databases containing customer due diligence (CDD) information collected during the on boarding and ongoing due diligence (particularly the beneficial ownership of legal persons and arrangements), and, if available, transaction records involving the sale of dual-use goods or goods subject to export control would be relevant. Another possible important source could be threat analysis reports, national PF risk assessments, and supervisory circulars on cases involving the breach, non-implementation or evasion of PF-TFS. Internal controls rules designed to identify designated persons and entities and those acting on their behalf or at their direction may also be relevant for compliance with PF-TFS.

[28] Useful sources may include: The *2008 FATF Typologies Report on PF* and the *2018 FATF Guidance on CPF* as well as the reference materials quoted in these two reports, recent UNSCR 1718 PoE reports, etc. The *2019 FATF TFRA Guidance* has separately provided guidance on good approaches and considerations during the information collection process in the TF context (see Part 2).

Indicators of the potential breach, non-implementation or evasion of PF-TFS

A risk indicator demonstrates or suggests the likelihood of the occurrence of unusual or suspicious activity. The existence of a single standalone indicator in relation to a customer or transaction may not alone warrant suspicion of proliferation financing, nor will a single indicator necessarily provide a clear indication of such activity, but it could prompt further monitoring and examination, as appropriate. Similarly, the occurrence of several indicators (especially from multiple categories) could also warrant closer examination. Whether one or more of the indicators suggests proliferation finance is also dependent on the business lines, products or services that an institution offers; how it interacts with its customers; and on the institution's human and technological resources.

The indicators listed below are relevant to both the public and private sectors. With respect to the latter, the indicators are relevant to financial institutions, designated non-financial businesses and professions and virtual asset service providers, regardless of whether they are small and mid-size businesses or large conglomerates. Within the private sector, these indicators are intended to be used by personnel responsible for compliance, transaction screening and monitoring, investigative analysis, client onboarding and relationship management, and other areas that work to prevent financial crime.

Some of the risk indicators require the cross-comparison of various data elements (e.g. financial transactions, customs data, and open market prices) often held in external sources. Due to this reliance on external data, the private sector will not observe all of the indicators identified below. For some of the risk indicators, the private sector will need additional contextual information from competent authorities, e.g. via public-private partnership and engagement with law enforcement authorities or financial intelligence units. These risk indicators may vary in degree and may not always weigh equal, with some potentially highly indicator and others less so. In using these indicators, private sector entities should also take into consideration the totality of the customer profile, including information obtained from the customer during the due diligence process, trade financing methods involved in the transactions, and other relevant contextual risk factors. Some of these risk indicators do not necessarily correspond to the breach, non-implementation, or evasion of PF-TFS, and are therefore not mandatory, but could be helpful to the private sector in understanding the wider risks. This list is by no means exhaustive and highlights only the most up-to-date and prevalent indicators (e.g. the use of shell companies) based on recent typologies of sanctions evasion, following the publication of the *2018 FATF Guidance on Counter Proliferation Financing (Annex A)*. This list should be read in conjunction with Section 2 of this Guidance on risk mitigation.

- **Customer Profile Risk Indicators**
  - During on-boarding, a customer provides vague or incomplete information about their proposed trading activities. Customer is reluctant to provide additional information about their activities when queried;
  - During subsequent stages of due diligence, a customer, particularly a trade entity, its owners or senior managers, appear in sanctioned lists or negative news, e.g. past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes;
  - The customer is a person connected with a country of proliferation or diversion concern, e.g. through business or trade relations – this information may be obtained from the national risk assessment process or relevant national CPF authorities;
  - The customer is a person dealing with dual-use goods or goods subject to export control goods or complex equipment for which he/she lacks technical background, or which is incongruent with their stated line of activity;
  - A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding;
  - A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money-remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the activity associated with originators appear to be entities who may connected a state-sponsored proliferation programme (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls;
  - A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control.
- **Account and Transaction Activity Risk Indicators**
  - The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern (i.e. DPRK and Iran);
  - Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the

account holders have previously violated requirements under dual-use or export control regimes;

- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g. companies do not have a high level of capitalisation or displays other shell company indicators. Countries or the private sector may identify more indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity;
- Demonstrating links between representatives of companies exchanging goods, i.e. same owners or management, same physical address, IP address or telephone number, or their activities may be co-ordinated;
- Account holder conducts financial transaction in a circuitous manner;
- Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services);
- Customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals;
- Transactions are made on the basis of "ledger" arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance these accounts;
- Customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.

- **Maritime Sector Risk Indicators**

  DPRK PF-TFS, i.e. UNSCR 2270 (2016) OP 23, has designated the DPRK firm Ocean Maritime Management and vessels in Annex III of the same UNSCR as economic resources controlled or operated by OMM and therefore subject to the asset freeze imposed in OP 8(d) of UNSCR 1718 (2006). UNSCR 2270 (2016) OP 12 also affirms that "economic resources" as referred to in OP 8(d) of UNSCR 2270 (2016), includes assets of every kind, which may potentially may be used to obtain funds, goods, or services, such as vessels (including maritime vessels).

- A trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit;
- The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination;
- The destination of a shipment is different from the importer's location;
- Inconsistencies are identified across contracts, invoices, or other trade documents, e.g. contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions;
- Shipment of goods have a low declared value vis-à-vis the shipping cost;
- Shipment of goods incompatible with the technical level of the country to which it is being shipped, e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry;
- Shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet;
- 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;
- Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement of export control laws;
- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g. by a shell or front company not involved in the trade transaction.

- **Trade Finance Risk Indicators**

  DPRK PF-TFS, i.e. UNSCR 2087 (2013) OP 5(a), UNSCR 2094 (2013) OP 8, UNSCR 2270 (2016) OP 10, UNSCR 2321 (2016) OP3, UNSCR 2371 (2017) OP 18, UNSCR 2375 (2017) OP 3, specifies that individuals and entities listed in Annex I and II of the resolutions are subject to the asset freeze imposed in OP 8(d) of UNSCR 1718 (2006). These designated entities include trading companies.

  - Prior to account approval, customer requests letter of credit for trade transaction for shipment of dual-use goods or goods subject to export control;
  - Lack of full information or inconsistences are identified in trade documents and financial flows, such as names, companies, addresses, final destination, etc.;
  - Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

  Source: *2018 FATF Guidance on Counter Proliferation Financing* (Annex A) and UNSC PoE Reports

b) Vulnerabilities

32. After formulating a list of PF threats, the next step is to compile a list of major PF vulnerabilities. Countries and private sector entities are encouraged to consider adapting their methodology used for identifying ML/TF vulnerabilities for PF purposes. Similar to ML/TF, these vulnerabilities could be based on a number of factors, such as structural, sectoral, product or service, customers and transactions. The vulnerabilities identified through a comprehensive assessment is inherently linked to a country's context and identified threats, and the results will be different from country to country, as well as from sector to sector, and may not be applicable to all countries and private sector entities in the same degree.

33. **Structural vulnerabilities** refer to weaknesses in the national counter proliferation financing regime that makes the country or the private sector entity (including its business and products) attractive to designated persons and entities, or those acting on their behalf or under their control, as noted in Section 2 of this *Guidance*. Some examples, which are non-exhaustive and may require further analysis during the risk assessment process, may include countries:

   a. having weak governance, law enforcement, export controls and/or regulatory regimes, weak knowledge of PF risks across agencies, and weak AML/CFT/CPF regimes identified in FATF Statements or during FATF Mutual Evaluations;

   b. lacking a legislative CPF framework and national CPF priorities, and having an implementation issue with UNSCR PF-TFS and FATF Standards (especially R.7 and IO.11);

   c. being subject to sanctions, embargoes, or other measures imposed by the UN;

d. having significant levels of organised crime, corruption, or other criminal activities which could be exploited by designated persons and entities;

e. having loose market entry, company formation and beneficial ownership requirements and poor internal identification and verification controls on customer and beneficial ownership identities, thereby making it more difficult to identify the designated persons and entities;

f. lacking a culture of inter-agency co-operation among public authorities and a culture of compliance with private sectors.

34. As illustrated in Part C of the *2018 FATF Guidance on Counter Proliferation Financing*, another key consideration is the contextual features of a country that provide opportunities for the potential breach, non-implementation or evasion of PF-TFS. In more recent reports of the UNSC PoE carrying out the mandate specified in UNSCR 1718 (2006) and UNSCR 1874 (2009) (hereafter "the UNSCR 1718 PoE"), designated persons and entities are known to have also shifted their activities through countries in other regions, especially through an international or a regional financial, trading, shipping, or company formation services centre, as well as transit countries for smuggling. These centres provide the needed services to designated persons and entities (and those acting on their behalf or in their direction) to circumvent PF-TFS. The size, complexity and connectivity of these centres, as well as large volume of transactions passing through these centres also make it easier for designated persons and entities to hide their illicit activities.

35. For a **PF risk assessment by a private sector firm**, considerations may also include the nature, scale, diversity, and geographical footprint of the firm's business; target market(s) and customer profiles; and the volume and size of transactions handled by a private sector firm.

Why is a PF risk assessment relevant to countries or private sector firms that are far away from the DPRK and Iran?

As noted in recent typologies, designated persons and entities continue to explore new ways to evade targeted financial sanctions, regardless of the geographical proximity to proliferating states (i.e. the DPRK and Iran). For example, they may arrange circuitous financial transactions and/or shipments, passing through countries that have weak AML/CFT/CPF controls. The UNSCR 1718 PoE had identified designated persons and entities routing their transactions through countries as far away as those in Africa and Europe to disguise the fund and shipment flows. Past Iran UNSC PoE Reports (e.g. S/2014/394, S/2015/401) had found that designated persons and entities conducted sanctioned activities in countries in other regions that were equipped with WMD technology development capabilities (e.g. in their academic or research institutes).

The Cayman Islands made this point directly in the introduction to its proliferation financing guidance: "As an international financial centre, the Cayman Islands is exposed to Proliferation Financing (PF) arising from external and internal sources. Financial services accounts for 40% of the GDP with majority of the financial services targeted towards non-resident customers, which contribute to higher PF risks. There is currently no evidence to suggest that Cayman Islands regulated entities are involved in financing proliferation activities. However, whilst there may be no direct PF links, the exposure of financial system when conducting business in the international financial market poses PF risks."

Source: *Cayman Islands Financial Reporting Authority Publication* (February 2020) *Identifying Proliferation Financing – Why Should You Be Concerned with the Prevention and Detection of Proliferation Financing*

36. **Sectoral vulnerabilities** refer to weakness in and contextual features of a particular sector that prompt designated persons and entities to exploit it for PF sanction evasion purposes. Weaknesses such as a low level of PF risk awareness, understanding of TFS requirements, and an overall weak culture of compliance within a sector all constitute vulnerabilities for misuse. Considerations may also include the relative complexity and reach of funds movement of each sector and sub-sector.

37. Based on the experiences of ML/TF risk assessments to date, countries tend to place greater emphasis on the banking or money or value transfer sectors, as designated persons and entities needed to access the international financial system to process payments for components or materials from overseas sources, which often have

more direct financial links to proliferating states (i.e. the DPRK and Iran).[29] The financial sector is only one sector that these actors have exploited. However, recent typologies have underscored how other sectors face exploitation by designated persons and entities, or those acting on their behalf or under their control, for the purposes of effecting a potential breach, non-implementation or evasion of PF-TFS. Countries should therefore be aware of which parts of the economy are subject to sector-specific UN sanctions, as these sectors would present a higher exposure to potential breach, non-implementation or evasion of PF-TFS. These sectors, as noted in recent UNSC PoE reports, include, but are not limited to:

a. **trust and company service providers**: creating corporate entities that designated persons and entities use to obscure the links between a financial transaction and a designated person or entity;

b. **dealers in precious metals and stones**: providing an alternative method for designated persons and entities to surreptitiously move financial resources across international borders;

c. **virtual assets service providers**: providing products to designated persons and entities have mined and stolen, and providing a platform for moving sums of money across international borders instantly; and

d. **the maritime sector**: designated persons and entities also exploit the maritime sector, which provide them the means to deliver components and materials for use in WMD or their delivery systems, to illicitly engage in economic sectors in violation of the provisions of UNSCRs, the revenue from which can provide the underlying financing for a WMD programme.

[29] "Despite the strengthening of financial sanctions in 2017, their effectiveness is being systematically undermined by the deceptive practices of the DPRK and the failure by Member States to recognise and prevent them. The DPRK enjoys ongoing access to the international financial system, as its financial networks have quickly adapted to the latest sanctions, using evasive methods in ways that make it difficult to detect their illicit activity." (UNSCR 1718 PoE Report, 2019)

How are DNFBPs misused for the purposes of the potential breach, non-implementation, or evasion of PF-TFS?

- **Trust and company service providers (including lawyers, notaries, and other legal professionals and accountants providing these services)**: use of shell and front companies, legal persons with ownership and control through nominees, legal persons or legal arrangements without apparent business reasons, company formation services.

  DPRK and Iran PF-TFS (e.g. UNSCR 2231 (2015), UNSCR 2270 (2016) OP 16) note that the both countries frequently use front companies, shell companies, joint ventures and complex, opaque ownership structures for the purpose of violating measures imposed in relevant UNSCRs, and the UNSCR 2270 (2016) also directs the UNSC 1718 Committee to identify individuals and entities engaging in such practices and designate them to be subject to relevant targeted financial sanctions in DPRK UNSCRs.

  Recent typologies identified by the UNSCR 1718 PoE indicated that designated persons and entities, and those persons and entities acting on their behalf have quickly adapted to sanctions and developed complex schemes to make it difficult to detect their illicit activities. One UNSCR 1718 PoE investigation in 2019 found that at least five front companies had been established by designated entities and those acting on their behalf to hide their beneficial ownership of the various cross-border (US-Dollar-denominated) financial transactions involving two different jurisdictions in Asia, and a different front company was used in each different transaction. In another UNSCR 1718 PoE investigation, shell and front companies were set up for transferring funds to designated persons and entities, and the companies were subsequently closed when the UNSCR 1718 PoE started enquiries about the companies.

- **Dealers in precious metals and stones:** designated persons and entities engaging such dealers to transport gold and diamonds to obtain foreign exchanges to finance their transactions. UNSC 1718 PoE reports highlight an investigation into DPRK diplomatic representatives smuggling gold between two countries in the Middle East (August 2020 Report) and the DPRK's involvement in gold mining in Sub-Saharan Africa (March 2020 Report).

Remarks: See Section 2 for guidance on risk mitigation measures
Source: UNSCR 1718 PoE Report (S/2019/691; S/2020/151; S/2020/840)

38. For a **PF risk assessment by a private sector firm**, it may consider the vulnerabilities associated with its products, services, customers and transactions. The vulnerabilities refer to weaknesses and features, which could be exploited for sanctions evasion purposes.

39. **Product- or service-specific vulnerabilities** may include whether a product or service provided by the financial institution or the DNFBP is complex in nature, has a cross-border reach (e.g. via the distribution channels), is easily accessible to customers, attracts a diverse customer base, or is offered by multiple subsidiaries or branches.

Which types of banking services/products are vulnerable to the potential breach, non-implementation, or evasion of PF-TFS?

Correspondent banking services provided by banks, though not always present a uniformly high-risk area, have been increasingly exploited by designated persons and entities as they often make use of international trade to conduct sanctions evasion activities. Correspondent banking services refers to the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services. Suh services enable financial institutions to conduct business and provide services to foreign customers without establishing a presence in foreign countries. Often, multiple intermediary financial institutions would be involved in a single transaction. These services allow the processing of wire transfers, international trade settlements, remittances, and cross-border payments. As identified in various UNSCR 1718 PoE Reports since 2017, correspondent banking services have enabled designated entities and their associates have made regular transfers to various facilitators in Asia and the Middle East, through personal and front company accounts, for these facilitators to perform transactions on their behalf. They had also set up a company in another jurisdiction in Asia and the company would arrange for payments to suppliers and transfers within the network, and initiate a series of transactions cleared through several U.S. correspondent banks that would have limited insight into the origin or beneficiaries of the transaction. As these cases demonstrate, financial institutions can face challenges screening transactions that go through foreign respondents as designated persons and entities tend to create layered corporate entities and shell companies to gain access to the international financial system. Financial institutions should understand the risk profile of their foreign respondents and determine appropriate measures to mitigate the risks.

Trade finance is another example of service exploited by designated persons and entities. This is because PF sanctions evasion often involves cross-border trade of goods or commodities. While the majority of trade is done through open-account transfers, many also take place using trade finance instruments, which involve a financial institution acting as an intermediary, guaranteeing a transaction if certain documentary requirements are met by the counterparties to the transaction (exporter and importer). As a result, the financial institution receives significantly more insight into the details of the trade. Designated persons and entities who have to rely on trade finance instruments will do so fraudulently, using forged documents, misrepresenting the parties to a transaction, or arranging for a different end-destination or end-user from the one listed in the paperwork.

Remarks: See Section 2 for guidance on risk mitigation measures
Source: UNSCR 1718 PoE Reports (S2017/150; S/2017/742; S/2018/171; S/2019/691)

How are virtual assets misused for the purposes of the potential breach, non-implementation, or evasion of PF-TFS?

As access to the formal financial system has become increasingly closed to designated persons and entities due to the introduction of various financial sanctions, they have used virtual assets as another means to evade sanctions. This novel method and technology to access financial services is particularly attractive to individuals, entities, and counterparties designated under DPRK-related PF-TFS, who have met increasing obstacles in accessing banking services due to the sanctions measures included in successive UNSCRs. The UNSCR 1718 PoE observed that there is a widespread and increasingly sophisticated use of cyber means by the DPRK to steal funds from financial institutions and VA exchanges across the world,[30] launder stolen proceeds and generate income, all while evading financial sanctions. Instances of such use have increased in "number, sophistication and scope since 2008, including a clear shift in 2016" to cyber/VASP-related attacks focused on generating revenue. Large-scale attacks against VA exchanges allow the DPRK to generate income that is often harder to trace and subject to less regulation than the traditional banking sector.

Some of the activities identified by the UNSCR 1718 PoE include, amongst others, the theft of VAs (through attacks on both exchanges and users) and the mining of cryptocurrencies through crypto-jacking (i.e. the introduction of malware to computers to turn those systems into cryptocurrency miners for the benefit of DPRK hackers), as well as through the use of its own computer networks to generate funds). To obfuscate these activities, a digital version of layering was used, which created thousands of transactions in real time through one-time use VA wallets. In one case, the stolen funds arising from an attack were transferred through at least 5 000 separate transactions and further routed through multiple jurisdictions before eventually converted to fiat currency. Transacting in some virtual asset arrangements allows largely instantaneous and nearly irreversible cross-border transfers of funds.

Some VA exchanges have been repeatedly attacked by entities designated under DPRK-related PF-TFS, with one exchanger suffering from at least four attacks over a period of three years from 2017 to 2019, resulting in losses of approximately USD 55 million in total. In another case, a VA exchange was attacked multiple times, with an initial loss of USD 4.8 million, and eventually 17% of its overall assets, forcing the exchange to close. Stolen VA proceeds were converted to anonymity-enhanced VAs through other VA exchanges, often in a complex series of hundreds of transactions with the aim of converting and cashing out all the stolen VAs into fiat currency.

Source: UNSCR 1718 PoE Report (S/2019/691); *2020 FATF Report on ML/TF Red Flag Indicators Associated with Virtual Assets*
Additional reference: *2019 FATF Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers*

40. **Identifying customer and transaction vulnerabilities** are crucial for risk assessments conducted by a financial institution or a DNFBP. As a starting point, they may consider to review the number of customers already identified as high risk, especially those often carrying out cross-border transactions involving legal persons and arrangements, or multiple shell or front companies. Information on the type and identity of the customer, as well as the nature, origin and purpose of the customer relationship is also relevant. Other considerations include: the number, amount (especially in cash), and frequency of transactions: (1) originating from, transiting through, or designating for an overseas jurisdiction that has weak implementation of relevant UNSCR obligations and FATF Standards, weak governance, law enforcement, and regulatory regimes; (2) involving individuals acting on behalf of a legal person or arrangement (e.g. authorised signatory, director); (3) that are unrelated to a private sector firm's stated business profile.

41. Additional **information sources for a risk assessment** may include known domestic or international typologies,[31] national risk assessments, supranational risk assessments, relevant sectoral reports published by competent authorities, relevant risk reports of other (especially neighbouring) jurisdictions on their respective sectors, supervisory reports on cases involving the breach, non-implementation or evasion of PF-TFS, risk assessment and risk mitigation (if publicly available), as well as FATF mutual evaluation reports and indicators/risk factors. A **private sector firm** would particularly benefit from information obtained from customer on-boarding and ongoing CDD processes, and transaction monitoring and screening, as well as internal audit and regulatory findings. Other information obtained through public-private information sharing initiatives on the weaknesses observed by both parties may also provide insights into vulnerabilities.

Analysis

42. Risk can be considered as a function of threat, vulnerability, and consequence. At this stage, countries, financial institutions, DNFBPs and VASPs should seek to understand the nature, sources, likelihood and consequences of the identified risk. As part of this process, they should assign a relative value or importance to each of these risks, and prioritise between identified risks. This stage involves a consideration of the potential likelihood and consequences of the materialisation of specific PF risks.

43. When analysing **likelihood**, considerations could include the prevalence of known cases, intelligence, typologies, strengths of CPF controls, as well as capabilities and intent of designated persons and entities. **Consequence** refers to impacts and harms, and can be further categorised into, for instance, physical, social, environmental, economic and structural. The starting point is to assume that the consequences of the potential breach, non-implementation or evasion of PF-TFS (including the potential development of WMD) would be severe. It is also important

---

30 The findings of the UNSCR 1718 PoE Reports were drawn from reports provided by member states from Africa (including North, South, and West), America (including Central and South), Asia (including North Asia, South Asia, and Southeast Asia) and Europe.

31 References can also be made to Part IIIA(ii) of the Guidance for higher risk customers and transactions that could be exploited by designated persons and entities, and those working on their behalf or direction.

to note that not all PF methods have equal consequences, and that consequences may differ depending on the source, channel, or intended recipients of the funds or assets. Ultimately, the consequence would like to make available funds to designated persons and entities, and those persons and entities acting on their behalf.

Evaluation and follow-up

44. As a result of risk analysis, the level of risks are often classified in one of these categories: low, medium, or high, with possible combinations between different categories (e.g. medium-high, medium-low). The same risk may be regarded as high in one country/private sector firm while in another country/private sector firm it may be regarded as low, depending on the prevailing context and circumstances. This classification aims to assist in the understanding and prioritisation of PF risks. **Evaluation** involves using the results of the analysis to determine priority risk areas. Section 4.3 of the *2013 FATF NRA Guidance* provides detailed guidance on this process, which can be adapted for the purpose of a PF risk assessment. The outcome of a risk assessment should be disseminated to competent authorities (including supervisors) and relevant personnel within relevant private sector firms.

45. At the national level, competent authorities should establish and implement a national CPF legislative framework, and national policies, priorities and action plans to address the identified risks. Competent authorities may also consider releasing the results of the assessment as appropriate to promote a broader understanding of the risk of PF-TFS evasion. As for the **private sector**, financial institutions, DNFBPs and VASPs should consider adapting/calibrating/enhancing their policies, controls, and procedures to effectively manage and mitigate the identified risks. Financial institutions, DNFBPs and VASPs may also review and make reference to suspected activity of the breach, non-implementation or evasion of PF-TFS[32] to inform their findings of any risk assessment. They should allocate appropriate and proportionate resources, and provide training to relevant personnel on the implementation of CPF measures based on the findings.

Public-private collaboration

46. Assessment of proliferation financing risks requires co-operation between public and private sectors.[33] Similar to the implementation of TFS, effective sharing of information and a co-ordinated approach in communicating with the private sector are fundamental when conducting a risk assessment. The public sector authorities may have typologies or information on suspected and previous proliferation financing sanctions evasion or information on structural and sectoral

---

32 The FATF Standards do not require filing of PF-TFS information to financial intelligence units. However, if a jurisdiction requires the reporting of suspicious or other information in relation to the breach, non-implementation or evasion of PF-TFS within the jurisdiction, and corresponding information is available, financial institutions, DNFBPs and VASPs may also consider making reference of such available information.

33 The *2019 FATF TFRA Guidance* also provides guidance and examples on engagement with non-government stakeholders, including the use of multi-stakeholder working groups and public-private collaboration to assess TF risks (see paragraphs 24-26 and case boxes).

vulnerabilities mentioned in previous section, which would be essential to the private sector in terms of identifying, assessing, and understanding their risks. The information related to proliferation financing sanctions evasion activities is very sensitive, but this should not prevent it (or an unclassified/sanitised version of it) from being shared for the purpose of a risk assessment, if possible, and subject to appropriate safeguards in place. There is a variety of ways in which the public sector can share information, with varying degrees of sensitivity, with the private sector. For example, discussion and sharing of sensitive information on an ad-hoc basis to a selected number of private sector participants and/or industry roundtables focus on best practice or general trends. Information sharing by relevant public authorities would be particularly useful for smaller, non-bank financial institutions, DNFBPs and VASPs, which may likely have a weaker understanding or fewer support in carrying out a risk assessment. On the other hand, the private sector may hold vital information for both public and other private sector for PF risk assessment purposes. For example, the banking sector would likely hold information relevant to the assessment of PF risks in a number of other sectors such as Trust and Company Service Providers (TCSPs).

47. Having an ongoing or a continuous public-private engagement or dialogue prior to the commencement of and throughout the different stages of a risk assessment, and in line with relevant legislative requirements, public-private-partnership frameworks, and confidentiality considerations, may enhance the quality of data used and analysis applied in a risk assessment. The involvement of all relevant competent authorities and private sector stakeholders (including both small and large entities in different sectors) may also build trust and allow open dialogue throughout the preparation of risk assessments. Countries can maintain this dialogue on an ongoing basis in order to educate the private sector on the evolving nature of the threat from the financing of proliferation, which can shift rapidly. The dialogue will also provide a feedback mechanism for the private sector to inform governments about how they have applied risk assessments to their day-to-day compliance function.

Maintaining an up-to-date assessment

48. The FATF Standards (INR.1) require jurisdictions to maintain an up-to-date assessment of their PF risks. Similar to an ML/TF risk assessment, an assessment of PF risks should be updated regularly and be an evolving process, taking into account current threats and sanctions requirements on the potential breach, non-implementation or evasion of PF-TFS. These updated assessments need to develop more specific or thematic analysis, and are likely to become more refined over time. Countries are strongly encouraged to make available the results of the updated risk assessments (or a sanitised version) in the public. If a publication is considered not possible, countries may consider sharing an updated version (full or sanitised) with private sector entities in a confidential manner to ensure that information on PF threats and indicators is reaching the widest possible audience.

49. As additionally noted in INR.1, countries should ensure compliance with R.1 in all risk scenarios. For situations where countries have identified a high level of risk, countries should require financial institutions, DNFBPs and VASPs to take commensurate measures to manage and mitigate these risks (see Section 2 below). Countries doing so will strengthen their national legal and regulatory regime for countering the financing of proliferation, and be in a stronger position to effectively

require appropriate actions by their private sector. For countries that have identified a lower risk, the FATF requires countries to apply measures commensurate with that risks. Those countries should, however, understand that the nature of the PF threat is ever changing and methodologies that designated persons or entities, or those acting on their behalf or under their control, deliberately target jurisdictions who feel that they have weaker risk exposure.

SECTION TWO: MITIGATION OF PROLIFERATION FINANCING RISKS

50. The FATF Standards require countries, financial institutions, DNFBPs and VASPs to take appropriate steps to manage and mitigate proliferation financing risks that they identify. Section 1 of this Guidance provides guidelines to countries and to the private sectors on conducting proliferation financing risk assessments.

51. In the context of FATF Recommendation 1 and this Guidance, proliferation financing risk refers strictly and only to the risk of potential breach, non-implementation or evasion of TFS obligations as set out in Recommendation 7. This requires countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, 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, or persons and entities acting on their behalf, at their direction, or owned or controlled by them.[34]

52. Apart from using other means, proliferation support networks use the international financial system to carry out their activities, often acting through a global network of indirectly connected illicit intermediaries, front companies and shell companies to hide their beneficial ownership. These global networks are complex and designed to erode the effectiveness of TFS by separating proliferation activity from designated persons and entities. These networks also co-mingle legitimate business with illicit transactions, which adds another challenge and layer of complexity for the robust enforcement of the UN sanctions regime.

53. This section highlights specific measures that countries, financial institutions, DNFBPs and VASPs could take to mitigate their proliferation financing risks. The nature and extent of mitigation measures would depend on contextual factors, as well as on the source of proliferation financing risks.

54. Financial institutions, DNFPBs and VASPs should identify, assess and understand their proliferation financing risks and take commensurate measures in order to mitigate them. It is, however, inappropriate to indiscriminately terminate or restrict business relationships of entire classes of customers, without taking into account, seriously and comprehensively, their level of risk and risk mitigation measures for individual customers within a particular sector. Risk avoidance does not equate risk mitigation; rather it can result into subsequent problematic consequences like

[34] Provided, those acting on behalf or under control of designated persons and entities or owned or controlled by them are not designated under national/supranational sanctions regimes.

financial exclusion risk, leading to denial of access to financial services for those who need it. Financial exclusion of customers holds serious risks as customers may seek the services of unregulated providers or providers who may not have robust risk control measures. Where decisions to restrict or terminate relationship with customers is due to a lack of understanding of the regulatory expectations, supervisors should be able to provide appropriate guidance.

Risk mitigation measures by countries

55. Understanding the ways in which a breach, non-implementation or evasion of TFS could occur within a jurisdiction will help countries put in place an effective domestic framework for mitigating the risks and ultimately ensuring full compliance with targeted financial sanctions obligations under relevant country specific UNSCRs. An assessment of risks and vulnerabilities will identify potential gaps that will help countries and the private sectors to set out appropriate mitigation measures to address them.

56. Countries should allow financial institutions, DNFBPs and VASPs to leverage their existing targeted financial sanctions and/or compliance programmes to manage and mitigate these proliferation financing risks. This would help them build upon their existing frameworks and tools for an effective CPF regime. In many cases, the enterprise-wide risk management programmes conducted by large/complex financial institutions with tailored and sophisticated processes for ML/TF and sanctions risk already incorporates the assessment and mitigation of PF risks. A PF risk assessment does not have to be an individual exercise but can be covered by existing ML or sanctions risk assessments. PF risk management and controls can be part of existing enterprise-wide risk management programmes and processes.

Foundational elements of proliferation financing risk mitigation

57. A robust system for implementing targeted financial sanctions sets a strong foundation for effective risk mitigation, and has the following elements in place:

    a. **National risk assessment:** As highlighted in Section 1 of this Guidance, national risk assessments could be helpful to informing and strengthening the CPF regime of a country. They should also help countries and private sector entities to determine and prioritise the amount of resources necessary to mitigate the risks.

    b. **Institutional risk assessment**: Financial institutions, DNFBPs and VASPs should be required to take appropriate steps to identify and assess their proliferation financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Financial institutions, DNFBPs and VASPs should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

c. **Effective legal framework:** Countries should have effective legal frameworks to implement proliferation-related targeted financial sanctions without delay in line with Recommendation 7. They should establish the relevant authorities and identify competent authorities responsible for implementing and enforcing targeted financial sanctions. Clear institutional mechanisms, processes and responsibilities would help authorities focus on areas of vulnerability and detect means by which designated persons and entities might evade the sanctions in different sectors. It would help them effectively implement the sanctions regime, including by taking relevant actions (e.g. ensuring that financing is denied, funds and assets are frozen and violations are sanctioned).

d. **Communication of sanctions:** Countries should have effective mechanisms to ensure that designations are notified to all relevant parties, including financial institutions, DNFBPs and VASPs, in a timely manner. Countries should also have efficient processes for updating lists of designated entities and persons, so that changes are communicated to and are acted upon by the private sectors promptly. This would prevent financial institutions, DNFBPs and VASPs from dealing with the designated persons and entities during the time changes are being transposed to the domestic frameworks following the UN designations.

e. **Domestic co-operation, co-ordination and information sharing:** In line with Recommendation 2 and its Interpretive Note, countries should have an inter-agency framework in place to mitigate proliferation financing risks more effectively. This would mean effective co-operation and co-ordination among all the relevant departments, agencies and organisations, which are generally involved in combating proliferation and proliferation financing at the national level. This could include supervisors, import and export controls and licensing authorities, customs, as well as border controls and intelligence agencies, where possible. A close co-operation and co-ordination among these competent authorities would facilitate exchange of relevant information. This could help initiate and pursue investigations into potential violations of the targeted financial sanctions regime.

f. **Compliance monitoring and enforcement** is key to ensure sustained compliance. Financial institutions, DNFBPs and VASPs should be subject to supervision or monitoring to ensure their full compliance with their targeted financial sanctions obligations. Failure to comply should result in appropriate civil, administrative or criminal sanctions where required. Supervisors should consider the PF risks faced by financial institutions, DNFBPs and VASPs in their supervision or monitoring activities and approach. The frequency, depth and intensity of such supervision or monitoring mechanisms, and the level of sanctions applied in response to compliance failures should be reviewed periodically to ensure that risks are adequately addressed and mitigated.

g. **Regular and in-depth training (conducted by both public and private sectors) in the areas of targeted financial sanctions obligations and risks** for supervisors, customs and export controls, financial intelligence, regulatory authorities and other agencies involved in counter proliferation financing as well as financial institutions,

DNFBPs and VASPs should help build capacity and lead to better overall compliance with the TFS regime. Understanding public/private training needs and identifying priority areas for expanded training may advance the effective implementation of controls to mitigate the risks.

Mitigating specific sanctions evasion risks at national level

58. **Operational and strategic co-ordination and information sharing** among key organisations and departments would ensure that CPF authorities can communicate with one another and respond to requests for assistance where needed, according to their institutional framework. This would also help authorities identify networks and/or funding channels associated with designated persons and entities and potential avenues of evasion of sanctions. For example, effective exchange of actionable information between export controls authorities and relevant competent authorities, where appropriate, could, in some cases, unearth cases of evasion of targeted financial sanctions.

59. Many authorities maintain their own enforcement and other databases and reports such as cases where export licences were denied due to suspected linkages with designated persons and entities, past cases of sanctions evasion, and information on suspected sanctions violations. Timely sharing of such information, if available and as appropriate within the existing institutional framework could help relevant authorities to develop a comprehensive picture of recent trends and methods designated persons and entities might be using to circumvent the applicable sanctions, and take measures to prevent or mitigate these risks.

60. **Public-private information sharing partnerships** are valuable platforms for information sharing between stakeholders. They could allow governments to share useful information (e.g. typologies, evasion indicators, best practices) with private sector contacts, which can then analyse their own customer and transaction records to identify current and historical potentially illicit activity, including the potential evasion of sanctions. The exchange would strengthen the public sector's ability to identify and mitigate risks and issue targeted guidance aimed at the private sector entities (including higher and small and lower risk sectors or institutions), while preserving its responsibility to maintain customer privacy. Conversely, as appropriate within the existing domestic framework, any suspected proliferation financing activity identified through this analysis can be shared with the public sector to strengthen the government's ability to assess its own risks. Such exchanges of information should be subject to legal requirements (including data protection and privacy considerations) and proper evaluation and verification. Nonetheless, creating opportunities for regular interactions and exchanges between public and private sector entities would help ensure that proliferation financing targeted financial sanctions evasions are properly understood and guarded against.

61. **Outreach and points of contact enable private sectors to contact governments when they have concerns or need guidance.** In accordance with the institutional framework, countries should conduct outreach to financial institutions, DNFBPs and VASPs to explain key elements of their targeted financial sanctions programmes, including the action required if financial institutions, DNFBPs and VASPs find a match against designated entities or persons. Where needed, financial institutions, DNFBPs and VASPs should be able to access timely guidance from relevant competent authorities (including supervisors) on potential matches and

implications for the proliferation financing sanctions regime. This would help avoid inadvertent breach, and build trust and confidence between the public and private sectors.

62. **Specific guidance on preventing the evasion of sanctions and feedback:** One of the key challenges to effective implementation of targeted financial sanctions is how to prevent evasion of sanctions by ensuring that financial institutions, DNFBPs and VASPs are adequately implementing CDD measures such that they are able to ascertain the ultimate beneficial owner of a customer. This is relevant as designated persons and entities, including those acting on their behalf, can use offshore accounts and set up joint ventures with accessory or unaware third party companies to hide the true beneficial owners. They can also use shell and front companies, dummy accounts and strawmen to access the regulated financial system and hide their connection to illicit transactions and business relationships.[35] All countries should comply fully with the FATF Recommendations relevant in ensuring the transparency of beneficial ownership of legal persons and legal arrangements.

63. **Regulatory actions to address specific risks:** This could include the following specific measures put in place by countries, if the risk of evasion of targeted financial sanctions cannot be mitigated by the private sectors:

    a. Regulatory actions (e.g. limiting business relationships or financial transactions) if they pose an unacceptably high risk of sanctions evasion, which cannot be adequately mitigated by the private sectors;

    b. Regulatory or supervisory directives to apply specific measures (e.g. enhanced due diligence, transaction monitoring and screening) to prevent and mitigate the risk of evasion of targeted financial sanctions- such directives should be complemented by relevant guidance and best practice papers from the authorities; and

    c. Supervisory actions (e.g. additional/thematic inspections focused on at-risk business units; restriction of the activities of firms found to be negligent; enhanced monitoring of firms) where applicable.

Risk mitigation measures by financial institutions, DNFBPs and VASPs

64. Financial institutions, DNFBPs and VASPs are at the front lines of combating proliferation financing. Countries should ensure that financial institutions, DNFBPs and VASPs take steps to identify circumstances in which customers and transactions may present proliferation financing risks, and ensure that their sanctions policies, controls and procedures address these risks, in accordance with national legislation. Countries should provide relevant information (e.g. sanitised case examples, typologies, results of national risk assessments), and share their knowledge and experience to facilitate the understanding of proliferation financing risks by financial institutions, DNFBPs and VASPs.

65. Financial institutions, DNFBPs and VASPs should develop a clear understanding of the contextual information and the sources of proliferation financing risks that they are exposed to, and take appropriate measures to mitigate them, in accordance with

[35] See UNSCR 1718 PoE May 2020 Report (Section IV).

national legislation. The nature of risk mitigation measures will depend on the source and degree of risks and could include:

a. Improved onboarding processes for customers (including beneficial owners);

b. Enhanced customer due diligence procedures;

c. Effective maintenance of customer master data;

d. Regular controls to ensure effectiveness of procedures for sanctions screening; and

e. Leveraging the existing compliance programmes (including internal controls) to identify potential sanctions evasion.

Risk mitigation in case of low risk

66. Low risk financial institutions, DNFBPs and VASPs such as those, which are small and serving predominantly locally-based and lower risk customers, are not expected to devote a significant amount of time and resources to risk mitigation. It would be reasonable for such institutions to rely on publicly available records and information supplied by a customer for screening against the list of designated entities and individuals to meet their obligations. For the vast majority of low risk institutions, it is also reasonable to expect them to maintain their sanctions screening measures and customer due diligence measures to mitigate their risks, without the need to deploy enhanced measures despite the existence of low risk.

67. The FATF Standards provide flexibility to countries to exempt a particular type of financial institution, DNFBP or VASP from the requirements to identify, assess, monitor, manage and mitigate proliferation financing risks, provided there is a proven low proliferation financing risk relating to such financial institutions, DNFBPs or VASPs. The national risk assessment should provide useful background information to identify low risk situations, which could benefit from an exemption. This will also help develop an understanding of financial inclusion products and services, including risks associated with financial exclusion, which could be counterproductive. Countries should consider using the flexibility provided in the FATF Standards in a timely and responsive manner. As risk profiles can change over time, countries should monitor such exemptions. Nevertheless, full application of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

Mitigating the risks of a potential breach or non-implementation of sanctions

68. A sanctions breach and failure to implement sanctions may typically result from inadequate internal controls (e.g. inadequate CDD and record keeping, delays in screening customers, inadequate transaction monitoring and screening systems and procedures, use of out-of-date sanctions lists and lack of accuracy in matching names). Mitigating these risks essentially requires building sound processes and internal controls, and ensuring these are followed.

69. The FATF Standards require the implementation of targeted financial sanctions without delay. Where the domestic regulatory framework allows it, financial institutions, DNFBPs and VASPs could incorporate changes in UN designations into

their monitoring and surveillance system without waiting for national transposition or communication.

70. Training for staff, in particular for those responsible for onboarding customers and maintaining customer relationships, monitoring and screening transactions and handling risk assessments is fundamental in a strong compliance regime. As appropriate, staff should be aware of proliferation financing risks, typologies in relation to the breach, non-implementation or evasion of targeted financial sanctions, and the required risk mitigation measures. These training programmes can be rolled into the existing sanctions training or wider AML/CFT training modules.

Mitigating the risks of evasion of sanctions

71. Mitigating sanctions evasion risks does not imply a "zero-failure" approach. It aims at reducing the risks as much as reasonable and practicable by following an approach proportionate to risks. Sanctions evasion schemes aim to hide the designated persons and entities. As the very objective of these schemes is to circumvent sanctions, financial institutions, DNFBPs and VASPs could be in situations where despite a good understanding of risks, a robust compliance function and sound due diligence, they might not be able to detect all potential evasion of targeted financial sanctions. However, this gives rise to financial, legal and reputational risks for these institutions. The risks increase when a financial institution, DNFBP or VASP does not understand the risks of potential sanctions evasion schemes and how to implement tailored, risk-based measures to mitigate those risks.

72. Financial institutions, DNFBPs and VASPs with higher risks may proactively incorporate, as appropriate, a wide range of information for their compliance policies and procedures, which may include guidance provided by governments, risk indicators, typologies and reports of Panel of Experts of the relevant UNSCRs regarding proliferation financing aspects, into their risk management practices and procedures to prevent the evasion of sanctions by illicit players. These practices and procedures should be tailored to the risk profile of these institutions and periodically reviewed to ensure they remain relevant and up-to-date with current trends.

73. Investment in technology and advanced software, capable of machine learning and artificial intelligence to conduct analysis may help strengthen the compliance practices of large and complex financial institutions, DNFBPs and VASPs that could be exposed to a higher level of proliferation financing risks. This would enable them to identify linkages and relationships, and build proliferation financing scenarios and recognise patterns (e.g. transaction times, value, purpose, counterparties, geolocation), which would be difficult to establish otherwise. As designated entities and individuals are increasingly using advanced deception techniques, including wire/payments stripping techniques[36] to hide their true identities and conceal the

[36] Stripping is the deliberate act of changing or removing information from a payment or instruction, to obscure the identity of the payment originator/beneficiary or to connect them to designated individuals or entities.

beneficial owners, financial institutions, DNFBPs and VASPs should be vigilant to such risks and deploy appropriate tools to address such risks.

Enhanced customer due diligence

74. Effective implementation of customer due diligence measures helps financial institutions, DNFBPs and VASPs manage and mitigate their proliferation financing risks, as designated persons and entities continue to adapt and advance their sanctions evasion techniques to avoid detection and identification. Their efforts include the creation of complex networks of corporate entities with opaque ownership in order to avoid linkage with a designated person or entity. As a result, financial institutions, DNFBPs and VASPs could find that screening against list of designated entities is insufficient to properly manage the risk of breach, non-implementation or evasion of TFS related to proliferation or its financing.

75. Some financial institutions, DNFBPs and VASPs have adapted their existing CDD measures and monitoring of transactions to enable the detection of potential violations of TFS including sanctions evasion. Financial institutions, DNFBPs and VASPs should consider using additional Proliferation financing – TFS specific risk indicators to the criteria used for customer onboarding and monitoring ongoing customer relationships, in order to effectively defend against such risks.

76. The nature of business of financial institutions, DNFBPs and VASPs and their services should determine the scope of internal controls, including CDD measures, suitable for mitigating the risk of evasion of sanctions. For example, small and low risk businesses having limited business activities with regular customers and a pattern of repeat micro-transactions often linked to a pay or salary cycle, may not have a board or separate and sophisticated compliance function and system.

77. Financial institutions, DNFBPs and VASPs should: (a) use a proliferation financing risk assessment to guide institutional compliance regimes and employee awareness of the risks, and of which customers may be exposed to those risks; and (b) apply specific enhanced measures, where necessary (e.g. obtaining additional information on the customer, obtaining additional information on the intended nature of the business relationship, and updating more frequently the identification data of customer and beneficial owner, obtaining information on the source of funds and wealth, on the reasons for intended or performed transactions, obtaining the approval of senior management to commence or continue business relationship, conducting enhanced monitoring of the business relationship by increasing the timing and number of controls applied, requesting information from counterparty financial institution on the nature of their business, where allowed and appropriate).

Correspondent banking relationships[37]

78. Cross-border correspondent banking is a key element of an integrated financial system and therefore of global trade. However, screening transactions that go

[37] The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15. The issues raised in this section and mitigation measures applied, are not to be assessed under Recommendation 13.

through foreign respondents can be challenging as designated persons and entities tend to create layered corporate entities and shell companies to gain access to the international financial system. Financial institutions should understand the risk profile of their foreign respondents and determine appropriate measures to mitigate the risks.

79. However, it does not mean that all correspondent banking relationships present a uniform or unacceptably high risk of being exploited for proliferation financing, and that banks should avoid doing business with respondent banks based in jurisdictions or regions perceived to be exposed to high proliferation financing risk. Risk assessment of correspondent relationships should be done on a case-by-case basis for each relationship, and should always take account of the internal controls and risk mitigation measures applied by the respondent bank, like with regard to ML/TF risks. This would help them manage and mitigate their own risks by having appropriate controls, due diligence and additional CDD measures. Correspondent institutions should conduct ongoing due diligence of the correspondent banking relationship, including periodical reviews of the CDD information on the respondent institution as outlined in the *2016 FATF Guidance on Correspondent Banking Services*.[38]

Shell and front companies

80. Shell companies can be relatively quick and simple to set up. They provide designated entities and individuals the ability to conduct business anonymously. Often, these companies are abused for a brief period of time, moving money for a particular transaction or series of transactions. Designated entities or individuals have been found to use extensive networks of shell companies for perpetrating their schemes. Failure to conduct thorough due diligence, as required under R.10 (e.g. to understand the nature of the business and to identify the beneficial owners of companies), may result in the involvement of designated entities or individuals in the transactions going undetected, leading to significant compliance failures.

81. The use of shell companies and front companies, and intermediaries and middlemen acting on behalf of designated entities and persons creates complexity in transaction monitoring and screening. Where appropriate, financial institutions, DNFBPs and VASPs should supplement the reliance on list-based screening by additional due diligence measures (e.g. enhanced CDD) to mitigate the risk of potential sanctions evasion. Financial institutions, DNFBPs and VASPs should understand the nature of their customer's business and identify and verify the customer's authorised signatories and beneficial owners in order to ensure that they are not directly or indirectly dealing with designated persons and entities. They should be vigilant at the time of onboarding of customers and throughout the course of the customer relationship to adequately address these risks.

82. Company service providers, lawyers and accountants involved in the creation or management of companies and other legal persons or legal arrangements, in particular, face transaction and service risks. These structures may be misused to obscure ownership or may have no real economic purpose, and the very objective of their formation or operation may be to circumvent and evade sanctions.

---

38 See paragraph 29 of the *2016 FATF Guidance on Correspondent Banking Services*.

Designated entities and individuals seek the involvement of these professionals to provide respectability and legitimacy to their activities. In order to mitigate the risks, these service providers should have internal policies and procedures to obtain information on the beneficial owners of their customers and understand the true nature of their customers' business and ownership and control structures, in accordance with national legislation.

SECTION THREE: SUPERVISION OF PROLIFERATION FINANCING RISK ASSESSMENT AND MITIGATION[39]

83. This section provides general guidance on how proliferation financing risk assessment and mitigation by financial institutions, DNFBPs and VASPs should be supervised or monitored by supervisors and SRBs, noting that mitigating sanctions evasion risks does not imply a "zero-failure" approach.

84. Supervisors can assess the proliferation financing risk assessments created by financial institutions, DNFBPs and VASPs as part of their pre-existing sanctions compliance or financial crimes compliance programme. It need not oblige financial institutions, DNFBPs and VASPs to do a separate risk assessment, or retain compliance staff specifically for proliferation financing risk.

85. The FATF has developed a separate risk-based Guidance[40] to clarify and explain how supervisors should apply a risk-based approach to their supervision and/or monitoring of financial institutions, DNFBPs and VASPs in assessing and managing ML/TF risk, in line with the FATF Standards. While that Guidance is focused on AML/CFT, supervisors should consider taking relevant aspects of that Guidance into account while developing their supervisory approaches for supervision or monitoring of proliferation financing risk assessment and mitigation by their supervised entities. Considerations that supervisors could take into account include, but are not necessarily limited to:

    a. Supervisors should have a process in place to obtain and maintain an up-to-date understanding of the proliferation financing risks landscape, and systematically identify and assess the level of risk in different sectors and individual entities on a periodic basis, taking into consideration their exposure to risks and efficacy of their internal controls;

    b. The proliferation financing risk classification of Financial Institutions, DNFBPs or VASPs should be taken into account, along with other parameters used by supervisors, when determining the intensity and

---

39 The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15. The issues raised in this section in the context of supervision and monitoring are not to be assessed under Recommendations 26, 27, 28 and 35.

40 See *2021 FATF Risk-based Supervision Guidance*.

frequency of supervision. For example, lower-risk institutions should attract less supervisory attention (e.g. less frequent or intense scrutiny than higher risk entities);

c. Supervisors should keep the risk assessment process dynamic, by leveraging available information and data from both internal and external sources,[41] as part of their ongoing supervision and monitoring of entities;

d. Supervisors should focus on the effectiveness of internal controls, targeted financial sanctions screening processes and customer onboarding processes and transaction monitoring and screening processes. They should review whether supervised institutions are adequately implementing CDD measures to identify and verify the identity of a customer, the customer's beneficial owner(s), understand the nature and purposes of the customer relationship in order to develop customer risk profiles, and conduct ongoing monitoring, on a risk basis, to maintain and updated customer information.

e. Supervisors may note that PF risks may be distributed differently from ML/TF risks between and within supervised institutions. Adequately supervising the implementation of PF risk assessment and mitigation may require supervisors to focus on different business units and different products from those which are relevant to AML/CFT supervision;

f. Supervisors should take steps (e.g. outreach, guidance, information sharing) to ensure that their supervised institutions understand their PF risks and apply commensurate risk mitigation measures;

g. Supervisors should consider the capacity and the counter proliferation financing experience of the supervised institutions and individual sectors, and their understanding of targeted financial sanctions obligations and risks while developing their supervisory programmes;

h. Based on supervisory risk assessment, supervisors should determine methodology and procedures of supervisory activities, including the types of tools employed (e.g. questionnaires, off-site reporting, interviews, sample testing, on-site visits);

i. Supervisors should consider risks faced by financial institutions, DNFBPs and VASPs for determining the intensity, type and frequency of supervisory activities;

j. Supervisors should determine in the course of supervision the extent of board and senior management oversight of proliferation financing matters and adequacy of escalation of proliferation financing-related issues to board and senior management;

---

41 The types of information that might form the basis of the supervisor's risk assessment include, but are not limited to: national risk assessments, information collected from financial institutions, DNFBPs and VASPs either off-site or on-site, the results of examinations and supervisory processes, and information from the Financial Intelligence Unit, including typologies and feedback on suspicious transaction reports.

k. Supervisors should focus on supervised institutions' identification and management of legitimate matches and false positives during screening;

l. Supervisors should focus on supervised institutions' ability to identify designated persons and entities in the implementation of controls on persons and entities subject to targeted financial sanctions;

m. For DNFBP sectors in particular, supervisors and self-regulatory bodies should note the vulnerabilities associated with company formation services, which are typically provided by company service providers, lawyers and accountants;

n. Where weaknesses are identified in the areas of risk assessment or risk mitigation, supervisors should follow up and assess the robustness of remedial actions taken to rectify the deficiencies, and to prevent recurrences;

o. For regulatory breaches arising from compliance failures, supervisors should have a broad range of regulatory/supervisory measures available that can be applied to address the risks and encourage individual firms and wider sectors to increase their compliance efforts. These enforcement measures include, but are not limited to: administrative sanctions, withdrawal of licenses to operate, etc. Proper enforcement can encourage a culture of compliance among supervised entities.

Annex A. FATF Recommendations on Counter Proliferation Financing

RECOMMENDATION 1: ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH
(Remarks: Extract text on PF only)

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 commensurate 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 commensurate with 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 action to mitigate their money laundering, terrorist financing and proliferation financing risks.

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING ML/TF RISKS AND APPLYING A RISK-BASED APPROACH)
(Remarks: Extract text on PF only)

ASSESSING PROLIFERATION FINANCING RISKS AND APPLYING RISK-BASED MEASURES

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.[2] These obligations set out in Recommendation 7 place strict requirements on all natural and legal persons, which are not risk-based. In the context of proliferation financing risk, risk-based measures by financial institutions and DNFBPs seek to reinforce and complement the full implementation of the strict requirements of Recommendation 7, by detecting and preventing the non-implementation, potential breach, or evasion of targeted financial sanctions. In determining the measures to mitigate proliferation financing risks in a sector, countries should consider the proliferation financing risks associated with the relevant sector. By adopting risk-based measures, competent authorities, financial institutions and DNFBPs should be able to ensure that these measures are commensurate with the risks identified, and that would enable them to make decisions on how to allocate their own resources in the most effective way.

Financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks.[3] This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate the

risks. Where the risks are lower, they should ensure that the measures applied are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

A. Obligations and decisions for countries

PF risk

Assessing PF risk - Countries[5] should take appropriate steps to identify and assess the proliferation financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's CPF regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of CPF resources by competent authorities; and (iii) make information available for PF risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and SRBs, financial institutions and DNFBPs.

Mitigating PF risk - Countries should take appropriate steps to manage and mitigate the proliferation financing risks that they identify. Countries should develop an understanding of the means of potential breaches, evasion and non-implementation of targeted financial sanctions present in their countries that can be shared within and across competent authorities and with the private sector. Countries should ensure that financial institutions and DNFBPs take steps to identify circumstances, which may present higher risks and ensure that their CPF regime addresses these risks. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate these risks. Correspondingly, where the risks are lower, they should ensure that the measures applied are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

B. Obligations and decisions for financial institutions and DNFBPs

PF risk

Assessing PF risk - Financial institutions and DNFBPs should be required to take appropriate steps, to identify and assess their proliferation financing risks. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

Mitigating PF risk - Financial institutions and DNFBPs should have policies, controls and procedures to manage and mitigate effectively the risks that have been identified. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies,

controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate the risks (i.e. introducing enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7). Correspondingly, where the risks are lower, they should ensure that those measures are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

Footnotes of INR.1

2. Paragraphs 1 and 2 of the Interpretive Note to Recommendation 7, and the related footnotes, set out the scope of Recommendation 7 obligations; including that it is limited to targeted financial sanctions and does not cover other requirements of the UNSCRs. The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15 only. The requirements under Recommendation 1 for PF risk assessment and mitigation, therefore, do not expand the scope of other requirements under other Recommendations.

3. Countries may decide to exempt a particular type of financial institution or DNFBP from the requirements to identify, assess, monitor, manage and mitigate proliferation financing risks, provided there is a proven low risk of proliferation financing relating to such financial institutions or DNFBPs. However, full implementation of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

5. Where appropriate, PF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

RECOMMENDATION 7: TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION

Countries should implement targeted financial sanctions to comply with United Nations 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.

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[14] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no

funds and other assets are made available to, and for the benefit of, any person[15] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[16]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.17 The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) provides that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions. Resolution 2231 (2015) provides that the Security Council shall make the necessary practical arrangements to undertake directly tasks related to the implementation of the resolution.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

a. identifying a competent authority(ies), either executive or judicial, as having responsibility for:

   (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions[18], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

   (ii) proposing to the Security Council, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 2231 (2015) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with

relevant Security Council resolutions).

b. having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 2231 (2015), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

c. having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

d. when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

e. when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the Security Council, pursuant to resolution 2231 (2015) and any future successor resolutions, providing as much detail as possible on:

   (iii) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

   (iv) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

f. having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

a. in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[19]; and

b. in the case of resolution 2231 (2015) and any future successor resolutions by the Security Council,

when acting under the authority of Chapter VII of the Charter of the United Nations.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

a. Countries[20] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

b. Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

c. Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

d. Countries should require financial institutions and DNFBPs[21] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

e. countries should adopt effective measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

f. Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of

resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

9. Where countries have determined that the exemption conditions set out in resolution 1718 (2006) and resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 2231 (2015) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) and continued by resolution 2231 (2015), or taken pursuant to resolution 2231 (2015), shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

(a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in resolution 2231 (2015) and any future successor resolutions;

(b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to resolution 2231 (2015); and

(c) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.[22]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016):

(i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

(ii) any person or entity providing support for DPRK's nuclear-related, other WMD related and ballistic missile-related programmes, including through illicit means;

(iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[23];

(iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[24];

(v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

(vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

(b) On Iran - Resolution 2231 (2015):

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities contrary to Iran's commitments in the Joint Comprehensive Plan of Action (JCPOA) or the development of nuclear weapon delivery systems, including through the involvement in procurement of prohibited items, goods, equipment, materials and technology specified in Annex B to resolution 2231 (2015);

(ii) any person or entity assisting designated persons or entities in evading or acting inconsistently with the JCPOA or resolution 2231 (2015); and

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

Footnotes of INR.7

14. Recommendation 7 is focused on targeted financial sanctions. These include the specific restrictions set out in Security Council resolution 2231 (2015) (see Annex B paragraphs 6(c) and (d)). 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.

15. Natural or legal person.

16. Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretive Note (June 2017), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). Resolution 2231 (2015), endorsing the Joint Comprehensive Plan of Action, terminated all provisions of resolutions relating to Iran and proliferation financing, including 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

17. Based on requirements set, for instance, in the Nuclear Non-Proliferation Treaty, the Biological and Toxin Weapons Convention, the Chemical Weapons Convention, and Security Council resolutions 1540 (2004) and 2235 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

18. Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

19. As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

20. In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within

the EU have to respect the freeze and not make funds available to designated persons and entities.

21. Security Council resolutions apply to all natural and legal persons within the country.

22. In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013.

23. The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

24. Ibid.

Source: The FATF Recommendations

Annex B. Bibliography and References

FATF Publications on Proliferation Financing

FATF (2008), *Proliferation Financing Report,* FATF, Paris, www.fatf-gafi.org/topics/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

FATF (2010), *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

FATF (2018), *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf

FATF Publications on Risk Assessment and Risk Mitigation

FATF (2013), *FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment*, FATF, Paris, www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

FATF (2015), *FATF Guidance for a Risk-based Approach Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf

FATF (2016), *FATF Guidance on Correspondent Banking Services,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

FATF (2019*), FATF Terrorist Financing Risk Assessment Guidance*, FATF, Paris, www.fatf-gafi.org/publications//methodsandtrends/documents/Terrorist-Financing-Risk-Assessment-Guidance.html

FATF (2019), *FATF Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

FATF (2021), *FATF Risk-based Supervision Guidance*, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/Guidance-Risk-Based-Supervision.pdf

Other Reference Materials on PF Risk Assessments

FATF Members

Portugal (2019), Portugal AML/CFT Coordination Commission - National Risk Assessment Working Group, *National Risk Assessment Money Laundering Financing of Terrorism and Proliferation Financing Summary*, www.portalbcft.pt/sites/default/files/anexos/nra_2019_-_summary.pdf

United States (2018), United States Department of the Treasury, *National Proliferation Financing Risk Assessment*, https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf

FSRB Members

Cayman Islands (2020), *Cayman Islands Proliferation Financing Threat Assessment May 2020*, https://amlu.gov.ky/wp-content/uploads/2021/02/PF-Threat-Assessment-FinalVersion25June.docx

Gibraltar (2020), Gibraltar Financial Intelligence Unit and Gibraltar Financial Services Commission, *Counter Proliferation Financing: Guidance Notes*, www.gfiu.gov.gi/what-is-proliferation-financing, or https://www.gfiu.gov.gi/uploads/docs/X86Ru_CPF_Guidance_Notes_v1.1.pdf

Gibraltar (2020), *HM Government of Gibraltar 2020 National Risk Assessment for AML/CFT and PF*, https://www.gfiu.gov.gi/uploads/docs/Ihhoj_2020_NRA_Final.pdf

Latvia (2019), Financial Intelligence Unit of Latvia, *National Terrorism Financing and Proliferation Financing Risk Assessment Report 2017-2018*, www.fid.gov.lv/images/Downloads/useful/ENG_TF_PF_report_FINAL_updated_2019.pdf; or https://fid.gov.lv/uploads/files/Dokumenti/Riska zi%C5%86ojumi/Nacion%C4%81l%C4%81 NILLTPF risku nov%C4%93rt%C4%93juma zi%C5%86ojuma kopsavilkums.pdf

United Nations Security Council Panel of Experts Reports (UNSC PoE Reports)

United Nations (2014*), Final report of the Panel of Experts established pursuant to resolution 1929 (2010), S/2014/394*. https://undocs.org/S/2014/394

United Nations (2015), *Final report of the Panel of Experts established pursuant to resolution 1929 (2010), S/2015/401*. https://undocs.org/S/2015/401

United Nations (2017), *Final report of the Panel of Experts submitted pursuant to resolution 2276 (2016), S/2017/150*. www.undocs.org/S/2017/150

United Nations (2017), *Midterm report of the Panel of Experts submitted pursuant to resolution 2345 (2017), S/2017/742*. www.undocs.org/S/2017/742

United Nations (2018), *Final report of the Panel of Experts submitted pursuant to resolution 2345 (2017), S/2018/171*. www.undocs.org/S/2018/171

United Nations (2019*), Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019), S/2019/691*. https://undocs.org/S/2019/691

United Nations (2020), *Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019), S/2020/151*. https://undocs.org/S/2020/151

United Nations (2020), *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020), S/2020/840*. https://undocs.org/S/2020/840

Remarks: Citation of external documents does not imply their endorsement by the FATF.

FATF

www.fatf-gafi.org

June 2021

GUIDANCE ON PROLIFERATION FINANCING RISK ASSESSMENT AND MITIGATION

In October 2020, the FATF revised its Standards (R.1 and INR.1) to require countries, financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess, understand and mitigate their proliferation financing risks.

This guidance will help countries, financial institutions, DNFBPs and VASPs effectively implement the new mandatory FATF requirements. It explains how both public and private sectors should conduct risk assessments in the context of proliferation financing, and how they can mitigate the risks they identify.