Draft Guidance on proliferation financing risk assessment and mitigation (for public consultation)

Table of contents

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], financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess, understand and mitigate their proliferation financing risks. 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.[2]

2. 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[3] could implement the new requirements to assess and mitigate proliferation financing risks given the rules-based nature of the targeted financial sanctions under Recommendation 7.

3. 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 financial institutions and DNFBPs, failure on the part of financial institutions and DNFBPs 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);

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

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

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

[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 the implementation of 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] All references to "private sector entities", "private sector(s)" or "private sector firms" apply equally to financial institutions and DNFBPs.

[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.

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.

5. Recommendation 1 requires countries, financial institutions and DNFBPs 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 DPRK and Iran, requires countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of (a) any person or entity designated by the United Nations (UN), (b) persons and entities acting on their behalf or at their direction, (c) those owned or controlled by them.

6. This Guidance is intended to assist countries and private sector entities implement 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 Iran or DPRK designated entities), or activity-based prohibitions (which apply to Iran and DPRK 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 may assist countries and private sector entities to implement their R.1 obligations more efficiently and IO.11 more effectively, particularly by avoiding 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 financial institutions and DNFBPs with respect to Recommendation 7 and to combating money laundering and terrorist financing (ML/TF) set out in Recommendations 9 to 23.

7. 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, financial institutions, and DNFBPs 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.

8. The FATF Standards provide flexibility to countries 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. As risk profiles can change over time, such exemptions should be monitored. Nevertheless, full application of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

9. 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, financial institutions and DNFBPs.

10. 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 is 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

11. The Guidance is aimed at the following audience:

a. Countries and their competent authorities, including supervisors;

b. Financial institutions and DNFBPs.

12. 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.

13. The FATF adopted the present Guidance in [June] 2021 (*Remarks: planned project complete date included here as placeholder*).

Box 1. Question for consultation:

Does the introduction section above provide sufficient clarity in distinguishing the mandatory requirements of the updated FATF Standards on proliferation financing risk assessment and mitigation, and additional measures that may support the implementation of these new requirements?

Section 1: Assessment of proliferation financing risks

Introduction

14. 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 targeted financial sanctions (TFS) related to proliferation and its financing is one of the measures that contributes to a stronger counter proliferation financing (CPF) regime.

15. 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

[5] As included in the operative paragraphs 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.

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, financial institutions and DNFBPs to identify, assess, and understand the proliferation financing risks for the country and respective private sectors, 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]

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

17. 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. 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 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.

Box 2. Question for consultation:

Does the section above provide sufficient clarity in distinguishing the mandatory requirements of the updated FATF Standards on proliferation financing risk assessment and mitigation, and additional measures that may support the implementation of these new requirements?

[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.

[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 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 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 as required in the revised Recommendation 1, as well as the implementation of Recommendation 7 and Immediate Outcome 11.

Key Concepts relevant to Assessing and Understanding Proliferation Financing Risks

18. Similar to an ML/TF risk assessment, countries and private sectors 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

19. A **proliferation financing risk**, similar to a 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.

20. Another concept relevant for any risk assessment process is the understanding of **inherent risk** and **residual risk**, and applying those concepts specifically to PF risks, in the same 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 is 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 or WMD-related goods of the country, and trade pattern 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 suggests that control measures are inadequate and that a country or a private sector firm should take remedial action to address that risk.

Threat, Vulnerability, and Consequence

21. 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 with the potential to cause harm by evading, breaching or exploiting 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 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 beneficial ownerships for entities incorporated under its laws. 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. For example, a client base that consists of small trading firms located in well-known jurisdictions of diversion concern.

c. **Consequence** refers to the outcome where funds or assets are made available to designated persons and entities, to allow them 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. The consequence of proliferation financing, i.e. 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

22. 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 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. The risk assessment should be comprehensive enough to inform national counter proliferation financing strategies, and to assist in the effective implementation of risk-based measures. 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 the exercise is to ensure full implementation of PF-TFS requirements under relevant UNSCRs, effectively preventing the breach, non-implementation, or evasion of PF-related TFS. 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.

23. The FATF Standards provide flexibility in how countries and private sectors assess their PF risks and do not prescribe a particular risk assessment methodology. Nevertheless, as

[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.

the risk assessment process involves a number of agencies and stakeholders, and often stretches over a period of time, it would 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 *2019 FATF TFRA Guidance* in great detail. This section will focus on salient issues distinctive to the PF risk assessment process.[9]

Preliminary Scoping

24. To date, 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.

25. Given the limited literature on typologies of the breach, non-implementation or evasion of PF-TFS, conducting a **contextual analysis** as part of scoping would 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, other typologies common to TFS breaching, circumvention or evasion, and recent case examples and 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 also include a mapping of the UNSCR PF-TFS obligations[13] applicable to financial institutions and DNFBPs 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.

[9] Countries and private sectors 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 assessment as of the publication of this Guidance. They are Cayman Islands, Gibraltar, Latvia and the United States.

[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.

[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.

Planning and Organisation

26. 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 should 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, MVTS institutions, insurance companies, trust and company service providers, lawyers, and trading companies. 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 regulated entities where appropriate. For example, through closed-door briefings to discuss outcomes of the assessment.[15] 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[16], as well as developing a secured platform to allow ongoing engagement, consultations, and information sharing with regulated entities to the extent possible. The publication and sharing of such information will promote the understanding of PF risks and compliance with CPF requirements.

Identification

a) Threats

27. A good foundation of the identification process is to begin by **compiling a list of major known or suspected threats**; key sectors, products, or services that have been exploited; and the primary reasons why designated persons and entities are not deprived of their assets or identified. This is especially useful as UNSCR PF-TFS requirements focus not only on the designated persons and entities, but also persons and entities acting on their behalf.

28. While the **methodology** of identifying PF threats is similar to that of ML/TF[17], 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. the DPRK and Iran) and the international networks they have created to disguise their activities; and can also be indirectly

[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] 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.

[16] Risk assessments with classified components may be redacted or summarised for dissemination to regulated entities, and that further adaptation may need to be made for such assessments to be made available for broader, public consumption.

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

related to designated persons and entities[18]. As a result, the financing needs and methods of designated persons and entities may not necessarily 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 the trade in natural resources in contravention of relevant UNSCRs.[19] As for illegitimate activities, possible examples may include smuggling of cash[20], gold, and other high-value goods[21], cyberattacks[22], drugs trafficking[23], arms export, sand, etc.[24] 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.

29. Countries and the private sector should note that different countries and private sector firms would have 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[25], and to draw on available information sources relating to domestic, regional, and international proliferation financing threats.

[18] 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.

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

[20] UNSCR 1718 PoE Report.

[21] UNSCR 1718 PoE Report provides example, amongst others, sale of luxury yachts.

[22] 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.

[23] UNSCR 1718 PoE Report.

[24] UNSCR 1718 PoE Report.

[25] 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 no or very few known or suspected breaches, 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 for proliferation financing purposes 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. PoE carrying out the mandate specified in UNSCR 1718 (2006) and UNSCR 1874 (2009)) 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 62-64). 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).

30. **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. [26] 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 would provide additional

[26] 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).

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. the 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 can 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 information collected during the on boarding and ongoing due diligence (particularly the beneficial ownership of legal persons and arrangements), and transaction records involving the sale of dual-use or controlled goods would be relevant. Another important source could be threat analysis reports, national 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.

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

Below is an updated list of indicators based on the information contained in the *2018 FATF Guidance on Counter Proliferation Financing*.

A risk indicator demonstrates or suggests the likelihood of the occurrence of unusual or suspicious activity. The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of proliferation financing, nor will the 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 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, including banks and money value transfer services; designated non-financial businesses and professions; and small and mid-size businesses and large conglomerates. Within the private sector, these indicators are intended to be used by personnel responsible for compliance, transaction 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 engagement with law enforcement authorities or financial intelligence units. 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.

- 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 as a result of negative news;
    - During subsequent stages of due diligence, a customer, particularly a trade entity, its owners or senior managers, appear in negative news, e.g. past money laundering 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. The risk assessment process may include an identification of countries of proliferation or diversion concern to assist the private sector;
    - The customer is a person dealing with 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 potentially proliferation-sensitive or export-controlled items.

- 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.the DPRK and Iran);
  - Account holders conduct transactions that involve items controlled under multilateral WMD export control regimes or national control regimes;
  - Accounts or transactions involve possible 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 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

  Countries and private sector entities may wish to note that 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) OP12 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 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;
  - 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;
  - 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

  Countries and private sector entities may wish to note that DPRK PF-TFS, i.e. UNSCR 2087 (2013) OP 5(a), UNSCR 2094 (2013) OP 8, UNSCR 2270 (2016) OP 10, UNSCR 2270 (2016), 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.

  - A shipment is routed through a country with weak export control laws or weak enforcement of export control laws;

- Prior to account approval, customer requests letter of credit for trade transaction for shipment of proliferation-sensitive or dual-use goods;
- 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* and UNSC PoE Reports

b) Vulnerabilities

31. 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.

32. **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.

33. 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.

34. 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 located or a private sector firm operating 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

35. **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.

36. 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 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).[27] 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. 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: providing designated persons and entities the means to deliver components and materials for use in WMD or their delivery systems. These same actors also exploit the maritime sector 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.

[27] "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 PF-TFS (i.e. UNSCR 2270 (2016) OP 16) notes that the DPRK frequently uses front companies, shell companies, joint ventures and complex, opaque ownership structures for the purpose of violating measures imposed in relevant UNSCRs, and direct 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 (USD-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.

Remarks: See Section 2 for guidance on risk mitigation measures

Source: UNSCR 1718 PoE Report (S/2019/691; S/2020/151; S/2020/840)

37. 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.

38. **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 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 also allow the processing of wire transfers, international trade settlements, remittances, and cross-border payments. As identified in various UNSCR 1718 PoE Reports since 2017, 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 little 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 type 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 finance are 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[28], 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 attacks 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 and counterparties 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*

39. **Identifying customer and transaction vulnerabilities** are crucial for risk assessments conducted by a financial institution or a DNFBP. As a starting point, considerations should include 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 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.

40. Additional **information sources for a risk assessment** may include known domestic or international typologies[29], 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 non-implementation 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 customer due diligence processes, and transaction monitoring, 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

41. Risk can be considered as a function of threat, vulnerability, and consequence. At this stage, countries, financial institutions and DNFBPs 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.

42. 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 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.

Evaluation and follow-up

43. As a result of risk analysis, PF risks are often classified as 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 private sector firms.

44. 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

[28] 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.

[29] 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.

the assessment as appropriate to promote a broader understanding of the risk of PF-TFS evasion. As for the **private sector**, financial institutions and DNFBPs should consider adapting/calibrating/enhancing their policies, controls, and procedures to effectively manage and mitigate the identified risks. Financial institutions and DNFBPs may also review and make reference to suspected activity of the breach, non-implementation of evasion of PF-TFS[30] 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

45. Assessment of proliferation financing risks requires co-operation between public and private sectors.[31] Similar to the implementation of TFS, effective sharing of information and a co-ordinated approach in communicating with the private sectors are fundamental when conducting a risk assessment. The public sector authorities may have information on suspected proliferation financing sanctions evasion, which would be essential to the private sectors in terms of identifying, assessing, and understanding their risks. The information related to proliferation financing sanctions evasion activities may be 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 sectors. 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. On the other hand, the private sectors may hold vital information for both public and other private sectors 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).

46. 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

47. 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

[30] The FATF Standards do not require filing of PF-TFS related STR. However, if a jurisdiction requires STR filing in relation to the breach, non-implementation, or evasion of PF-TFS within the jurisdiction, and corresponding information is available, financial institutions and DNFBPs may also consider making reference of such available information.

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

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.

48. 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 and DNFBPs to take commensurate measures to manage and mitigate these risks. While countries will not be assessed on such steps as part of the Mutual Evaluation process, 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 sectors. 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 2: Mitigation of proliferation financing risks

49. The FATF Standards require countries, financial institutions and DNFBPs 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.

50. 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.

51. 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.

52. This section highlights specific measures that countries, financial institutions and DNFBPs 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.

53. Financial institutions and DNFPBs 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 financial exclusion risk, leading to denial of access to financial services for those who need it.

Risk mitigation measures by countries

54. 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.

55. Countries should allow financial institutions and DNFBPs 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.

Foundational elements of proliferation financing risk mitigation

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

a. **Conduct a Risk Assessment:** Financial institutions and DNFBPs 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 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.

b. **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).

c. **Communication of sanctions:** In line with Recommendation 7, countries should have effective mechanisms to ensure that designations are notified to all relevant parties, including financial institutions and DNFBPs, 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 and DNFBPs from dealing with the designated persons and entities during the time changes are being transposed to the domestic frameworks following the UN designations.

d. **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 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.

e. **Compliance monitoring and enforcement** is key to ensure sustained

compliance. Financial institutions and DNFBPs should be subject to 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. 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.

f. **Regular and in-depth training in the areas of targeted financial sanctions obligations and risks** for supervisors, custom and export controls, financial intelligence, regulatory authorities and other agencies involved in counter proliferation financing as well as financial institutions and DNFBPs can help build capacity and lead to better overall compliance with the TFS regime.

Mitigating specific sanctions evasion risks

57. **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.

58. 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 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.

59. **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 a network of key 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, 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 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.

60. **Outreach and points of contact enable private sectors to contact governments when they have concerns or need guidance.** As relevant and in accordance with the institutional framework, countries could conduct outreach to financial institutions and DNFBPs to explain key elements of their targeted financial sanctions programmes, including the action required if financial institutions and DNFBPs find a match against designated entities or persons. Where appropriate, financial institutions and DNFBPs should be able to access general 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.

61. **Specific guidance on preventing the evasion of sanctions and feedback:** One of the key challenges to effectively implementing targeted financial sanctions is ensuring that financial institutions and DNFBPs are adequately implementing Customer Due Dilligence (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.[32] All countries should comply fully with the FATF Recommendations relevant to ensuring the transparency of beneficial ownership of legal persons and legal arrangements.

62. **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) to prevent and mitigate the risk of evasion of targeted financial sanctions- such directives can 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 and DNFBPs

63. Financial institutions and DNFBPs are at the front lines of combating proliferation financing. Countries should ensure that financial institutions and DNFBPs take steps to identify circumstances in which customers and transactions may present proliferation financing risks, and ensure that their CPF 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 and DNFBPs.

64. Financial institutions and DNFBPs 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 national legislation. The nature of risk mitigation measures will depend on the source 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;

[32] See UNSCR 1718 PoEMay 2020 Report (Section IV).

d. Regular controls for effectiveness of procedures to conduct sanctions screening; and
e. Leveraging the existing compliance programmes (including internal controls) to identify sanctions evasion.

Risk mitigation in case of low risk

65. Low risk financial institutions and DNFBPs, such as those, which are small and serving predominantly locally-based and low risk customers, may not be expected to devote a significant amount of time and resources to risk mitigation. It may 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 current AML/CFT measures and combining them with sanctions screening to mitigate their risks.

66. The FATF Standards provide flexibility to countries 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. As risk profiles can change over time, such exemptions should be monitored. 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

67. 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 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.

68. The FATF Standards require the implementation of targeted financial sanctions without delay. Where the domestic regulatory framework allows it, financial institutions and DNFBPs could incorporate changes in UN designations into their monitoring and surveillance system without waiting for national transposition or communication.

69. Training for staff, in particular for those responsible for onboarding customers and maintaining customer relationships, monitoring 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.

Mitigating the risks of an evasion of sanctions

70. 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 and DNFBPs 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 or DNFBP does not understand the risks of potential sanctions evasion schemes and how to implement tailored, risk-based measures to mitigate those risks.

71. Financial institutions and DNFBPs 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, into their risk management practices and procedures to prevent the evasion of sanctions by illicit players. These practices and procedures should be periodically reviewed to ensure they remain relevant and up-to-date with current trends.

72. Investment in technology and advanced software, capable of machine learning and artificial intelligence to conduct analysis may help strengthen the compliance practices of financial institutions and DNFBPs that are 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, which would be difficult to establish otherwise. As designated entities and individuals are increasingly using advanced deception techniques to hide their true identities and conceal the beneficial owners, financial institutions and DNFBPs should be vigilant to such risks and stay ahead of the curve.

Enhanced customer due diligence

73. Effective implementation of customer due diligence measures can help financial institutions and DNFBPs 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 and DNFBPs could find that screening against list of designated entities is insufficient to properly manage the risk of breach, non-implementation of TFS related to proliferation or its financing. Some financial institutions and DNFBPs have adapted their existing CDD measures and monitoring of transactions to enable the detection of potential violations of TFS including sanctions evasion. Financial institutions and DNFBPs should consider using additional Proliferation financing - specific risk indicators to the criteria used for customer onboarding and monitoring ongoing customer relationships, in order to effectively defend against such risks.

74. The nature of business of financial institutions and DNFBPs and their services should determine the scope of internal controls, including CDD measures, suitable for mitigating the risk of evasion of sanctions. Financial institutions and DNFBPs 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 regularly 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[33]

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

76. 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 of 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 FATF Guidance on correspondent banking services.[34]

Shell and front companies

77. 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.

78. 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. Where appropriate, financial institutions should supplement the reliance on list-based screening by additional due diligence measures to mitigate the risk of potential sanctions evasion. Financial institutions and DNFBPs should understand the nature of their customer's business and identify and verify the customer's authorised signatories and beneficial owners 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.

79. 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. 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

[33] 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.

[34] See paragraph 29 of the FATF Guidance on Correspondent Banking Services.

of their customers' business and ownership and control structures, in accordance with national legislation.

Section 3: Supervision of proliferation financing risk assessment and mitigation[35]

80. This section provides general guidance on how proliferation financing risk assessment and mitigation by financial institutions and DNFBPs should be supervised or monitored by supervisors and self-regulatory bodies (SRBs). As noted in INR.1, supervisors can assess the proliferation financing risk assessments created by financial institutions as part of their pre-existing sanctions compliance or financial crimes compliance programme. It need not obligate financial institutions or DNFBPs to do a separate risk assessment, or retain compliance staff specifically for proliferation financing risk.

81. The FATF has developed a separate risk-based Guidance[36] to clarify and explain how supervisors should apply a risk-based approach to their supervision and/or monitoring of financial institutions and DNFBPs 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. For Financial Institutions or DNFBPs who are assessed as higher risk for proliferation financing, supervisors should subject them to closer supervision, such as more frequent and/or more comprehensive examination or inspection;
c. Supervisors should keep the risk assessment process dynamic, by leveraging available information and data from both internal and external sources[37], as part of their ongoing supervision and monitoring of entities;
d. Supervisors may note that proliferation financing risks may be distributed differently from ML/TF risks between and within supervised institutions. Adequately supervising the implementation of proliferation financing 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;
e. Supervisors should take steps to ensure that their supervised institutions understand their proliferation financing risks and apply commensurate risk mitigation measures;
f. 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;

[35] 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.

[36] To be added, following the publication of the risk-based supervision Guidance.

[37] 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 and DNFBPs 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.

g. 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);
h. Supervisors should adopt an approach for determining the intensity, type and frequency of off-site and on-site supervision;
i. 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;
j. Supervisors should focus on the effectiveness of internal controls, targeted financial sanctions screening processes and customer onboarding processes and transaction monitoring 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;
k. Supervisors should focus on supervised institutions' identification and management of false positives during screening;
l. Supervisors should focus on supervised institutions' inability to identify designated persons and entities, either due to the failure of automated sanctions screening software or other policies and procedures-related deficiencies, in the implementation of controls on persons and entities subject to targeted financial sanctions;
m. For DNFBP sectors in particular, supervisors 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, and referral to law enforcement. Proper enforcement can encourage a culture of compliance among supervised entities.

Annex: Bibliography and References[38]

FATF Publications on Proliferation Financing

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

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

FATF (2015), 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

Other Reference Materials on PF Risk Assessments

FATF Members

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,
https://www.gfiu.gov.gi/uploads/X86Ru_CPF_Guidance_Notes_v1.1.pdf

[38] Citation of external documents in this section does not imply their endorsement by the FATF.

Latvia (2019), Financial Intelligence Unit of Latvia, National Terrorism Financing and Proliferation Financing Risk Assessment Report 2017-2018, https://www.fid.gov.lv/images/Downloads/useful/ENG_TF_PF_report_FINAL_updated_2019.pdf

Other Organisations

{UNSC PoE Reports to be added here}