Royal United Services Institute
for Defence and Security Studies

Guide to Conducting a National Proliferation Financing Risk Assessment

Anagha Joshi, Emil Dall and Darya Dolzikova

Guide to Conducting a National Proliferation Financing Risk Assessment

Anagha Joshi, Emil Dall and Darya Dolzikova

May 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

May 2019.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Foreword

THIS GUIDE AIMS to assist governments in conducting a national risk assessment on proliferation financing (PF). It will help them to understand their exposure to PF risks, implement financial provisions of proliferation-related UN Security Council resolutions, and achieve effective implementation of the Financial Action Task Force's (FATF) recommendations on proliferation finance. It includes the RUSI Proliferation Financing Rapid Risk Assessment Tool, a spreadsheet-based tool developed by Anagha Joshi for conducting national risk assessments.

This risk assessment guide is a resource for jurisdictions to adapt to their own national priorities and processes. Not every aspect of the guide will be relevant to all jurisdictions. Jurisdictions that have not previously considered PF as a national financial crime risk distinct from money laundering or terrorist financing will be able to use the guide and the RUSI Proliferation Financing Rapid Risk Assessment Tool to carry out a risk assessment for the first time. Jurisdictions that have already conducted a national risk assessment on PF can make use of this narrative discussion to adapt their existing methodologies and frameworks.

This guide is a key resource used by RUSI staff to support jurisdictions in carrying out national risk assessments on PF. RUSI can provide further assistance on risk assessments through:

- Awareness-raising of PF risks among government and the private sector.
- Support for conducting a rapid risk assessment using RUSI tools.
- Support for developing or adapting a tailored risk-assessment methodology.
- Support and input during a risk-assessment process and development of a final report.

For further assistance or information, please contact:

Counter-Proliferation Finance, Royal United Services Institute
cpf@rusi.org

Introduction

COUNTERING THE FINANCIAL flows available to state and non-state proliferators plays an important role in wider efforts to counter the proliferation of weapons of mass destruction (WMD). Proliferators rely on access to the formal financial system to raise and gain access to funds, conduct payments and facilitate illicit activities. Because of the importance of countering these illicit financial flows, several United Nations Security Council Resolutions (UNSCRs) impose international legal obligations related to proliferation financing (PF): UNSCR 1540 on the non-proliferation of WMDs,[1] UNSCR 2231 on the implementation of the Joint Comprehensive Plan of Action related to Iran,[2] and the expanded requirements of UNSCRs related to North Korea.[3]

In 2012, the Financial Action Task Force (FATF), the global standard-setter on combating money laundering and terrorist financing, included standards on counter-proliferation financing in its mandate. While the FATF does not require jurisdictions to formally assess their PF risk, the latest FATF Guidance on Countering Proliferation Financing recognises that understanding PF risks can 'positively contribute to a jurisdiction's ability to prevent persons and entities involved in WMD proliferation from raising, moving and using funds'.[4] The need to understand risks associated with the proliferation of WMDs is also alluded to in several UNSCRs.[5]

A risk assessment is therefore a necessary precursor for an effective response to PF. It is unlikely that jurisdictions can meet international legal obligations and demonstrate their effective implementation of PF controls without fully understanding the risks they are attempting to detect and disrupt.

---

1. UN Security Council Resolution 1540, 28 April 2004, S/RES/1540.
2. UN Security Council Resolution 2231, 20 July 2015, S/RES/2231.
3. UN Security Council Resolution 1718, 14 October 2006, S/RES/1718; UN Security Council Resolution 1874, 12 June 2009, S/RES/1874; UN Security Council Resolution 2087, 22 January 2013, S/RES/2087; UN Security Council Resolution 2094, 7 March 2013, S/RES/2094; UN Security Council Resolution 2270, 2 March 2016, S/RES/2270; UN Security Council Resolution 2321, 30 November 2016, S/RES/2321; UN Security Council Resolution 2371, 5 August 2017, S/RES/2371; UN Security Council Resolution 2375, 11 September 2017, S/RES/2375; UN Security Council Resolution 2397, 22 December 2017, S/RES/2397.
4. Financial Action Task Force (FATF), 'FATF 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', February 2018, p. 4.
5. For example, UN Security Council Resolution 2325, 15 December 2016, S/RES/2325 calls upon states to consider the evolving nature of the risk of proliferation.

This guide offers jurisdictions specific information for conducting a PF national risk assessment. The aim of this guide is not to promulgate a new risk-assessment methodology; several international organisations, national governments and private sector bodies have already developed detailed risk assessment methodologies for money laundering and terrorist financing.[6] Instead, the RUSI Guide to Conducting a National Proliferation Financing Risk Assessment draws upon existing best practices from these methodologies and provides guidance on areas of divergence or further consideration in the context of PF. These include: relevant stakeholders and information sources that inform a PF risk assessment; defining PF as distinct from money laundering or terrorist financing; and identifying a range of PF threats, including those relating to sanctioned state actors.

Jurisdictions may choose to use the guidance to adapt existing money-laundering or terrorist-financing risk-assessment methodologies to develop a targeted and nuanced assessment of PF risks specifically. Alternatively, and recognising that some jurisdictions may not have existing risk-assessment methodologies suitable for adaptation, the guide is also accompanied by the RUSI Proliferation Financing Rapid Risk Assessment Tool, see Annex 6. This tool can be a useful starting point for better understanding a jurisdiction's PF risk exposure and for launching a more extensive PF risk assessment, although it is not a sufficient substitute for the latter. While this document should provide jurisdictions with the guidance necessary to develop a national PF risk-assessment framework and process, each jurisdiction's methodology should be adapted to take into account jurisdiction-specific considerations.

Chapter I sets out the argument for the need to conduct a national risk assessment on PF and tackles the difficult question of defining PF to determine the scope of the risk assessment. Chapter II articulates key principles of risks assessments, explaining certain terms and formulas, and discussing threats, vulnerabilities and consequences in a PF context. Chapter III considers the pros and cons of different assessment methodologies when applied in the context of PF and highlights other key considerations. Annexes 1 to 5 provide lists of threats, vulnerabilities and consequences as well as lists of stakeholders and sources of information for a PF risk assessment. For jurisdictions interested in using the RUSI Proliferation Financing Rapid Risk Assessment Tool, a multi-tab spreadsheet is available upon request by emailing cpf@rusi.org. Annex 6 contains instructions for how to use the tool, as well as visual depictions of the tool.

6. For example, the World Bank Risk Assessment Methodology, 'Presentation at 20th OSCE Economic and Environmental Forum First Preparatory Meeting, Vienna, February 2012, Session III, AML/CTF National Risk Assessments'; International Monetary Fund (IMF), 'Annex 3: The Fund Staff's Approach to Conducting National Money Laundering or Financing of Terrorism Risk Assessment', in International Monetary Fund, 'Anti-Money Laundering and Combating the Financing of Terrorism (AML/CTF): Report on the Review of the Effectiveness Program', 11 May 2011, p. 63, <https://www.imf.org/external/np/pp/eng/2011/051111.pdf>, accessed 25 April 2019.

I. Understanding Proliferation Financing Risk

THE FATF RECOMMENDATIONS on money laundering (ML), terrorist financing (TF) and PF 'set an international standard, which jurisdictions should implement' in their own domestic laws and regulations.[7] In 2012, the FATF included counter-proliferation financing in its mandate through two recommendations for jurisdictions: Recommendation 2 on national cooperation and coordination on financial crime risks, including ML, TF and PF; and Recommendation 7 on targeted financial sanctions against specific proliferating actors designated by UNSCRs.[8]

The narrow focus on implementing targeted financial sanctions against designated individuals and entities in Recommendation 7, not commensurate with the breadth of UN requirements today. In January 2016, most UN-targeted financial sanctions against Iran were removed in accordance with UNSCR 2231,[9] leaving the Recommendations, in effect, to cover mostly North Korean-designated entities and individuals. Meanwhile, international sanctions against North Korea go far beyond a list-based approach and now include a range of activity-based prohibitions (see Table 1) that require an understanding of risk in order to apply enhanced controls.

The FATF's other Recommendations – which cover a range of preventive measures around customer due diligence and reporting of suspicious transactions, transparency and beneficial ownership provisions, effective supervision and monitoring of the private sector, and international cooperation with other jurisdictions on financial crime risks – do not specifically extend to cover PF.

The FATF, however, not only measures how jurisdictions implement technical requirements of the Recommendations, but also the effective implementation of those Recommendations. Immediate Outcome 11 (IO.11) requires jurisdictions to 'develop and implement policies and activities to combat the financing of proliferation of WMD',[10] in addition to implementing targeted financial sanctions without delay.[11] This too requires an appreciation of PF risks. The FATF, in its 2018 Guidance on Counter Proliferation Financing, has since stated that the risk-based measures contained in other Recommendations 'can assist effectiveness under IO.11'.[12]

7. FATF, 'The FATF Recommendations', updated October 2018, p. 6.
8. *Ibid*.
9. UN Security Council Resolution 2231, 20 July 2015, S/RES/2231.
10. Certain elements of IO.10 on national coordination mechanisms are also relevant to countering proliferation financing.
11. FATF, 'Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', updated February 2019, p. 123.
12. FATF, 'FATF Guidance on Counter Proliferation Financing', p. 6.

In 2018, the incoming FATF president stated that '[PF] measures lag significantly behind those directed at countering money laundering and terrorist financing' and that the FATF should 'consider new ways to address the full range of illicit proliferation-related activity that is only partially addressed by the current targeted financial sanctions regime'.[13]

One of the most significant gaps is in understanding and assessing national PF risk. FATF Recommendation 1, which requires jurisdictions to assess risks and apply a risk-based approach to countering other financial crime,[14] does not extend to PF. As a result, many jurisdictions do not conduct such a risk assessment and do not adequately understand their exposure to PF risks, or proliferation risks more generally. Knowledge of how proliferation activities might manifest themselves within a country's borders will help in understanding how underlying finance supports that activity.

Private sector implementation, which is informed by government guidance, also lacks risk-based insight and jurisdictions struggle to prevent persons and entities involved in proliferation of WMDs from raising, moving and using funds.

While there is a growing focus on assessing PF risks, there are currently very limited resources to assist jurisdictions in undertaking such risk assessments in a meaningful way.[15] More recently, PF has been included in some jurisdictions' national risk assessments, including the US.[16] However, due to the size and operation of the US financial system, where most exposure to PF comes from correspondent banking relationships, other jurisdictions' risk assessments will differ significantly. Many assessments also lack an appreciation of the underlying proliferation risk, and generally rely on the same risk methodologies as ML and TF assessments, without adapting to a PF context. A common approach has been to consider PF together with TF, which excludes a range of PF-specific activity.[17] This guide addresses this gap.

---

13. Marshall Billingslea, 'Objectives for FATF-XXX (2018–2019): Paper by the Incoming President', FATF, 2018, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/objectives-2018-2019.html>, accessed 18 February 2019.
14. FATF, 'The FATF Recommendations'.
15. A November 2018 report published by the Center for a New American Security focuses on conducting PF risk assessments in financial institutions. See Jonathan Brewer, 'The Financing of WMD Proliferation: Conducting Risk Assessments', Center for a New American Security (CNAS), 2018. The FATF Guidance on Counter Proliferation Financing references the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessments as a general guide for conducting risk assessments.
16. US Department of the Treasury, 'National Proliferation Financing Risk Assessment 2018', <https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf>, accessed 29 March 2019.
17. See, for example, Financial Intelligence Unit, Government of Vanuatu, 'Vanuatu National Risk Assessment: Money Laundering Through the Offshore Sector and Terrorist Financing', 2017, p. 34, <http://fiu.gov.vu/publications>, accessed 29 March 2019. PF is briefly considered under the topic of terrorist financing.

What is Proliferation Financing?

The nature of PF is multifaceted: it is at once a financial crime risk, a sanctions risk, and a risk to international counter-proliferation measures. Designated entities and individuals evade sanctions and fund their WMD proliferation efforts by employing a complex network of front companies and diversion techniques borrowed from the world of money laundering. Whereas money laundering is a circular process deployed by criminals to conceal the illicit origin of the proceeds of crime, sanctions are about the individuals to whom funds are made available or the purposes for which they are being used. This is an important distinction, as it means that the funds involved in sanctions evasion are not the end goal in themselves, but are used to facilitate other illicit activities.

In this way, PF could be defined in a similar linear fashion to TF. The International Convention for the Suppression of the Financing of Terrorism criminalises providing or collecting funds 'with the intention that they should be used or in the knowledge that they are to be used' to carry out acts prohibited by counterterrorism conventions.[18] A report by the Center for a New American Security similarly describes PF as a linear three-stage process: (1) WMD programme fundraising through state budgets as well as commercial and illicit activities; (2) disguising the funds as they move through the international financial system; and (3) procuring materials and technology.[19]

Unlike ML or TF, both of which have generally accepted definitions in international conventions,[20] there is no agreed international definition of PF. In 2010, the FATF published a working definition of PF, which focused its scope on the financing of nuclear, chemical or biological weapons, their means of delivery and related materials.[21] As previously mentioned, the FATF's corresponding Recommendation focuses on specific proliferating actors in UNSCRs. However, the definition does not exclude non-state actors or other countries of nuclear proliferation concern – including Pakistan, India and Israel, which are not recognised nuclear powers under the Nuclear Non-Proliferation Treaty – or China, which is identified as a PF threat by the US.[22]

Much of the current understanding of PF has developed primarily – although not exclusively – in response to North Korea's WMD programme. Recent expansion of UN sanctions regimes against North Korea also means that what is potentially covered under the umbrella of PF is broader than the FATF definition, in terms of the types of activities covered. PF may not only be limited

18. 'International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in Resolution 54/109 of 9 December 1999', Article 2.
19. Jonathan Brewer, 'The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation', CNAS, January 2018, p. 5.
20. See 'International Convention for the Suppression of the Financing of Terrorism' and the 'United Nations Convention Against Transnational Organized Crime (UNTOC), Adopted by the General Assembly of the United Nations in Resolution 55/25 of 15 November 2000'.
21. FATF, 'Combating Proliferating Financing: A Status Report on Policy Development and Consultation', February 2010, p. 11.
22. US Department of the Treasury, 'National Proliferation Financing Risk Assessment 2018', p. 10.

to the financing of the procurement of WMD and missile components and technology, but also the financing, financial services and financial relationships that sustain North Korea's other sanctioned activities. However, as proliferation threats change in nature, or new proliferators are identified, international non-proliferation efforts will evolve in response, and the types of activities that fall under PF will adapt accordingly.

At the same time, it is useful to retain a definition of PF in its narrowest sense: in the case of Iran, PF relates to the financing of certain activities or certain actors, primarily related to ballistic missile activities, which are still sanctioned under UNSCR 2231. Additionally, UNSCR 1540 covers the financing of specific WMD goods and materials, to any actor (focusing on non-state actors), at any place and time. This guide addresses the threat of proliferation by non-state actors only as it relates to international non-proliferation obligations under UNSCR 1540, as other UNSCRs and international obligations aimed at countering terrorist financing are not included in the international non-proliferation regime. If the international community were to conclude that there is sufficient threat of terrorist funds being diverted to the proliferation of WMD, certain terrorist groups may be folded into the international non-proliferation regime, and related activities would therefore come under the umbrella of PF.

PF in its most narrow sense – as outlined by UNSCR 1540 and the FATF definition – will remain constant, as it focuses strictly on financial services and activities directly supporting trade in proliferation-sensitive materials and technology, by any actor. This forms the foundation and the starting point for any understanding of PF.

Box 1: FATF Definition of Proliferation Financing

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

Source: FATF, 'Combating Proliferation Financing', p. 5.

To conduct a national risk assessment on PF, jurisdictions therefore first need to determine the overall scope of the risk assessment, and a definition is helpful for that purpose. The lack of an international definition of PF means that many jurisdictions do not have a definition of PF in domestic law. A related challenge is that a single definition of PF may not be enough to cover the full range of measures that may be encapsulated by that term. While a national risk assessment on ML or TF can be easily premised on the criminal offences of these activities, that is not always the case with PF.

It is useful to break down the categories that constitute PF and understand the international legal obligations from which they arise. As a starting point, UNSCR 1540 provides some guidance as to what may be considered PF. The resolution is not specific to any state or any specific group of actors but prohibits the proliferation of WMDs to and by any non-state actors. Its operative paragraph 2 requires jurisdictions to prohibit specified activities related to the proliferation of WMDs by non-state actors, including by prohibiting the financing of these activities. The Resolution does not prescribe criminalisation of PF and therefore jurisdictions could adopt laws that are civil, criminal or administrative in nature. Operative paragraph 3(d) of the resolution also requires jurisdictions to prohibit the provision of funds and services (including financial services) for the export and trans-shipment of specified controlled goods through the deployment of civil or criminal measures.[23]

Based on the elements contained in UNSCR 1540, a basic definition of PF could be as outlined in Box 2.

23. UN Security Council Resolution 1540, 28 April 2004, S/RES/1540.

Box 2: Definition of Proliferation Financing from RUSI's Model Law on Proliferation Finance

(1) Proliferation financing is when a person:

(a) makes available an asset; or
(b) provides a financial service; or
(c) conducts a financial transaction; and

the person [knows that, or is reckless as to whether,] the asset, financial service or financial transaction is intended to, in whole or in part, facilitate an activity specified in Subsection (2) regardless of whether the specified activity occurs or is attempted.

(2) The specified activities are:

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of:
    (i) nuclear weapons; or
    (ii) chemical weapons; or
    (iii) biological weapons; or
    (iv) materials related to nuclear weapons, chemical weapons or biological weapons that are prescribed by Regulations; or
(b) the provision of technical training, advice, service, brokering or assistance related to any of the activities in Paragraph (a).

Nuclear, chemical and biological weapons are all defined terms in RUSI's model law and include their means of delivery. Financial transaction is defined in the model law and includes the physical transfer of an asset. Note that when the definition is applied in the context of domestic legislation, it should exclude lawful proliferation activity, for example, the activities of current nuclear states as defined under the Treaty on the Non-Proliferation of Nuclear Weapons. Note also that the mental elements of knowledge and recklessness are included in square brackets in the event that jurisdictions wish to convert the definition into a PF offence provision.

Source: Anagha Joshi, 'Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction Second Edition, Supplementary Material for Guidance Paper', RUSI, October 2018, Section 6B, p. 21.

In addition to UNSCR 1540, the UN maintains targeted financial sanctions against individuals and entities for involvement in WMD proliferation activities. Currently, that is largely in relation to Iran and North Korea sanctions requirements. Some may consider that assets and financial services provided to sanctioned individuals and entities constitutes proliferation financing.

Other proliferation-related UNSCRs regarding Iran and North Korea also contain a range of what may be classified as financial measures against certain activities that support proliferation

activity in those states. Some of these additional measures are not covered by the broad definition of PF in Boxes 1 and 2.[24]

The North Korea measures in particular are extensive and capture financing related to commodities and goods that are otherwise licit but are banned or restricted in so far as they relate to North Korea. The North Korea measures further capture financial measures that are aimed at curbing North Korea's proliferation activities, including the corporate and financial networks used by North Korea globally. Jurisdictions may consider these under the umbrella of PF, as any export revenues earned by North Korea, or any financial channels used for trade, can ultimately be either reinvested into the country's nuclear and missile programme, or used to benefit it in some way.[25] While this guide does not advocate for any particular definition of PF, it is important that jurisdictions consider the full breadth of UN-mandated sanctions measures when deciding on the scope of a PF risk assessment.

24. The RUSI Model Law on Proliferation Finance captures these additional measures in separate chapters on Iran and North Korea. UN Security Council Resolution 1718, 14 October 2006, S/RES/1718; UN Security Council Resolution 1874, 12 June 2009 S/RES/1874; UN Security Council Resolution 2087, 22 January 2013, S/RES/2087; UN Security Council Resolution 2094, 7 March 2013, S/RES/2094; UN Security Council Resolution 2270, 2 March 2016, S/RES/2270; UN Security Council Resolution 2321, 30 November 2016, S/RES/2321; UN Security Council Resolution 2371, 5 August 2017, S/RES/2371; UN Security Council Resolution 2375, 11 September 2017, S/RES/2375; UN Security Council Resolution 2397, 22 December 2017, S/RES/2397; UN Security Council Resolution 2231, 20 July 2015, S/RES/2231.
25. In September 2017, US Under Secretary of Treasury for Terrorism and Financial Intelligence, Sigal Mandelker, stated that 'any revenue that North Korea generates can be used to support, directly or indirectly, its weapons development programs'. See US Department of the Treasury, 'Testimony of Sigal Mandelker Under Secretary, Terrorism and Financial Intelligence U.S. Department of the Treasury Senate Banking Committee Thursday, September 28, 2017', press release, 28 September 2017, <https://www.treasury.gov/press-center/press-releases/Pages/sm0168.aspx>, accessed 29 March 2019.

Box 3: Summary of Items Under Import, Export or Sale Restrictions in Relation to North Korea

- Aviation fuel, rocket fuel
- Coal
- Condensates and natural gas liquids
- Copper, nickel, silver
- Earth, stone, wood
- Electrical equipment
- Food and agricultural products
- Helicopters
- Industrial machinery
- Iron, steel
- Lead, ore
- Luxury goods*
- Petroleum, crude oil
- Rare earth minerals
- Seafood, fishing rights
- Statues
- Textiles, fabrics
- Transport vehicles
- Vessels.

* Despite primarily being a punitive measure aimed at restricting the import of luxury goods into North Korea (unlike the rest of the goods on this list, whose PF value lies in the profits North Korea makes from their export), luxury goods have been included on this list due to their potential resale value.

Source: UN Security Council Resolution 1718, 14 October 2006, S/RES/1718; UN Security Council Resolution 1874, 12 June 2009, S/RES/1874; UN Security Council Resolution 2087, 22 January 2013, S/RES/2087; UN Security Council Resolution 2094, 7 March 2013, S/RES/2094; UN Security Council Resolution 2270, 2 March 2016, S/RES/2270; UN Security Council Resolution 2321, 30 November 2016, S/RES/2321; UN Security Council Resolution 2371, 5 August 2017, S/RES/2371; UN Security Council Resolution 2375, 11 September 2017, S/RES/2375; UN Security Council Resolution 2397, 22 December 2017, S/RES/2397.

Table 1: Additional Financial Measures to Curb North Korea's Proliferation Activities

Controls on Financial Institutions	Controls on Diplomats and Diplomatic Missions	Controls Around Vessels and Aircraft
Prohibit financial institutions from maintaining relationships, including correspondent banking relationships, with North Korean financial institutions.	Limit number of bank accounts of diplomats/consular staff and missions.	Prohibit leasing or chartering vessels, aircraft or crew services to/from North Korea.
Prohibit North Korean financial institutions from opening branches, subsidiaries in your jurisdiction.	Prohibit diplomatic agents from engaging in profit-making activities.	Prohibit owning, leasing, operating or insuring North Korean-flagged vessels.
	Prohibit use of real property for purposes that are not diplomatic.	Prohibit provision of insurance to vessels owned, controlled or operated by North Korea.
Prohibition on Financial Support for Trade with North Korea	**Prohibition on Bulk Transfer of Gold and Cash to North Korea**	**Controls on Joint Ventures and Cooperative Entities**
Prohibition on financial support for trade, including granting of export credits, guarantees or insurance.	Prohibition may be implemented through a combination of a cross-border cash and gold transportation regime and prohibition on physical transfer of these items to North Korean persons or entities.	Prohibit joint ventures or cooperative entities with North Korean persons and entities, including designated persons and entities.

Source: Table developed by authors based on UN Security Council Resolution 1718, 14 October 2006, S/RES/1718; UN Security Council Resolution 1874, 12 June 2009, S/RES/1874; UN Security Council Resolution 2087, 22 January 2013, S/RES/2087; UN Security Council Resolution 2094, 7 March 2013, S/RES/2094; UN Security Council Resolution 2270, 2 March 2016, S/RES/2270; UN Security Council Resolution 2321, 30 November 2016, S/RES/2321; UN Security Council Resolution 2371, 5 August 2017, S/RES/2371; UN Security Council Resolution 2375, 11 September 2017, S/RES/2375; UN Security Council Resolution 2397, 22 December 2017, S/RES/2397.

In addition to the above measures, UNSCRs related to North Korea also contain some particularly broad 'catch-all' provisions that require jurisdictions to identify other goods or activities that could contribute to North Korea's proliferation activities, including evasive tactics employed to circumvent UNSCR measures. For example, UNSCR 2094, operative paragraph 11 contains some of the broadest terms when it prohibits the provision of financial services and any financial or other assets or resources that could contribute to North Korea's nuclear or ballistic missile programme, and other activities prohibited by relevant UNSCRs related to North Korea or to the evasion of measures contained in such UNSCRs.[26]

26. UN Security Council Resolution 2094, 7 March 2013, S/RES/2094, p. 3. The RUSI Model Law on Proliferation Finance also captures these catch-all provisions in the specific chapter on North

It is therefore useful to define certain terms found within the basic definition of PF in the RUSI Model Law definition in Box 2 as broadly as possible, to allow the definition and its corresponding offence provision to also be used against some (but not all) aspects of the UNSCRs related to North Korea and Iran. First, in the RUSI Model Law, 'asset' is defined broadly to include funds, financial resources and economic resources, an interpretation which is likely to be broader than the concept of 'financing' and 'funds' contemplated by the authors of UNSCR 1540. Second, the definition of 'financial services' combines activities included in the FATF definitions of 'financial institutions' and 'Designated Non-Financial Businesses and Professions' (DNFBPs) and further expands on those activities through, for example, the coverage of maritime and cargo insurance.[27]

While these broad definitions are useful, they also highlight the potentially fine line between proliferation and what is considered PF. This may be further complicated when one considers conduct ancillary to proliferation, such as aiding, abetting and facilitating proliferation activities. Financial products and services related to trade in WMD-related materials, for example, could well be classified as the ancillary conduct of facilitating proliferation rather than financing proliferation; while the goods are being provided to North Korea, for example, the financial payment is not being made to North Korea.

Another example is the prohibition against providing insurance to a North Korean-flagged vessel used to transport materials related to nuclear weapons. Under the RUSI Model Law definition of PF, the provision of insurance would be considered PF since maritime insurance falls under the definition of a financial service and that service was facilitating the provision of material related to nuclear weapons. The issue arises particularly in the context of financial services directly related to the procurement of WMDs and their means of delivery as well as to export-controlled goods in relation to North Korea.

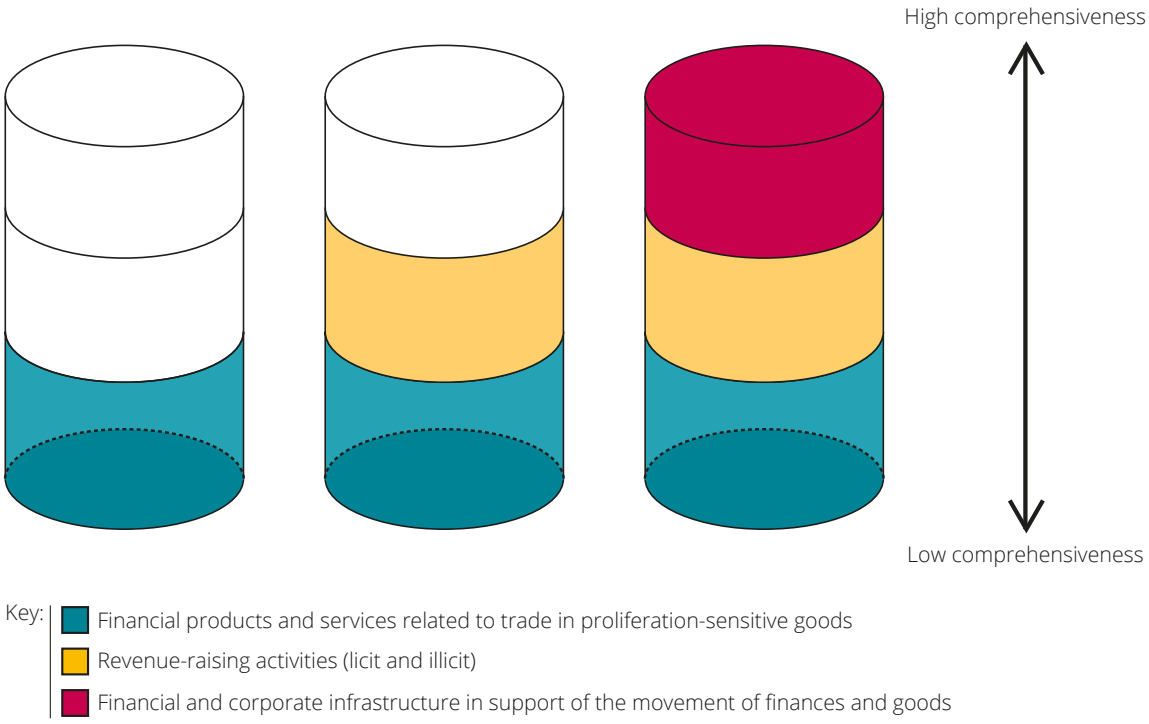
Three Categories of Proliferation Financing

For the purpose of this guide, the authors are less concerned about articulating a single definition of PF. Rather, they have created three categories of activities that may be considered PF and could be captured within the scope of a PF national risk assessment.

Korea (Chapter IV).

27. Joshi, 'Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction Second Edition, Supplementary Material for Guidance Paper', pp. 12, 15–16. A definition of financial services is not provided in UNSCRs or the FATF Recommendations. The RUSI definition of financial services captures the services included in the FATF definitions of financial institutions and DNFBPs, but it goes further to expand some elements of those definitions. For instance, maritime and cargo insurance products are captured by the RUSI definition of financial service since these types of products are particularly relevant in the PF context, as they play an important facilitating role in the movement of sanctioned goods.

Figure 1: Three Categories of Proliferation Financing



Source: The authors, 2019.

1. **Financial products and services directly related to trade in proliferation-sensitive goods.** The first category is the narrowest definition of PF. It encapsulates financial products and services associated with trade in goods that are directly usable or modifiable for use in the development of WMDs, their means of delivery and related materials. They also include financial products and services related to the import or export of goods as well as the transport of the goods: for example, trade finance, maritime or cargo insurance, and export guarantees. This category of activities is not limited to sanctioned states; it also captures financial products and services associated with the procurement of goods by non-state actors as prohibited by UNSCR 1540.

2. **Licit and illicit revenue-raising activities**. The second category encapsulates a broader range of activities that generate revenue to finance the procurement and development of WMDs, their means of delivery and related materials. It includes:

    - Activities which are considered illicit regardless of the actor, such as the smuggling of illicit goods (see Chapter II for a further discussion of illicit profit-generating activities). This therefore covers the activities of both sanctioned states and non-state actors. For example, terrorist groups can also

use illicit revenue-raising activities to finance the procurement of WMDs and their means of delivery.

- Activities which would normally be considered licit unless carried out by a proliferator who is specifically prohibited by the UN from engaging in these activities. For example, in the case of North Korea, the operation of restaurants, fisheries businesses, or construction companies would fall into this category. They also cover the purchase of licit goods that are otherwise import controlled with respect to North Korea since the sale of these goods forms part of North Korea's revenue-raising activities, as well as financial products and services directly associated with trade in licit goods that are otherwise controlled with respect to North Korea. Examples of such goods are listed in Box 1.

3. **Financial or corporate infrastructure that facilitates the first two categories**. The third category reflects the broadest definition of PF. It covers any kind of corporate or financial infrastructure that facilitates activities included in the above two categories, as well as any assets or financial services provided to individuals or entities subject to targeted financial sanctions.

   The corporate or financial infrastructure need therefore not have PF as its sole or predominant purpose and may also be unwittingly used for PF activities. This category includes the following types of corporate or financial activities:

   - The establishment of legal persons (particularly companies) and legal arrangements such as trust structures.
   - The establishment of joint business ventures.
   - The provision of banking and non-banking financial services, regardless of whether the entity in question is licensed to provide those services.
   - The provision of services by DNFBPs (such as lawyers, accountants or real-estate agents) that relate to real property.
   - Ledger-based payment services, such as *hawala*.[28]
   - Money or other value mules used to physically transport cash, gold or other valuable assets across borders, including through the use of diplomatic bags.

While the third category does not necessarily exclude non-state actors, it draws predominantly on sophisticated networks and methods used by sanctioned states, particularly North Korea.

When conducting a PF national risk assessment, jurisdictions should consider the three categories of PF described in this chapter. They should note that a single PF offence provision (as

28. *Hawala* is one of several terms used to describe a money-transfer mechanism that operates outside the financial sector. Such informal transfer service providers can arrange for the transfer or receipt of funds or equivalent value and arrange settlement through trade, cash or net settlement mechanisms over a period of time. See FATF, 'The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing', October 2013, p. 9.

defined in the RUSI Model Law or by FATF) is not sufficient to capture the full range of financial activities that support proliferation encapsulated in the three categories above. In addition, jurisdictions should note that the broader aspects of PF, particularly the third category, may be combated using non-criminal measures such as preventative measures imposed through regulatory controls. The RUSI Model Law captures these broader aspects of PF in additional chapters relating to Iran and North Korea.

To assist jurisdictions in defining PF for the purpose of determining the scope of their risk assessment, Annex 3 of this paper lists PF threats corresponding to the three identified categories of activities. It is recommended that jurisdictions are clear about the PF activities that the risk assessment will cover before embarking on a risk-assessment exercise.

Proliferation Pathways

Before jurisdictions proceed with identifying PF threats relevant to their jurisdiction, it is important that they are complemented and underpinned by a robust understanding of proliferation patterns generally.

Proliferators use an evolving set of tactics to evade sanctions and move goods and materials around the world, and therefore seek to exploit an ever-changing range of jurisdictions through which to route these activities. The procurement of materials for a WMD programme is not confined to one jurisdiction but involves a range of intermediary actors and trans-shipment points. Furthermore, jurisdiction risk is not only created through direct involvement with obvious parts of the proliferation supply chain, such as the procurement of dual-use goods and technologies, but also indirectly through exposure to front company networks, trans-shipment or shipping services, or – as this guide focuses on – financial access points. Because the financing of proliferation ultimately relates to the proliferator's wider underlying activity, a robust understanding of proliferation pathways is at the heart of identifying PF threats.

Jurisdictions should therefore consider where they sit within these 'proliferation pathways'. For example, jurisdictions with a manufacturing industry producing high-tech or dual-use goods will be the first link in the procurement process and will have exposure to risks emerging from: the presence of sensitive technological know-how and capabilities in national labs or research centres; the production and subsequent physical movement of goods; and the payment for those goods. Jurisdictions with high trade volumes or significant trade ports will face the risk of being trans-shipment points. Other jurisdictions may not have any direct exposure to the development, production or movement of goods but may still be key links in facilitating proliferation activities by hosting front companies, or by being the base for revenue-raising activities, which can ultimately be reinvested into a proliferation programme.

Jurisdictions will also need to consider that risk exposure to some proliferators may be higher than to others. Geographic proximity to proliferating countries and other social, economic, legal and institutional issues might make it possible for certain actors to prefer some jurisdictions over others. When identifying PF threats, as outlined in the next chapter, jurisdictions should

carefully consider their context vis-à-vis different proliferators and their activities, in order to understand the role their economy might play in PF activities.

Table 2 illustrates how three countries' geographical exposure to proliferation activities differs, and their corresponding exposure to PF.

Table 2: Countries' Exposure to Proliferation Activities

Country A	Country B	Country C
Geographical Exposure	**Geographical Exposure**	**Geographical Exposure**
Country A is close to Iran and is at risk of sensitive goods and materials being diverted.	Country B is not located near any major proliferator but has a sophisticated manufactuing base which could be exploited by proliferators.	Country C is not located near any major proliferator but has pockets of areas controlled by non-state actors who might seek to procure controlled goods.
Related Finance	**Related Finance**	**Related Finance**
Country A is not a financial hub but has local banks where funds from the proliferating state could be desposited.	Country B is a financial hub, and therefore provides correspondent banking services to banks, including those in Country A.	Country C has limited financial channels, and most cash is carried physically over the border.
	Country B hosts several front companies that facilitate transactions and trade on behalf of Iran.	

Source: The authors, 2019.

II. Identifying PF Threats, Vulnerabilities and Consequences

THE BASIC RISK-ASSESSMENT methodology used in this guide will be familiar to those who have previously completed a national risk assessment on ML or TF. However, there are also important components which distinguish PF from other types of financial crime. Therefore, a PF risk assessment can take inspiration from other risk-assessment methodologies, but will likely require some adaptation. This chapter outlines how to adapt ML or TF risk-assessment methodologies to the PF context. While there is no singular methodology for conducting a national risk assessment, for the purpose of this guide a baseline formula will be used, where risk is a function of the likelihood of events occurring and the consequences of those events; further, likelihood is the coexistence of threats and vulnerabilities.[29]

While each of these factors (threats, vulnerabilities and consequences) can be considered individually, addressing all three factors is necessary for undertaking a comprehensive risk assessment. These factors need to be considered in sequence – threats, then vulnerabilities, then consequences – as, for the purposes of this methodology, threats need to be identified so that vulnerabilities and consequences can be considered in relation to each identified threat.

Jurisdictions should consider their jurisdiction-specific contexts when evaluating the presence and importance of the suggested threats, vulnerabilities and consequences. The national risk-assessment process and accompanying tools detailed in this document are not intended to produce a national risk rating for each jurisdiction, nor do they aim to compare the risk ratings of various jurisdictions against each other. Instead, the guide provides guidelines for identifying threats in individual jurisdictions and assessing various vulnerabilities and consequences commensurate with each identified threat. The objective is to identify PF-related risks at national and sectoral levels and consider corresponding mitigating strategies so that resources and effort can be directed appropriately. The assessment of threats, vulnerabilities and consequences should be completed with this in mind.

29. IMF, 'Annex 3: The Fund Staff's Approach'.

Threats

The first of the factors, threats, includes people, entities, objects or activities that have the potential to cause the risk in question. An assessment of threats is therefore the starting point for assessing risk, as discussed further below.[30]

In the context of ML, threats are generally posed by the existence of predicate crimes. A predicate crime is any crime that generates criminal proceeds capable of being laundered. In the context of TF, threats are posed by the existence or influence of terrorist actors. Predicate crimes and criminal actors are also relevant in the context of PF. However, neither of these categories of threats adequately captures the complex nature of PF and the range of possible threats.

Chapter I considered a definition of PF and identified three categories of activities that may fall under it: (1) financial products and services directly related to trade in proliferation-sensitive goods; (2) revenue-raising activities (licit and illicit); and (3) financial and corporate infrastructure that facilitates the first two categories. The first category of activities is relevant to state and non-state proliferation actors, whereas the second two feature more prominently in relation to state proliferation actors, in particular North Korea.

PF typologies show that North Korea has engaged in illicit profit-generating crimes such as wildlife trafficking[31] and drugs trafficking,[32] small and non-nuclear arms trafficking,[33] cybercrime (including hacking of financial messaging systems, extortion, or theft of cryptocurrency assets),[34] labour exploitation (for example in the construction and food processing industries),[35] and smuggling of cash and high-value goods,[36] among others. This is similar to the concept

30. FATF, 'FATF Risk Assessment Guidance: National Money Laundering and Terrorist Financing Risk Assessment', February 2013, p. 7.
31. Rachel Nuwer, 'North Korean Diplomats Accused of Smuggling Ivory and Rhino Horn', *National Geographic*, 16 October 2017.
32. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2010/571, 5 November 2010, p. 10.
33. See Andrea Berger, *Target Markets: North Korea's Military Customers in the Sanctions Era*, RUSI Whitehall Paper 84 (London: Taylor and Francis, 2015).
34. Jim Finkle, 'Cyber Security Firm: More Evidence North Korea Linked to Bangladesh Heist', *Reuters*, 3 April 2017; *Reuters*, 'South Korean Intelligence Says N. Korean Hackers Possibly Behind Coincheck Heist – Sources', 5 February 2018; Juan Andres Guerrero-Saade and Priscilla Moriuchi, 'North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign', *Recorded Future*, 16 January 2018, <https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/>, accessed 18 February 2019.
35. For more on the role of North Korean foreign labour in financing North Korea's proliferation activities, see Jason Arterburn, 'Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System', *Center for Advanced Defence Studies*, 2 August 2018.
36. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017, pp. 72, 78.

of predicate crimes for ML, although laundering of proceeds may or may not occur. Profit-generating crimes for PF may also be a greater feature for some jurisdictions and regions than others. For example, wildlife trafficking and arms trade used to finance proliferation have been more prominent in Africa, while labour exploitation has occurred globally but is most prevalent in Asia and Russia. In other jurisdictions and regions, profit-generating crimes may not be a key source of PF threats at all.

The second category of revenue-raising activities is not limited to criminal activities. Typologies also show the use of business or employment activities that are otherwise licit, but which generate income for proliferation actors. Examples of this include North Korean restaurants operated in certain Asian jurisdictions,[37] or the sale of North Korean-made statues to some African jurisdictions.[38]

The presence and influence of proliferating countries, their state-entities, or their citizens and dual nationals may pose PF threats. The physical in-country presence of actors with connections to a proliferator should therefore be considered as a potential threat. Additionally, the influence of these actors – even if they are not located in-country – should be considered, given the propensity of proliferators to establish broad proliferation networks through complicated transnational corporate structures. Influence means proliferation actors legally owning (for example, ownership of a threshold amount of shares in a company) or otherwise controlling legal persons or legal arrangements through trusts, arrangements or agreements, regardless of whether they have legal or equitable force. The UN Panel of Experts, in its latest report released in March 2019, even highlighted the risk that North Korean diplomats may seek to control bank accounts in jurisdictions to which they are not accredited, or in which they do not have an embassy presence.[39]

It is, however, important that governments do not automatically assume that all nationals or dual citizens of proliferating countries, or countries of proliferation concern, pose a PF threat without further context or information to justify such conclusions.

Annex 3 identifies a range of possible threats corresponding to the three categories of PF activities identified in Chapter I. Risk-assessment methodologies often create a clear demarcation between factors that can be considered threats and those that can be considered vulnerabilities.[40] Annex 3 includes threat factors that many assessment methodologies would consider in the context of vulnerabilities. However, in the context of PF, a more flexible approach to classification of threats and vulnerabilities is needed. Activities in certain sectors may be threats since they are

37. For more on the role of North Korean restaurants in financing North Korea's proliferation activities, see Arterburn, 'Dispatched'.
38. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', p. 44.
39. *Ibid*., p. 64.
40. US Department of the Treasury, 'National Proliferation Financing Risk Assessment', December 2018, pp. 2–5.

known activities in PF typologies, or because they are sanctioned (such as certain commodities that North Korea is restricted from trading). Annex 3 identifies some of these activities or modalities as threats for two reasons. First, it provides a clearer picture of PF threats, which is important to address the lack of awareness of PF methods; second, it enables more targeted consideration of vulnerabilities against each of these threats.

The RUSI Proliferation Financing Rapid Risk Assessment Tool therefore focuses less on whether certain matters should be classified as threats or vulnerabilities, but rather takes the approach of identifying modalities of PF (threats) and then stress testing national controls (vulnerabilities) against each modality for gaps or weaknesses that may allow those PF modalities to materialise.[41]

The threats in Annex 3 have been drawn from a study of proliferation and PF tactics employed by North Korea and Iran as outlined in United Nations Panel of Experts reports, as well as activities that proliferators are prohibited from engaging in.[42] Not all the listed threats will be relevant to each jurisdiction. Jurisdictions should identify the threats that are relevant to their specific national context by considering contextual factors such as: political and social factors; economic and technological factors; geographic and environmental factors; legal and institutional factors; and legal persons and legal arrangements.

Additionally, jurisdictions should take into account both actual and potential threats, as explained in further detail in Chapter III. Jurisdictions should take into consideration the presence of a threat in similar jurisdictions or factors that may lead to the manifestation of a certain threat in the future.

Vulnerabilities

Vulnerabilities are matters that may be exploited by threats or may be used in support of, or to facilitate, threats.[43] Jurisdictions should consider national vulnerabilities under categories such as political and social factors, economic and technological factors, geographic and environmental factors, legal and institutional factors, and legal persons and legal arrangements

41. Authors' telephone interview with expert, John Chevis, 22 October 2018. John Chevis is an anti-money laundering and counter-terrorism financing expert who has worked as an adviser with the United Nations Office of Drugs and Crime and was previously an Australian Federal Police Officer.
42. For reports related to North Korea, see United Nations Security Council (UNSC), 'Reports', <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>, accessed April 2019; for reports related to Iran, see Security Council Report, 'UN Documents for Iran: Sanctions Committee Documents', <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=Iran&cbtype=iran>, accessed April 2019. For the full list of activities prohibited under UN sanctions on North Korea, see UNSC, 'Security Council Committee Established Pursuant to Resolution 1718 (2006)', <https://www.un.org/securitycouncil/sanctions/1718>, accessed 29 April 2019.
43. FATF, 'FATF Risk Assessment Guidance', p. 7.

that may exacerbate or mitigate a threat. They could also go further and consider vulnerabilities at the sectoral level, identifying key industries or sectors that are particularly exposed to a threat, and analysing the vulnerabilities of that sector.[44]

The key principle of residual risk warrants mention here. Residual risk measures the level of risk after taking into account the effectiveness of controls that mitigate or reduce risk.[45] Inherent risk, on the other hand, does not consider mitigating factors. The RUSI Proliferation Financing Rapid Risk Assessment Tool helps measure residual risks. Mitigating factors should be considered in the context of assessing vulnerabilities.

Annex 4 provides a table listing vulnerabilities under each of the categories mentioned above for jurisdictions to consider. The list is not exhaustive. When evaluating national vulnerabilities for a PF national risk assessment, jurisdictions should consider jurisdiction-specific vulnerabilities they have identified for ML and TF risk assessments, as many of these are also relevant in the PF context. The table in Annex 4 includes some of these generic vulnerabilities that jurisdictions will be familiar with from ML and TF risk assessments. However, it emphasises vulnerabilities that are particularly important to consider in the PF context. It draws on key vulnerabilities that have been detected through UN Panel of Experts reports,[46] FATF and FATF-Style Regional Bodies mutual evaluation reports,[47] and policy reports.[48]

Consequences

Consequences refer to the impact or harm caused by the presence of PF activities on a national economy and society.[49] Analysing consequences is important to assist with prioritising prevention and mitigation efforts. Consequences need not be limited to financial or economic impacts, but can also include social and security consequences. Identifying consequences therefore requires judgement calls and the application of qualitative values as well as tangible, economic calculations.

There are different approaches to incorporating consequences as part of a risk assessment. One approach is to consider consequences in relation to each threat and again in relation to each vulnerability. The more severe the consequence, the higher a threat would be classified. In the same vein, if a vulnerability was of minor consequence, it would lower the seriousness of the vulnerability. Alternatively, consequences could be considered against the overall likelihood

44. IMF, 'Annex 3: The Fund Staff's Approach'.
45. *Ibid.*
46. UNSC, 'Reports'; Security Council Report, 'UN Documents for Iran: Sanctions Committee Documents'.
47. FATF, 'Topic: Mutual Evaluations', <http://www.fatf-gafi.org/publications/mutualevaluations>, accessed 26 April 2019.
48. See Emil Dall, Andrea Berger and Tom Keatinge, 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance', *Whitehall Report*, 3-16 (June 2016).
49. FATF, 'FATF Risk Assessment Guidance', p. 7.

(threats and vulnerabilities combined) of a risk. For simplicity, the RUSI Proliferation Financing Rapid Risk Assessment Tool contained in Annex 6 of this guide takes the latter approach.

In the context of PF, consequences may be difficult to quantify. In the case of ML and its predicate crimes, there is relatively more investigation, prosecution and asset forfeiture case data than for PF, which can assist in quantifying the monetary value of the crimes and comparing that figure against a jurisdiction's economy. The broader security and societal implications (for example, the potentially large-scale threat to human life) of the proliferation of WMDs means that, similar to TF, non-economic value judgements must also be taken into consideration when measuring consequences of PF. In this guide, consequences take into consideration the effect of PF activities on financial systems and institutions, on the broader economy and on society more generally.

Some jurisdictions may wish to classify the consequence of any PF threat as automatically high in light of the ultimate impact caused by a proliferation event, resulting in the use of WMDs. This is an approach that is often used in TF risk assessments, such as the European Commission's Supranational Risk Assessment Report in its assessment of ML and TF risks.[50] Ireland also adopted this understanding of consequences in its national ML and TF risk assessment, focusing instead on threats and vulnerabilities as the main indicators of risk.[51] An alternative approach is to consider the interim or immediate impact of PF threats. This often involves financial, economic or reputational impacts.[52] In light of the broad scope of the three categories of PF activities identified in Chapter I, some activities would be too far removed from, or would make too limited a contribution towards, the ultimate impact of proliferation in order for a high consequence rating to be automatically applied to every threat.

Instead, the guide finds a middle ground and proposes that jurisdictions consider the consequences of PF activities in their jurisdiction across three contexts: impact on human life, environment or infrastructure; impact on international or regional security or stability; impact on national economy or financial system and industry or reputational damage. As an example, jurisdictions may wish to classify any PF activity which has a direct impact on human life as automatically severe. Alternatively, activities or infrastructure which simply sustain existing

50. European Commission, 'Report from the Commission to the European Parliament and the Council on the Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities', 26 June 2017, <ec.europa.eu/newsroom/document.cfm?doc_id=45319>, accessed 18 February 2019; for the methodology for the European Commission's Supranational Risk Assessment Report, see European Commission, 'Commission Staff Working Document', SWD (2017) 241 final, 2017, p. 235, <https://ec.europa.eu/newsroom/document.cfm?doc_id=45653>, accessed 18 February 2019.
51. Department of Justice and Equality, 'National Risk Assessment for Ireland: Money Laundering and Terrorist Financing', October 2016, p. 6, <http://justice.ie/en/JELR/Pages/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16>, accessed 18 February 2019.
52. Authors' telephone interview with John Chevis, 22 October 2018.

proliferation or PF networks may be classified as of moderate or limited consequence depending on the significance of the activity. Annex 4 contains a matrix for rating consequences.

Box 4: Evaluating Consequences of Proliferation Financing Activity

Impact on human life, environment or infrastructure. While the economic impact of damage to infrastructure and potential casualties following a nuclear or radiological event can be estimated (for example, see tools such as Nukemap by Alex Wellerstein), attempts at quantifying the value of human lives are ethically problematic. Due to these challenges, impacts on human life, environment or infrastructure should be classified as severe.

While the likelihood of a North Korean nuclear missile strike remains relatively low, use by North Korea of radiological dispersal devices, targeted assassinations with chemical or biological weapons, or another form of chemical, biological or radiological attack is a distinct possibility, as was demonstrated by the assassination of Kim Jong-nam in Kuala Lumpur in February 2017.

The consequences of non-state actors procuring and using a WMD could be equally devastating, as was demonstrated by the 1995 chemical weapons attacks on the Tokyo subway by the Japanese cult Aum Shinrikyo. The more recent allegations of the use of chemical weapons in Syria by government forces and the terrorist group Daesh (also known as the Islamic State of Iraq and Syria, ISIS) highlight the importance of continued international vigilance over potential efforts by non-state actors to procure WMD-related materials.

Impact on international or regional security or stability. The national and international security implications of supporting the financing of proliferation activities should also be considered. North Korea's WMD programme, Iran's missile tests, and developments in these fields by other state and non-state actors pose serious regional and international security risks. For instance, in 2017 North Korea conducted 20 ballistic missile tests and tested a high-yield nuclear device that Pyongyang claimed was a thermonuclear weapon. Pyongyang has also demonstrated medium-, intermediate- and intercontinental-range missile capabilities, although it remains unclear whether North Korean intercontinental-range ballistic missiles are capable of delivering a nuclear warhead that would survive re-entry. Further expansion of North Korean WMD capabilities will in and of itself be destabilising to regional and international security, even if an actual North Korean nuclear attack is never actually carried out.

Impact on national economy or financial system and industry or reputational damage. The failure of a jurisdiction to demonstrate efforts to address likely PF threats can itself produce significant negative consequences for an economy. Financial institutions and other businesses are wary of operating with or in jurisdictions that fail to take the necessary precautions to guard themselves against exposure to PF activities or sanctions evasion more broadly. Jurisdictions that have serious deficiencies in compliance with PF controls are publicly identified by the FATF on a list of 'high-risk and other monitored jurisdictions'. Engaging in business with entities who may – knowingly or unknowingly – be

involved in PF or sanctions evasion also implicates the business in question and may make it liable to prosecution in its home jurisdiction.

Sources: Alex Wellerstein, 'Nukemap', 2012–2019, <https://nuclearsecrecy.com/nukemap/>, accessed 29 March 2019; Richard C Paddock and Choe Sang-Hun, 'Kim Jong-nam was Killed by VX Nerve Agent, Malaysians Say', New York Times*, 23 February 2017; Organisation for the Prohibition of Chemical Weapons (OPCW), 'Report of the OPCW Fact-Finding Mission in Syria Regarding the Incidents in Al-Hamadaniyah on 30 October 2016 and in Karam Al-Tarrab on 13 November 2016', S/1645/2018, 2 July 2018; OPCW, 'Interim Report of the OPCW Fact-Finding Mission in Syria Regarding the Incident of Alleged Use of Toxic Chemicals as a Weapon in Douma, Syrian Arab Republic, on 7 April 2018', S/1645/2018, 6 July 2018; UN Security Council, 'Seventh Report of the Organisation for the Prohibition of Chemical Weapons – United Nations Joint Investigative Mechanism', S/2017/904, 26 October 2017; UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2018/171, 5 March 2018, pp. 6–7; David E Sanger and Choe Sang-Hun, 'North Korean Nuclear Test Draws U.S. Warning of "Massive Military Response"',* New York Times*, 2 September 2017; FATF, 'High-Risk and Other Monitored Jurisdictions', <http://www.fatf-gafi.org/countries/#high-risk>, accessed 18 February 2019.*

Mitigation Strategies

Jurisdictions should ensure that once risks have been identified, jurisdictions take the next step of considering mitigation strategies, agreeing to timelines for completion and identifying agencies responsible for implementation. Based on an assessment of risk likelihood, and coupled with an analysis of the consequences, jurisdictions may choose to accept, further mitigate or seek to prevent certain risks.[53]

The RUSI Proliferation Financing Rapid Risk Assessment Tool in Annex 6 provides a column for recording mitigation strategies. Since the tool calculates residual risk, jurisdictions may choose to accept the residual risk of a certain threat in light of limited consequences and low likelihood. Alternatively, jurisdictions may consider it necessary to put in place strategies to further mitigate a risk to decrease its likelihood or in light of the severe consequences. For instance, they may provide the private sector with further guidance and obligations in a particular risk area or focus law enforcement efforts on certain criminal activities that fund proliferation. In some instances where the likelihood and consequences are particularly high, jurisdictions may explore options for preventing the risk altogether. For example, jurisdictions may be able to make certain activities, such as providing a particular financial service to a particular jurisdiction, entirely unlawful in order to prevent a risk from manifesting. It should be noted that prevention may not be feasible in all circumstances.

53. FATF, 'FATF Risk Assessment Guidance', p. 27.

All in all, the risk assessment methodology helps jurisdictions identify priority risk areas within their jurisdiction, to focus efforts and resources towards addressing those specific areas of risk.

III. Additional Considerations for a PF National Risk Assessment

Threat Assessment

AS PREVIOUSLY MENTIONED, unlike ML or TF risks, where governments often have extensive built-up knowledge of the threat and vulnerability landscape, a key issue in the context of PF is how to tackle a risk assessment on a topic on which limited national data, statistics or knowledge may be available.

Awareness raising of PF therefore remains a key area of need for many jurisdictions' governments and private sectors. Because proliferators use an evolving set of tactics to evade sanctions, they also seek to exploit an increasing range of jurisdictions. Consequently, in many jurisdictions the proliferation risk may not be immediately obvious, and PF risk may be even further removed. In addition, jurisdictions may currently have little or no legal, institutional, policy, procedural or other responses to PF, which makes the consideration of vulnerabilities a cursory exercise. In light of these challenges, some jurisdictions may find a threat assessment, that only focuses on threats, to be a useful starting point.

Jurisdictions should note, however, that in the absence of consideration of vulnerabilities and mitigating factors for risk reduction, a threat assessment is unlikely to meet the FATF concept for an assessment of ML or TF risks.[54] However, noting that the FATF methodology currently does not require a PF risk assessment, a threat assessment would still provide a useful starting point for jurisdictions seeking to gain an understanding of PF threats in their jurisdiction and inform government actions. A threat assessment promotes understanding of PF threats within a jurisdiction and builds the groundwork for developing policy responses.

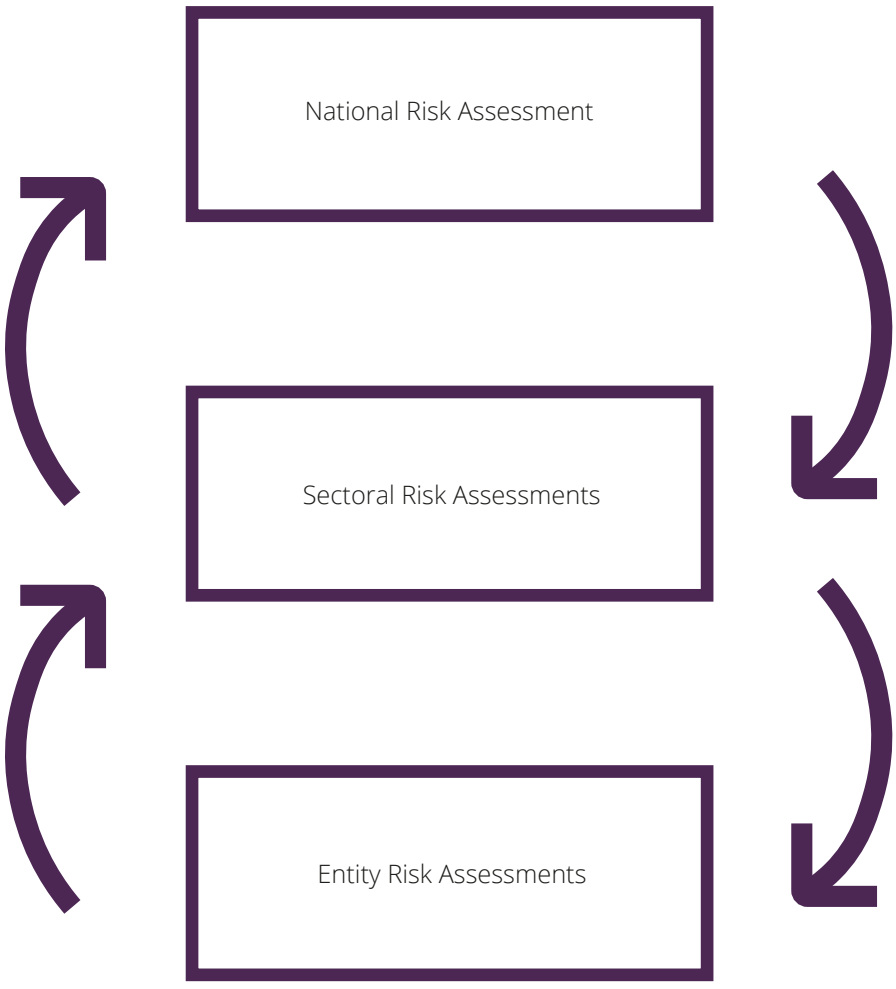
By beginning with a threat assessment, jurisdictions can decide whether to take a top-down or a bottom-up approach to a more comprehensive risk assessment.[55] For a top-down approach, the initial threat assessment would provide the foundational framework to eventually include

54. FATF, 'FATF Risk Assessment Guidance', pp. 6–7.
55. See Australian Criminal Intelligence Commission, 'Organised Crime in Australia 2017', 2017, <https://www.acic.gov.au/publications/intelligence-products/organised-crime-australia>, accessed 27 October 2018; Australian Government/AUSTRAC, 'Australia's Securities and Derivatives Sector: Money Laundering and Terrorist financing Risk Assessment', July 2017, <http://www.austrac.gov.au/australias-securities-and-derivatives-sector>, accessed 27 October 2018.

considerations on national vulnerabilities and consequences in a comprehensive national PF risk assessment. On the other hand, a bottom-up process would involve disseminating the threat assessment, along with PF typologies, indicators and other relevant information, to the private sector and encouraging entity-level risk assessments that would eventually feed into sectoral-level risk assessments. The sectoral-level risk assessments would in turn feed from the bottom up to a comprehensive national risk assessment. This is demonstrated in Figure 2.

This RUSI Proliferation Financing Rapid Risk Assessment Tool in Annex 6 takes a largely top-down approach to conducting a risk assessment; however, an optional sectoral worksheet is also offered and adds a bottom-up element to the methodology.

Figure 2: Top-Down or Bottom-Up Approach to National Risk Assessment



Source: The authors, 2019.

Considering Actual or Potential Risks

While all risk assessments should be evidence based, the assessment methodology may be driven to a greater or lesser extent by quantitative case data and known occurrences, or by qualitative input and analysis of potential risks. The former methodology focusing on known data is often referred to as an 'actuality-based assessment',[56] which predominantly focuses on existing case and statistical data as the basis for determining threats, vulnerabilities and consequences. For example, case data on threats is derived from sources such as criminal investigations, prosecutions, confiscation actions, regulatory enforcement actions, and financial and other intelligence reports. Vulnerabilities are assessed by analysing the modalities used in the crime and the detection, disruption and prosecution responses in sectoral and national control systems. Consequences are measured by calculating monetary or economic values relating, for example, to the documented amount of assets laundered or confiscated. It can be most useful in relation to ML risk assessments where jurisdictions are likely to have the requisite case data and where value assessments on consequences are easier to quantify.[57]

In the context of PF, however, an actuality-based assessment may be of limited use. First, many jurisdictions are unlikely to currently have the same amount of national data related to PF that they would in relation to ML. The lack of data and cases to draw on may be due to a lack of legal requirements, awareness among government agencies and the private sector, or a lack of institutional mandates. This means that the risk assessment would be based on a very narrow set of information. Risk-assessment methodologies that are driven by actualities may therefore not be sufficiently reflective of a jurisdiction's PF risks.

Another method of risk assessment which allows a greater emphasis on qualitative input and reasoning is therefore needed when assessing PF risks, which can be labelled a 'qualitative reasoning-based risk assessment'. This type of methodology combines any available national data with a broader range of information and places greater reliance on qualitative judgements in calculating risk.[58] This means jurisdictions will have to look beyond data and cases in their own jurisdiction, and instead consult a broader range of information sources. It also means that jurisdictions should consider how knowledge and information about proliferation risk more generally can help formulate a view of PF risk specifically. Some of the key sources of information on proliferation activities are currently contained in international case studies found in UN Panel of Experts reports and other reputable typologies reports (see Annex 2). In addition to drawing on international typologies, a qualitative reasoning-based risk assessment also allows for similar jurisdiction analysis.[59]

56. Authors' telephone interview with John Chevis, 22 October 2018.
57. *Ibid*.
58. Authors' telephone interview with Neil Jensen, 22 October 2018. Neil Jensen is the former CEO of AUSTRAC and now a consultant assisting jurisdictions to conduct national risk assessments in ML, TF and PF.
59. Authors' telephone interview with John Chevis, 22 October 2018.

A qualitative reasoning-based risk assessment also does not require a quantitative assessment of consequences. As discussed earlier, in the context of PF, it is important to consider non-financial consequences such as the harm of proliferation of WMDs on peace, security and broader social impacts.

There are, of course, dangers in over-reliance on qualitative judgements that draw predominantly on international or similar jurisdiction analysis without national data and statistics. A qualitative assessment combined with a top-down approach may produce findings that draw broad conclusions based on limited evidence. Jurisdictions should be careful to ensure that a detailed analysis of the jurisdiction context against known PF typologies is undertaken, and that findings are made on the basis of sound reasoning. For example, jurisdictions should understand their role in proliferation pathways and consider issues such as whether sanctioned proliferators have a diplomatic presence or other established networks in their jurisdiction, or whether their jurisdiction is a known source or destination of sensitive goods traded with proliferators. If yes, then sound judgement would indicate that finance will almost inevitably flow through their jurisdiction through certain financial products and services.

Identifying Sources of Information

Information on PF threats, vulnerabilities and consequences can come from a wide variety of national and international government, private sector, and other non-governmental sources. A non-comprehensive list of key sources of PF-relevant information is provided in Annex 1. Fundamentally, effective information gathering requires regular engagement with and input from all relevant PF stakeholders. A range of stakeholders are exposed to PF threats at different points in the PF supply chain and proliferation activities more generally, and thus capture discrete snapshots of proliferation and PF activity within a jurisdiction. Bringing these snapshots together allows the lead agency to develop a more complete picture of the jurisdiction's PF risks.

A useful starting point for sources of information is government-held data and statistics on proliferation activities, as well as PF cases if they exist. Intelligence agencies, government bodies responsible for foreign affairs and economic development, financial regulators, and regulators of controlled or otherwise PF-vulnerable sectors all collect information and produce analysis that is relevant to understanding the scope and nature of PF activity within a jurisdiction's economy. An intra-governmental information-sharing mechanism should allow these agencies to share information with each other and with the lead agency, so that it can be fed into the national assessment of PF risk.

The value of information gathered by the private sector should also not be overlooked, and is considered later on in this chapter.

Another particularly useful source of information, especially for jurisdictions that have little intelligence or statistics on PF activities within their economy, is information from similar jurisdictions whose PF-specific threats and vulnerabilities are better documented or more easily accessible. These jurisdictions may have already conducted a national risk assessment

and have PF data and statistics readily available, or they may have been involved in a PF case ,the details of which are publicly accessible, or where the jurisdiction is otherwise willing to share the case details. Similar jurisdictions are those jurisdictions that have similar economic, social, geographic or other contextual factors. Similar jurisdictions from the same region would be even more useful from an analysis point of view since they may involve networks that are operational in multiple jurisdictions in that region, including the jurisdiction undertaking the national risk assessment.

Further still, in the context of PF, international and non-governmental information sources are vital. For example, the UN Panel of Experts reports contain valuable cases that build an understanding of PF methodologies and networks.[60] Several research institutions have also produced PF typology reports and PF red-flag indicators[61] to complement those already identified by the FATF.[62] Given that PF is an area that has received little attention in the past at national levels, these international and non-governmental resources are vital in understanding a broad picture of PF activities to analyse national threats and vulnerabilities in an informed manner.

Identifying Relevant Stakeholders

Many of the government and private sector actors that are normally considered stakeholders in ML and TF efforts will also be relevant in a PF context. The World Bank National Risk Assessment Tool identifies several government agencies as important contributors to an ML/TF national risk assessment. These contributors include a jurisdiction's:

> Financial Intelligence Unit, Central Bank, Financial Regulation and Supervision Agency (if exists), Capital Markets Authority, Regulator of the Insurance Market, Tax Authority, Intelligence Agency, Police … Anti-Corruption Agency, Anti-Drug Agency, Customs Authority, Office of Public Prosecutor, Ministry of Finance, Regulators of other financial services, and authorities related to DNFBPs.[63]

The above stakeholders should all also be included in a PF risk-assessment process. However, jurisdictions should take care that their stakeholder engagement on a PF risk assessment is not limited to just those actors engaged in ML and TF efforts. The list of stakeholders engaged in PF is necessarily likely to be broader, given the broader scope of activities that may be classified as PF.

Governments also need to ensure that the corresponding government agencies responsible for implementing sectoral bans or supervising relevant sectors are included early on in the

60. UN Security Council, 'Reports'; Security Council Report, 'UN Documents for Iran: Sanctions Committee Documents'.
61. Emil Dall, Tom Keatinge and Andrea Berger, 'Countering Proliferation Finance: An Introductory Guide for Financial Institutions', *RUSI Guidance Paper* (April 2017); Brewer, 'Study of Typologies of Financing of WMD Proliferation'.
62. FATF, 'Proliferation Financing Report', 18 June 2008.
63. FATF, 'The World Bank Risk Assessment Methodology', p. 7, <www.fatf-gafi.org/media/fatf/documents/reports/risk_assessment_world_bank.pdf>, accessed 18 February 2019.

risk-assessment process, and consulted frequently throughout. Given the wide range of government and private sector stakeholders in the PF risk-assessment process, jurisdictions should consider convening a smaller group of core agencies and conduct more expansive consultations with a wider range of stakeholders as required. They would also make good candidates for a regularly convened working group on CPF more broadly.[64]

Additional stakeholders whose contributions to the PF risk-assessment process are likely to be helpful on an ad hoc basis may include academic and research institutions, DNFBPs with exposure to PF threats in certain aspects of their operations, and regulators of these DNFBPs. The list of stakeholders should be reviewed regularly over the course of the process, and revised as necessary. As with the collection of information, an understanding of a jurisdiction's exposure to proliferation pathways generally – not just their financial aspects – will be extremely valuable in identifying the relevant stakeholders.

Table 3 provides a few examples of the kinds of information that various stakeholders may be able to provide to assist in the identification of PF-relevant threats in an economy. Input from a wide range of stakeholders should also be sought in identifying vulnerabilities, consequences and general trends in PF activity within a jurisdiction or a region. A non-comprehensive list of relevant stakeholders can be found in Annex 2.

64. RUSI recommends that countries establish an inter-agency coordination group on CPF, separate from the national risk-assessment process. Convening a multi-agency group early during the development of CPF policies is not only important for developing a legal framework that is effective, but also raises awareness of PF obligations among a wide range of governments from an early stage. If such a working group is already well established, identifying relevant agencies to take part in a national risk-assessment process will be easier. For more on the process of setting up a multi-agency working group, see Berger and Joshi, 'Countering Proliferation Finance'.

Table 3: Examples of Key Stakeholders and Information Related to Individual Threats

Threat	Stakeholder(s)	Information
Nationals or dual citizens of proliferating states, or their family members (regardless of citizenship), used as intermediaries in jurisdictions not of proliferation concern to facilitate procurement of goods and/or for payment of funds. Likely to involve use of personal banking products.	Immigration agency	• Presence of nationals and dual citizens of proliferating states, or family members, in the jurisdiction.
	Financial intelligence unit	• Suspect individuals, businesses, accounts and financial activity patterns.
	Export control, customs and border control agencies	• Controls and vulnerabilities in export, customs or border controls that could be exploited by proliferators. • Proliferators and their patterns of activity. • Information on controlled goods, including dual-use goods.
Cross-border smuggling of cash, gold or other high-value goods by mules to support state and non-state proliferation activities.	Export control, customs and border control agencies	• Vulnerabilities in export, customs or border controls that could be exploited by proliferators. • Proliferators and their patterns of activity. • Data from cross-border declarations.
	Law enforcement and prosecution agencies	• Ongoing or past PF cases and investigations in the jurisdiction, to develop a better understanding of national PF trends.
	Immigration agency	• Information on cross-border movement, including intended destinations, of persons matching certain demographics.

Threat	Stakeholder(s)	Information
Financial institutions with known histories of providing accounts to, or otherwise facilitating, financial activities of proliferation states.	Intelligence agencies	• Active proliferation threats – the activities and capabilities of proliferators and sanctioned entities.
	Financial intelligence unit	• Registration data of financial institutions, compliance assessments, suspect individuals, businesses, accounts and activity patterns, correspondent relationships and accounts.
	Prudential regulatory for financial institutions	• Background information and prudential data concerning financial institutions.
	Law enforcement and prosecution agencies	• Information on ongoing or past PF cases and investigations in other jurisdictions.

Source: Developed by authors, 2019, based on Berger and Joshi, 'Countering Proliferation Finance'.

The Role of the Private Sector

The private sector, and financial institutions in particular, are key to the implementation of financial sanctions and wider PF obligations. The private sector should therefore be involved in a risk-assessment process on PF, as the information it holds could be crucial in determining PF threats and vulnerabilities.

It is worth noting that when it comes to PF, the scope of private sector involvement is broader than that of ML and TF. Whereas private sector engagement in combating ML and TF is largely limited to the financial sector and DNFBPs, the ability to counter PF requires other private sector stakeholders that deal in goods that may be exploited for the proliferation of WMDs and the financing thereof. This includes manufacturers of dual-use items or sensitive technology that may be vulnerable to diversion for proliferation purposes, or shipping and transport services exploited by proliferators to move those goods.

In the case of North Korea, the wide scope of sectoral sanctions mandated by the UN Security Council including restrictions on coal, oil, iron and other minerals, textiles, food products and more, means that an even greater number of industries are brought into the North Korea sanctions implementation picture. As a result, even though these sectors are not financial institutions, they may have relevant information pertaining to the general proliferation threat picture in a jurisdiction and should be included in the national risk-assessment process.

Financial institutions and sectors that deal with trade in controlled goods collect information on clients and on financing and trade patterns that can provide important context for understanding PF threats to an economy. Trade financing documents, due diligence and 'know your customer' analysis, transaction records and sales reports are all useful sources of information that a lead agency can leverage within a national risk-assessment process. Some larger financial institutions also have extensive research operations which seek to understand the organisation's own exposure to PF, including analysis of how proliferation networks operate in the national economy or the wider region. These insights, from a private sector perspective, can complement a government's own assessment of PF threats and vulnerabilities.

As outlined earlier in this chapter, the role of the private sector becomes even more pronounced if jurisdictions choose to follow a bottom-up risk-assessment process. Here, private sector stakeholders will conduct entity-level risk assessments, which will eventually feed into sectoral-level risk assessments, and eventually a comprehensive national PF risk assessment. While this guide largely takes a top-down approach to conducting a PF risk assessment, sectoral worksheets have been included in the RUSI Proliferation Financing Rapid Risk Assessment Tool depicted in Annex 6 to facilitate a bottom-up approach actively informed by private sector views.

Regardless of whether jurisdictions adopt a top-down or bottom-up risk-assessment approach, private sector actors will play an important role both as stakeholders to the process and as key sources of information to inform threats and vulnerabilities. However, it is worth keeping in mind that much of this exchange of information can only occur if mechanisms are in place to allow the private sector to share sensitive data – including information on customers and business operations – with government, in a way that protects client privacy and business interests.[65]

65. For more information on the role of public–private partnerships and exchanges of information in disrupting financial crime, see Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).

Conclusion

THIS GUIDE AIMS to provide guidance to jurisdictions on the necessary methodological foundation and tools for developing and conducting a national PF risk assessment. To this end, the guide suggests approaches to scoping the risk assessment, assessing PF threats, vulnerabilities and consequences within jurisdiction-specific contexts, and identifying relevant stakeholders and sources of information.

While the guide and the accompanying RUSI Proliferation Financing Rapid Risk Assessment Tool in Annex 6 will provide a useful starting point for conducting a national risk assessment, individual jurisdictions are ultimately responsible for analysing and applying these guidelines in a way that produces a reasonable judgement of their national risk. If conducted diligently, a national risk assessment, as well as the information collected over the course of the process, should be a critical first step in proactively addressing gaps in a national counter-PF regime, and in mitigating the impact of PF activity on the national economy and society more broadly.

About the Authors

Anagha Joshi is an Associate Fellow with RUSI's Centre for Financial Crime and Security Studies. Anagha was previously a Director in the Australian Attorney-General's Department managing technical assistance programmes to support countries across Africa, Asia and the Pacific to combat transnational crime and terrorism. She has particular expertise in anti-money laundering, counterterrorist financing, counter-proliferation financing and sanctions. Anagha is a qualified legal practitioner and has produced a range of model laws, implementation guides, policy guides and research reports for governments and inter-governmental organisations.

Emil Dall is a Research Fellow at RUSI, where he leads work on counter-proliferation finance. Since joining RUSI in 2015, his work has focused on conducting research into, and raising awareness of, the (illicit) financial networks of proliferators. Emil also co-leads RUSI's wider work on the design and implementation of sanctions, including its high-level Taskforce and research on country-based sanction regimes. Prior to joining RUSI, Emil was a risk analyst for a major international insurer operating out of Lloyd's of London, and before that he was a researcher at the Policy Institute at King's College London.

Darya Dolzikova is a Research Analyst in the Proliferation and Nuclear Policy Programme at RUSI. Her research focuses on countering the financing of proliferation activities and strengthening sanctions regimes, particularly in the context of the North Korean nuclear programme. As part of her contributions to RUSI's work on countering proliferation finance, she provides guidance to representatives of governments and financial institutions on strengthening their CPF and sanctions-compliance regimes. Prior to joining RUSI, Darya worked in a policy development and government relations role at an industry association. She also has experience working in the due diligence sector and on policy issues in Canada's Parliament.

Annex 1: Sources of Information

Information Source	Stakeholder	Type of Information
International Organisation Sources		
United Nations Panel of Experts Reports	United Nations Security Council	Details on proliferating actors, proliferator capabilities, proliferation and PF patterns and typologies, and developments in proliferation sanctions regimes.
FATF Guidance on Proliferation Financing	FATF	CPF-related obligations for governments and the private sector, and best practices for implementing a national PF regime.
FATF Typologies Report on Proliferation Financing	FATF	PF patterns and typologies, red flag indicators.
UNSCR 1540 Committee Reports	UNSCR 1540 Committee	Information on countries' implementation of measures to stop trade in controlled goods.
Global Integrated Shipping Information System	International Maritime Organization	Information on vessels and their activities, including ownership and incidents.
Government Sources (Domestic and Foreign)		
Law Enforcement and Intelligence		
Financial intelligence data and reports	Financial intelligence units	Details on financial networks and patterns of behaviour used by proliferators, including suspicious transaction/activity reports (STRs and SARs), cross-border cash transport reports, international transaction reports and intelligence analysis products.
Designations and sanctions listings	Department of foreign affairs, department of international trade, financial intelligence units	Details on sanctioned entities, sanctions-related reports and enforcement actions.
Criminal investigation and prosecution records, civil investigation and litigation records	Courts, law enforcement agencies, other investigative agencies	Details on past cases involving illicit financial networks and patterns of behaviour used by proliferators.

Other relevant data/intelligence (financial and otherwise)	Intelligence agencies, other relevant government bodies	Data on diplomatic presence and activities of proliferating states, information on proliferator capabilities and proliferation-related procurement priorities, and other relevant information on proliferator sanctions evasion.
Economic and Financial		
Economic, financial and trade reports	Department of finance, department of economic development, department of trade, department of industry, financial regulatory agencies	Data and statistics about the size of the economy and of the financial sector, information on size and activities of specific sectors, information on relevant manufacturing sector, and information on size and nature of trade relationships and trade patterns with other countries.
Regulatory		
Export/import documents	Port authority, trade financing agency, department of trade	Import/export data, data on size and nature of trade relationships and patterns, information on international transport and/or transit routes, and data on trade financing relationships.
Immigration and employment records	Department of immigration, department of labour	Data on migrant labour, and data on individuals holding passports from countries of concern, including dual nationals.
Vessel management and ownership and inspection records	Vessel management and ownership databases, regional port state control databases	Information on nature and size of foreign and national vessel activity.
Private Sector Engagement		
Bills of lading, export/import documents	Shipping companies, trade finance providers, export/import service providers	Import/export data, data on size and nature of trade relationships and patterns, information on international transport and/or transit routes, and data on trade financing relationships.
Vessel and cargo insurance documents	Insurance providers, shipping companies	Data on trade activity and relationships, data on trade financing relationships, information on international transport routes and patterns, and data on trade operations of entities suspected of engaging in proliferation-related activities.

Financial information-sharing partnerships	Financial institutions, insurance providers, industry associations, DNFBPs, relevant government stakeholders	Information on private sector due diligence practices and any challenges in understanding and implementing CPF obligations by the private sector and information on PF-related entities and patterns of behaviour.
Informal engagement	Financial institutions, insurance providers, industry associations, DNFBPs, relevant government stakeholders	Information on private sector due diligence practices and any challenges in understanding and implementing CPF obligations by the private sector, and information on PF-related entities and patterns of behaviour.
Other Sources		
Past case studies and similar jurisdiction analysis	Research institutions, relevant private sector and government stakeholders	Information on PF threats and activity in similar jurisdictions, including entities engaged in PF and their patterns of behaviour, and examples of successes or failures in efforts to reduce PF-related risk in similar jurisdictions.
King's College London typologies report, Center for a New American Security risk publications, Center for Advanced Defense Studies (C4ADS) reports, RUSI guidance papers, RUSI Project Sandstone, other open-source research and analysis products	Universities, think tanks, research institutions	Open-source data and analysis on proliferation actors and patterns of behaviour, and guidance on understanding and implementing international CPF obligations for governments and the private sector.
Automatic identification system (AIS) data	AIS tracking providers	Data on locations, travel routes and port call histories of vessels.
Media reporting	Journalistic sources	Open-source information and analysis on PF-related entities and activities.

Source: The authors, 2019.

Notes

The stakeholders listed alongside national and third-state government sources are suggestions and list the government bodies most commonly tasked with producing or managing the corresponding information source. Jurisdictions should identify the relevant government bodies in their particular case.

The information sources listed in this Annex should be consulted both within the jurisdiction conducting the national risk assessment and in relevant third jurisdictions, where available.

Some of these resources are made publicly available by foreign governments and can be accessed online or by submitting a request to the appropriate government body. Other information is likely to be classified or otherwise not made available to the public. Access to such information would have to be negotiated between the respective jurisdictions using appropriate channels and processes.

The ability of private sector actors to share information on their clients and business operations with the government and with each other is dependent on the existence of the necessary forums and regulatory frameworks to allow for such information sharing while accounting for privacy and commercial sensitivity restrictions.

Annex 2: Stakeholders

Stakeholder	Role in National Risk Assessment
Export control, customs and border control agencies	These agencies enforce compliance with export controls related to proliferation and other illicit or sanctioned goods. They will be able to provide information on: • Goods, services and sectors that have been (or might be) abused for proliferation • Proliferators and their patterns of activity • Controls and vulnerabilities in export, customs or border controls that could be exploited by proliferators.
Intelligence agencies	These agencies can provide information on: • Active proliferation threats – the activities and capabilities of proliferators and sanctioned entities • Threats, proliferation patterns and potential consequences of a proliferation-related event.
Financial intelligence units	These units play a key role in undertaking CPF risk assessments as they have access to a wide range of financial data. They also undertake network analysis, generate investigative leads and provide information on STRs, which can identify suspect individuals, businesses, accounts and activity patterns.
Law enforcement and prosecution agencies	These agencies are responsible for criminal enforcement of CPF laws and are critical in CPF investigations, which can generate information that is helpful to the work of other agencies. This includes information on: • Ongoing or past PF cases and investigations in the jurisdiction, to develop a better understanding of national PF trends • Information on ongoing or past PF cases and investigations in other jurisdictions.
Financial supervisors and other regulatory authorities	These agencies can monitor compliance of private sector institutions to ensure that sanctions are implemented effectively. These agencies will have a good understanding of the nature, size and scale of business activities across each sector. Supervisors and regulators may also hold information on how well private sector institutions understand their PF obligations and how aware they are of PF risks. Given their understanding of the scale of the sector and its relationship to the broader economy, supervisors and regulators are also helpful in determining economic consequences of PF on the national economy.
Trade promotion and investment agencies	These agencies need to be aware of PF risks when considering whether to provide support for trade. These agencies may also gain information on patterns of illicit procurement, which can then be shared with other government agencies.

Policy agencies such as foreign affairs, finance, home affairs, immigration or justice	These agencies can play an important role in ensuring that a country's CPF legal regime is compliant with international obligations and that practical mechanisms are robust and effective in reducing a country's exposure to PF risk. Foreign affairs agencies also play a crucial role in international cooperation on CPF and in contextualising national risk within the context of regional and international risks and proliferation patterns. In many countries, foreign affairs agencies are also responsible for disseminating information on international obligations and sanctions to other government agencies and authorising sanctions exemptions. In this way, these agencies may be important to minimising PF-related vulnerabilities. They may also be useful in facilitating interagency coordination within government. Immigration agencies may be able to provide information on the presence of nationals or dual citizens of proliferating countries within their own country.
Agencies involved in implementing targeted financial sanctions or sectoral sanctions	There may be other agencies not mentioned above that are involved in the implementation of targeted financial sanctions or sectoral sanctions. These agencies may be involved in liaison with UN bodies, national coordination, or monitoring and outreach activities. Countries should ensure that they identify all relevant agencies not specifically covered above.
Private sector entities	Private sector entities responsible for implementation of certain CPF controls should also be considered relevant stakeholders and should be consulted accordingly. Private sector entities may include: financial institutions; DNFBPs; insurance providers; industry associations; shipping companies; export/import service providers; relevant manufacturing industries; and relevant technical and training industries. Private sector entities may assist authorities in identifying suspicious individuals and businesses and in developing typologies for suspicious financial transaction patterns.

Source: Authors, 2019, adapted from Berger and Joshi, 'Countering Proliferation Finance: Implementation Guide and Model Law for Governments'.

Annex 3: Example List of Threats

Financial Products and Services Directly Related to Trade in Proliferation-Sensitive Goods
Use of trade finance products and services and clean payment services in procurement of proliferation-sensitive goods.
Use of front companies, shell companies or brokers to obtain trade finance products and services or as parties to clean payments.
Use of companies to provide unlicensed money remittance services.
Nationals or dual citizens of proliferating states, or family members of such persons (regardless of citizenship), used as intermediaries in countries not of proliferation concern to facilitate procurement of goods and/or for payment of funds. Likely to involve use of personal banking products.
Use of universities or research centres to procure dual-use goods and/or for payment of funds, including Iranian and Syrian institutions.
Money transfer services used to conduct cash transfers related to procurement of goods.
Use of third countries to channel financial transactions related to mining deals.
Use of professional intermediaries and firms to mask parties to transactions and end users.
Use of personal accounts to purchase industrial items.
Use of non-specific, innocuous or misleading descriptions of goods or purpose of payments.
Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance.
Use of financial routes that are circuitous to the movement of sensitive goods or to countries not of proliferation concern.
Use of vessels that do not attract proliferation concern to obtain maritime or cargo insurance products.
Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. Often combined with use of front companies with opaque ownership structures.
Licit and Illicit Revenue-Raising Activities
Arms trafficking (small and conventional) used by state and non-state actors to raise revenue.
Sale of non-nuclear arms, military equipment or technologies, or paramilitary equipment or technologies by proliferating states to other states.
Sale of coal used by state and non-state actors to raise revenue.
Construction industry and/or related trades owned or operated by or on behalf of nationals or dual citizens of North Korea or North Korean entities. Profits from payment of contracts form part of North Korea's revenue-raising activities.
Cross-border smuggling of cash, gold or other high-value goods by mules to support state and non-state proliferation activities.
Cross-border smuggling of cash, gold or other high-value goods in diplomatic bags by diplomats or consular officers to support state proliferation activities.
Cybercrime, such as hacking accounts to obtain value, largely used by state actors.

Drug trafficking by state and non-state actors, including through connections with organised criminal networks. Proceeds used to support proliferation activities.
Export of art or statues by North Korea or involving North Korean designated entities and individuals to raise revenue.
Sale of minerals (gold, iron, steel, copper, zinc and so on) by North Korea or involving North Korean designated entities and individuals to raise revenue.
Payments made to labourers or workers (nationals or dual citizens) from North Korea. Payments are then largely confiscated by North Korea as part of its revenue-raising activities.
Restaurants or other small to medium-sized, largely cash-based businesses owned or operated by or on behalf of nationals or dual citizens of North Korea. Profits from businesses are sent to North Korea as part of its revenue-raising activities.
Export of seafood originating from North Korea or involving North Korean designated entities and individuals.
Export of textiles originating from North Korea or involving North Korean designated entities and individuals.
Wildlife trafficking by state and non-state actors including through connections with organised criminal networks.
'Taxes' and 'duties' collected by terrorist groups in controlled areas, as well as donations made to terrorist groups, as part of revenue-raising activities to support procurement of WMD materials, particularly chemical or biological weapons.
Financial and Corporate Infrastructure in Support of the Movement of Finances and Goods
Use of banks and other financial institutions with foreign branches operating in countries of proliferation concern.
Use of cryptocurrencies to avoid the formal financial system.
Use of diplomats, consular officers or diplomatic or consular missions of North Korea to build networks, including corporate networks, within a country. These networks then facilitate a range of revenue-raising activities as well as facilitating financial products or services related to trade in goods.
Use of local branches of banks and financial institutions based in countries of proliferation concern.
Money-exchange businesses used for cash transfers in support of proliferation networks, where transfers involve individuals or entities owned or controlled by proliferation actors. Can also involve structured payments to organised crime networks involved in revenue-raising activities.
Use of *hawala* or bartering systems of value transfer to pay and settle debts among members of a proliferation network.
Use of a ledger payment system among members of a network that minimises the need for international financial transactions. Banks may be used to facilitate some end-of-term settlements between companies and/or individuals.
Financial institutions with known histories of providing accounts to, or otherwise facilitating, financial activities of proliferation states.
Use of companies to provide unlicensed money-transfer services among members of networks or to conduct ad hoc transactions.
Use of professional intermediaries and corporate service providers to mask the presence of proliferation actors.
Use of trade or other economic relations of countries with links or significant exposure to a proliferating country. Often facilitated by a complex corporate network.

Use of organised or transnational crime networks, particularly their transport corridors and intermediaries in their networks.
Establishment of corporate networks that facilitate but may not be solely involved in PF activities. Ultimate beneficial ownership, connections and control structures are opaque.

Source: The authors, 2019, based on Panel of Experts Reports for North Korea, <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports> and Iran, <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=Iran&cbtype=iran>; also see Jonathan Brewer, 'Study of Typologies of Financing of WMD Proliferation', Project Alpha, Centre for Science and Security Studies, King's College London, October 2017.

Annex 4: List of Vulnerabilities

Category	Vulnerabilities
Legal and institutional factors	• Limited enforcement capabilities • Difficulties or limitations in international cooperation • Efficacy of measures to counter organised crime networks involved in illicit activities • Deficiencies in interagency coordination and information sharing • Limited financial intelligence and investigation capabilities in government • Deficiencies in controls for detection of cross-border movement of cash, precious metals and stones (particularly gold), and bearer-negotiable instruments • Deficiencies in controls for detection of cross-border movements of wildlife products • Limited mechanisms for reciprocal sharing of relevant data/intelligence with authorities • Limited private sector and public outreach, guidance or awareness raising on PF, including red flag indicators and circulation of typologies • Limited private sector outreach and guidance on sanctions obligations, including sanctions-specific reporting mechanisms (as opposed to suspicious transaction reporting) • Limited private sector compliance monitoring and enforcement mechanisms • Weak laws, including weak proliferation and PF laws that comply with international obligations • Weak regulatory frameworks, including gaps in knowledge of the market • Existence of a shipping registry, including one that offers flags of convenience.
Legal persons and legal arrangements	• Lack of transparency of legal persons and legal arrangements, including beneficial ownership structures of businesses • Lack of robustness in government procurement processes to screen against sanctions risks • Lack of robustness in market entry requirements for financial institutions, DNFBPs, legal persons and legal arrangements.
Geographic and environmental factors	• Porous land borders • Shared land borders or regional proximity with proliferating countries or other high-risk jurisdictions for proliferation activity (North Korea, Iran, Syria, China and Russia) • Offshore territories in proximity with proliferating countries • Significant transport activity (transport hub), and thus more likely to be involved in illicit flows • Host to wildlife or other natural products that are protected, for example under the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), that are used as part of revenue-raising activities by proliferators (for example, rhino horns and elephant tusks/ivory).

Economic and technological factors	• Over-reliance on friendly business practices to attract foreign investment • Weak trade or trans-shipment controls • Existence of cryptocurrencies and cryptocurrency exchanges • Limited knowledge of, lack of regulation of, or limited outreach to cryptocurrency exchanges • Limited regulation or monitoring of internet platforms for trade • Chemical or petrochemical industry and/or trade • Dual-use or controlled goods industries and/or trade • High-tech industry and/or trade • Maritime or cargo insurance or re-insurance industry • Missile component, aerospace, military or related industries and/or trade • Significant import/export businesses and trading activity (hub), and thus more likely to be involved in related illicit financial flows • Significant trade finance industry • Significant regional financial hub facilitating international funds transfers and access to international markets • Existence of free-trade zones • Significant freight-forwarding businesses.
Social and political factors	• Lack of political will or political priority to combat proliferation or PF • Poor awareness of third-country diplomatic activities in the country • Significant diasporas of nationals or dual nationals from proliferating countries with limited foreign labour and employment regulation • Visa-free regimes with proliferating countries • Hosting diplomatic or consular missions of proliferating countries • Presence of universities or other research bodies involved in subject matter potentially related to WMDs or dual-use goods training or development – particularly universities having ties with jurisdictions of proliferation concern or with foreign students from countries of proliferation concern.

Source: The authors, 2019.

Annex 5: Consequences Matrix

Consequence Level	Description
Severe	• Impact on human life, environment or infrastructure, or • Severe impact on international or regional security or stability, or • Severe impact on national economy or financial system, or • Severe impact on industry sectors; global reputational damage.
Moderate	• Moderate impact on international or regional security or stability, or • Moderate impact on national economy or financial system, or • Moderate impact on industry sectors; domestic reputational damage only.
Limited	• Limited impact on national economy or financial system, or • Limited impact on industry sectors; limited reputational damage only.

Source: The authors, 2019.

Annex 6:
RUSI Proliferation Financing Rapid Risk Assessment Tool

Developed by Anagha Joshi

RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

Instructions

FOR JURISDICTIONS THAT wish to use the RUSI Proliferation Financing Rapid Risk Assessment Tool, this Annex provides instructions on how to use it.

The tool comes in the form of a multi-tab spreadsheet, example images of which have been included in this Annex. The full version of the spreadsheet can be provided upon request by emailing cpf@rusi.org.

Jurisdictions should use the spreadsheet tabs in numerical order, from 1 to 3. Tabs 4 and 5 are optional extras for jurisdictions that wish to undertake a more detailed sectoral analysis of risks. The spreadsheet contains pre-inserted formulas that will automatically calculate some fields as well as drop-down lists with ratings. Other fields need to be manually entered. Guidance notes are inserted into the spreadsheet itself. Users can click on a cell or heading within the spreadsheet for further information and instructions.

Step I: Identifying and Assessing Threats

- Drawing upon various sources of information (see Annex 1), identify PF threats relevant to your jurisdiction. As a starting point, Annex 3 provides a non-exhaustive list of threats under the three categories of PF activities discussed in this guide.
- When identifying potential threats, consider each threat against the following contextual factors within your jurisdiction:
    - Social and political
    - Economic and technological
    - Geographic and environmental
    - Legal and institutional
    - Legal persons and legal arrangements
    - Sectoral.
- Undertake an analysis of the threats you have identified and give a preliminary rating for each threat. Ratings should be high, medium or low. Threat ratings should be assigned based on an assessment of the prevalence of the activity in your jurisdiction or the existence of contextual factors that may facilitate the activity. Consider also the potential volume or size of the activity. You should include potential threats that may materialise in the future and be as inclusive in your list of threats as possible.
- Insert each threat into the threats column in Spreadsheet 1, starting with threats ranked high (3), then medium (2), then low (1). Under each threat, there is room to insert a brief narrative summary of the analysis which justifies the rating level. The cell containing the threat will be automatically colour coded red (high), orange (medium) or yellow (low).

Step II: Identifying and Assessing Vulnerabilities

- Also in Spreadsheet 1, jurisdictions should consider their vulnerabilities against each identified threat. Vulnerabilities are split into two categories – national and sectoral – with each category containing a number of subcategories. National vulnerabilities have the following subcategories: social and political; economic and technological; geographic and environmental; legal and institutional; and legal persons and legal arrangements. Sectoral vulnerabilities have the following subcategories: financial institutions; designated non-financial businesses and professions; and other high-risk sectors.
- Annex 4 provides a non-exhaustive list of issues that jurisdictions may wish to consider in analysing each category of national vulnerability. This list contains some generic vulnerability indicators that are also used in ML and TF risk assessments, although it is focused predominantly on issues that are particularly relevant in the PF context. Jurisdictions should not be restricted to this list when identifying and analysing their vulnerabilities and should consider all relevant vulnerabilities under the subcategories identified.
- Jurisdictions should analyse each subcategory of vulnerabilities and rate each subcategory as a high (3), medium (2) or low (1) level of vulnerability. For each subcategory of vulnerability, you should balance gaps with mitigating factors so that the vulnerability rating is a residual rating. Examples of mitigating factors may be a high level of regulatory or law enforcement controls that make for a strong regime of detection and disruption of that threat.
- Sectoral vulnerabilities should be assessed by considering the exposure of each sectoral category to each threat, as well as balancing mitigating factors such as regulatory and operational controls. Alternatively, jurisdictions may wish to use the optional Sectoral Risk Workbook in Spreadsheet 4 to undertake a more detailed analysis of sectoral risks. This sectoral analysis then forms the information and data on which you can make a qualitative assessment of the sectoral vulnerability level in the national risk assessment.
- For each subcategory of vulnerability, jurisdictions should insert a brief narrative summary of the analysis which justifies the rating level. The cell will be automatically colour coded red (high), orange (medium) or yellow (low).
- The rating for each subcategory of vulnerabilities has equal weight and the overall vulnerability rating is the average of all subcategories of vulnerability. The method of averaging the vulnerability ratings provides a simple measure of the overall vulnerability. However, jurisdictions should consider where the specific areas of vulnerability exist and pay particular attention to areas where the vulnerability rating is high. The spreadsheet contains a separate column that automatically calculates the overall vulnerability rating.
- It is possible that for some threats, certain categories of vulnerabilities are simply not relevant at all. A low rating for these irrelevant vulnerabilities may result in an overall risk lower than appropriate. In this case, jurisdictions should insert 'N/A' (not applicable) in the vulnerability field and not give a numerical rating for that vulnerability. Where no rating is given for a vulnerability, the formula will automatically amend to discount that vulnerability. An instruction is provided on this in the spreadsheet. Jurisdictions should, however, use the 'N/A' option sparingly and with caution. In most circumstances, jurisdictions should give consideration to each vulnerability category.

Step III: Identifying and Assessing Consequences

- Annex 5 provides a matrix to guide considerations for rating consequences. Consequence severity is rated as severe (3), moderate (2) or limited (1).
- For each threat, jurisdictions should analyse consequences with reference to Annex 5. Consequences should be considered across three contexts: impact on human life, environment or infrastructure; impact on international or regional security or stability; and impact on national economic or financial system, including impact on industry or reputational damage.
- Within Spreadsheet 1, in the cell for consequences, jurisdictions should insert a brief narrative summary of the analysis which justifies the rating level. The cell will be automatically colour coded red (severe), orange (moderate) or yellow (limited).

Step IV: Depicting Likelihood as a Heat Map

Jurisdictions should plot the rating for each threat and its commensurate vulnerability rating in the heat map in Spreadsheet 2. The spreadsheet contains further instructions for doing this.

Step V: Depicting Overall Risk as a Heat Map

Jurisdictions should plot the likelihood rating for each threat (the combination of threats and vulnerabilities) and its commensurate consequences rating in the heat map in Spreadsheet 3. The spreadsheet contains further instructions for doing this.

Instructions for Optional Sectoral Assessments

In Spreadsheet 1, sectoral vulnerabilities are considered in three categories: financial institutions; DNFBPs; and other high-risk sectors. Each of these categories are considered at a macro level based on a top-down analysis of data and information across these sectors.

Alternatively, jurisdictions could choose to first undertake a more detailed assessment of risks in each sector. Instructions for completing detailed sectoral assessments are provided below. A new spreadsheet should be developed for each sector that is analysed. Jurisdictions should aim to cover financial institutions, DNFBPs and other high-risk sectors.

Step I: Identifying and Assessing Threats

- Consider the threats identified in Step I. List the threats in the left-hand column of Spreadsheet 4. For the sectoral analysis, a slightly different approach to assessing threats and vulnerabilities is taken. In order to arrive at an overall threat rating, each threat is considered and rated against the following contextual factors: products and services; volume of activity; customers; distribution; and jurisdictions. The spreadsheet gives guidance for providing a rating level for each factor. Room is provided for a short narrative justification.

- As consideration is given to the products and services provided by a sector, jurisdictions should note that some threats may ultimately not be relevant to that sector. For threats that are not applicable to that sector, jurisdictions can exclude the threat from the spreadsheet. It should be noted that a threat should not be removed simply because it has not materialised. Potential threats should be included in this process. The only threats that should be excluded are those that could not possibly occur because the products and services offered by that sector have no relation whatsoever to a particular threat.
- The spreadsheet automatically calculates overall threat as an average. Jurisdictions should nevertheless pay particular attention to threat categories that are rated high.

Step II: Identifying and Assessing Vulnerabilities

- Also in Spreadsheet 4, two categories of vulnerabilities are considered: CPF and other regulatory controls; and operational and other controls. Gaps in controls as well as mitigating factors should be balanced to arrive at a residual rating.
- The spreadsheet gives guidance for providing a rating level for each factor. Room is provided for a short narrative justification.
- The rating for each vulnerability has equal weight and the overall vulnerability rating is the average of both categories of vulnerabilities. The spreadsheet automatically calculates overall vulnerability. Jurisdictions should nevertheless pay particular attention to vulnerability categories that are rated high.

Step III: Identifying and Assessing Consequences

- Annex 5 provides a table of consequence ratings. Consequences are split into the following categories: severe; moderate; and limited. Descriptions for each category are provided as a guide for determining whether the consequence of a threat can be considered severe (3), moderate (2) or limited (1).
- In Spreadsheet 4, for each threat, jurisdictions should analyse consequences with reference to Annex 5.
- Within the spreadsheet cell for consequences, jurisdictions should insert a brief narrative summary of the analysis which justifies the rating level. The cell will be colour coded red (severe), orange (moderate) or yellow (limited), commensurate with the severity of the consequences.

Step IV: Calculating Risk

- The spreadsheet automatically calculates a risk rating per threat as well as an overall sectoral risk rating, which is the average of individual risk ratings. These overall ratings are only calculated for the purpose of summarising the findings in the quick reference table in Spreadsheet 5, described below. Jurisdictions and the private sector should consider the analysis of each threat for each sector, rather than simply relying on the final risk rating that is used only for the purpose of a broad summary of the information.

Option: Depicting Sectoral Assessments in a Table

The table in Spreadsheet 5 is intended as a quick reference table summarising the findings from the Sectoral Risk Workbook (Spreadsheet 4). Jurisdictions should list each sector analysed in order of its risk rating. For each sector, the final sectoral risk rating from Spreadsheet 4 should be inserted. The spreadsheet will then automatically calculate a risk rating per sector category (such as financial institutions). The overall ratings are only calculated for the purpose of summarising the findings of the sectoral risk assessments. Jurisdictions and the private sector should consider the analysis of each threat for each sector, rather than simply relying on the final risk ratings that are used only for the purpose of a broad summary of the information.

To use the findings of the sectoral assessments in the national Risk Assessment Workbook in Spreadsheet 1, jurisdictions should use the more detailed information, data, analysis and findings from the sectoral risk assessment to make an informed qualitative assessment of the sectoral vulnerability level in the national risk assessment.

Troubleshooting

On completing the rapid risk assessment outlined in this guide, a jurisdiction may find that the results are not in line with its preconceived understanding of its PF risk exposure. In this case, a few questions should be considered.

It is possible that a jurisdiction has underestimated or overestimated the presence of PF-related threats and vulnerabilities within its economy or has miscalculated their impact on the economy and society. The risk assessment may thus be helpful in adjusting national perceptions and responses to PF-related risk.

Alternatively, an unexpected result may be the product of an inaccurate or incomplete assessment of threats and vulnerabilities. Jurisdiction-specific threats and vulnerabilities that are not covered in Annexes 3 and 4 should have also been considered and included where necessary.

Finally, it is possible that the consequences of PF activity were not evaluated accurately. Jurisdictions should ensure that all potential impacts have been considered, particularly as they relate to the three contexts identified in this guide, as well as to jurisdiction-specific factors. The consequences of a specific PF activity may not be obvious at first and may require further analysis of potential downstream impacts on the economy and society.

Spreadsheet 1: Risk Assessment Workbook

Threats	Vulnerabilities					
	National Vulnerabilities					
	Political and Social	Economic and Technological	Geographic and Enviromental	Legal and Institutional	Legal Persons and Legal Arrangements	Financial Institutions
3	1	3	3	3	3	2
For example, use of front companies, shell companies or brokers to obtain trade finance products and services or as parties to clean payments (known previous cases)	For example, strong political will to combat CPF; no social factors relevant	For example, existence of significant dual-use goods industry and trade	For example, trade of dual-use goods is conducted with countries of PF diversion	For example, no CPF laws or regulations, supervisory oversight does not consider PF issues	For example, lack of transparency of legal persons and legal arrangements, including ultimate beneficial ownership	For example, banks provide a moderate level of trade finance products, regulatory and operational controls high, however, little CPF-specific awareness
1	1	2	1	1		1
For example, cybercrime, such as hacking accounts to obtain value, largely used by state actors	For example, strong political will to combat cybercrime, no social factors relevant	For example, no known cases of cyber attacks, however, growing regional prevalence	For example, no known concerns	For example, strong cybercrime laws and special cybercrime operational taskforce is highly capable	For example, N/A	For example, no known cases of cyber attacks, financial institutions have strong cybercrime controls

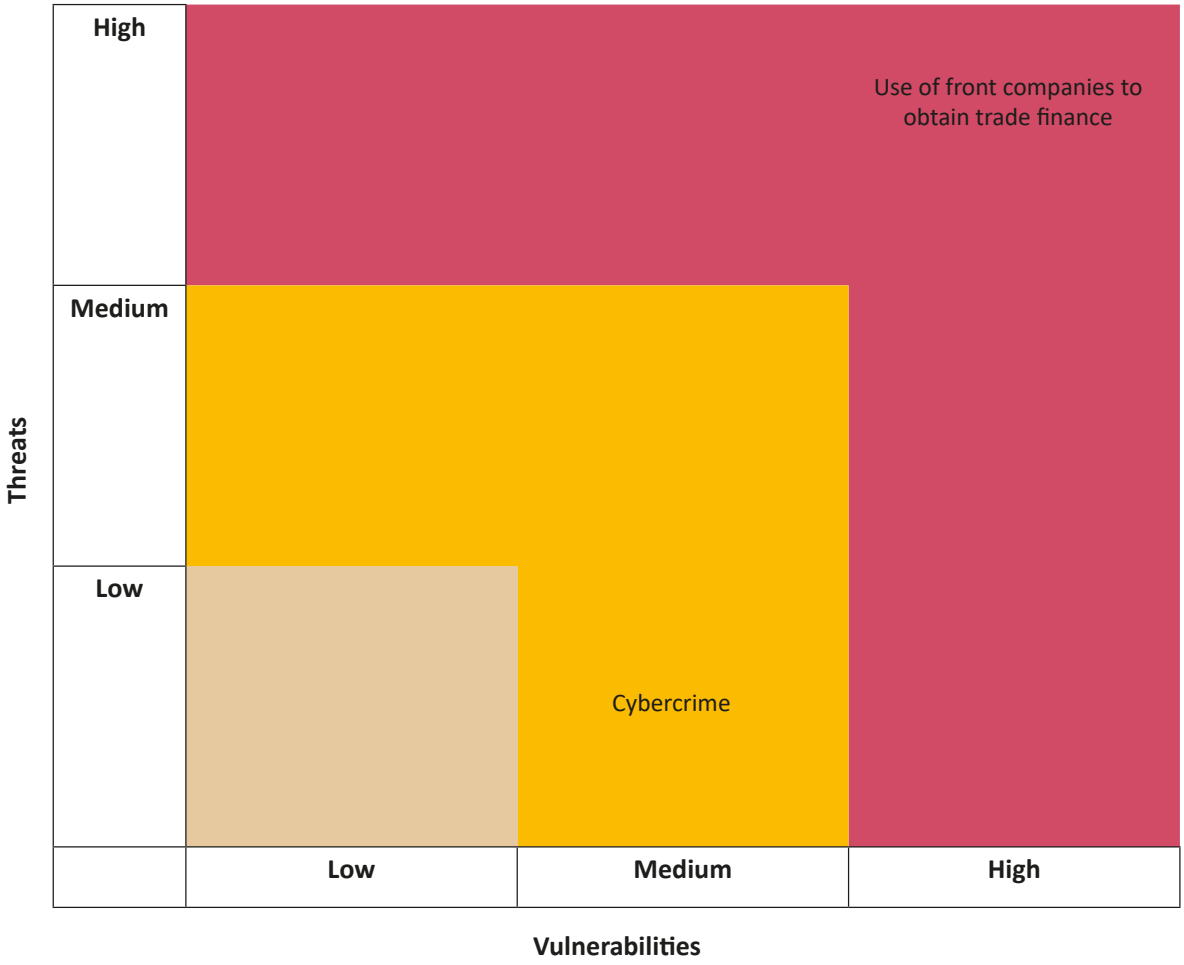
Threat and Vulnerability Rating Levels	Consequences Rating Levels	Mitigation Strategy Options	Colour Coding Guide for Overall Vulnerability and Likelihood
High – 3	Severe	Prevent	2.1–3 High
Medium – 2	Moderate	Mitigate	1.1–2.09 Medium
Low – 1	Limited	Accept	0–1.09 Low

			Likelihood	Consequences	Mitigation Strategies
Sectoral Vulnerabilities		**Overall Vulnerability Rating**			
Designated Non-Financial Businesses and Professions	**Other High-Risk Sectors**				
2	**1**	**2.25**	**2.63**	**3**	**Mitigate**
For example, company service providers may be used in operation of front companies involved in imports/exports	For example, no exposure			For example, products directly related to procurement of sensitive goods, banks are a key industry, severe security and reputational impact	For example, bank supervisor responsible for: legislative amendments required to impose CPF preventative measure; issuance of CPF guidance to banks; CPF focus in future compliance
	1	**1.17**	**1.08**	**2**	**Accept**
For example, N/A	For example, one regional case of hacking of government systems for ransom by a proliferation actor			For example, no direct link to proliferation activity, small attacks limited financial and reputational impact, large attack moderate to severe implications	For example, cybercrime controls are adequate and should be maintained

Instructions on Use of N/A

For some threats, certain vulnerability categories may simply not be relevant. Countries may use N/A and give no rating for that category. It is suggested that this option be cautiously used and only where the final result does not seem an appropriate reflection of the findings. N/A should only be used in relation to vulnerabilities. When N/A is used, the formula in column J calculates the average of the vulnerabilities that are actually rated.

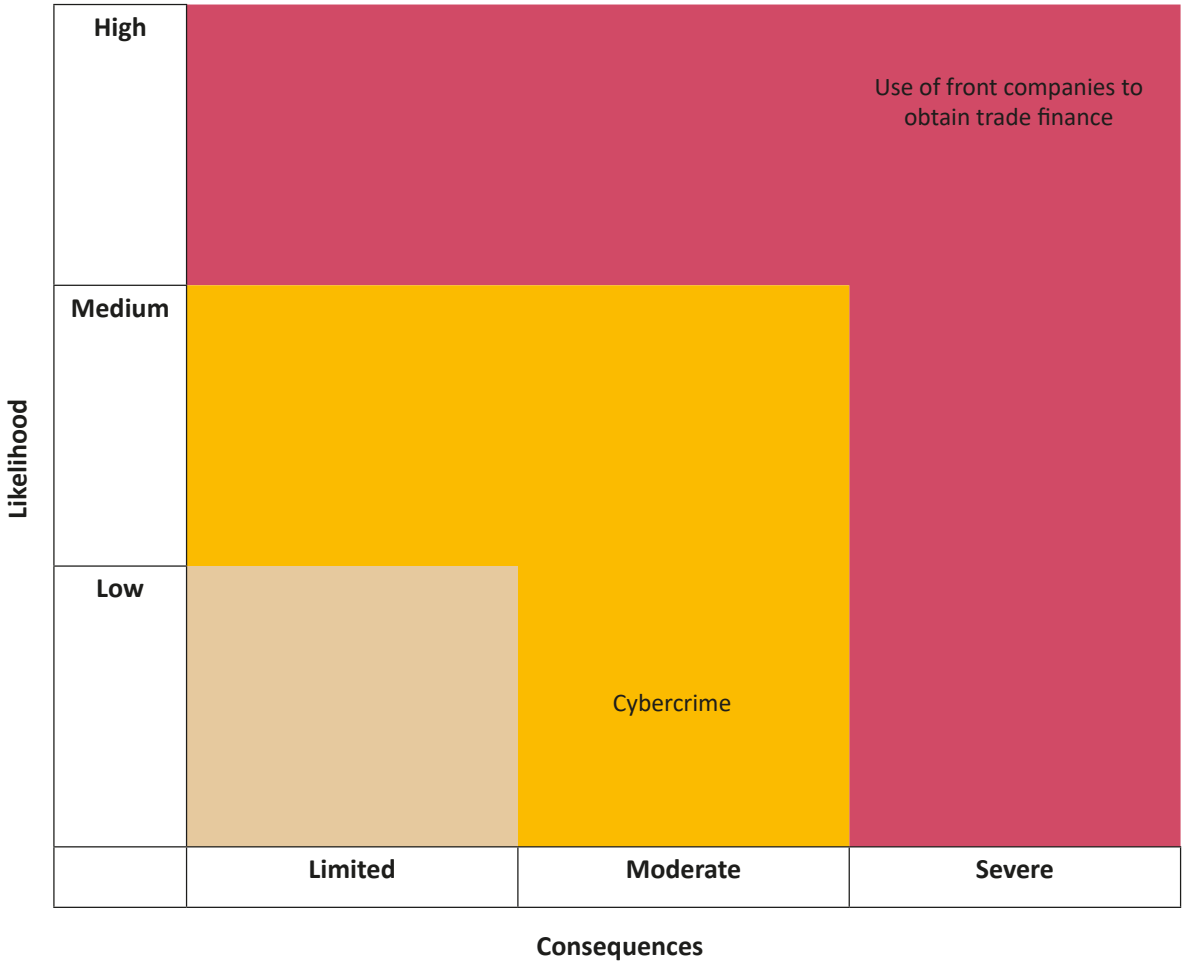
Spreadsheet 2: Likelihood Heat Map



Instructions

This spreadsheet provides an easy visual reference of the likelihood of different risks materialising. For each threat, take the threat rating and plot against the vertical axis. Then take the overall vulnerability rating for that threat and plot against the horizontal axis. Insert the threat into the cell where the two axes meet.

Spreadsheet 3: Risk Heat Map



Instructions

This spreadsheet provides an easy visual reference of overall risk, taking into account consequences. For each threat, take the likelihood rating and plot against the vertical axis. Then take the consequences rating for that threat and plot against the horizontal axis. Insert the threat into the cell where the two axes meet.

Spreadsheet 4: Sectoral Risk Workbook

	Threats					
	Products and Services	**Volume of Activity**	**Customers**	**Distribution Channels**	**Jurisdictions**	**Overall Threat Rating**
For example, use of front companies, shell companies or brokers to obtain trade finance products/services or as parties to clean payments	**3**	**2**	**3**	**3**	**3**	**2.80**
	For example, trade finance, clean payments. Known prior cases	For example, small volume of trade finance, moderate volume of clean payments	For example, companies, businesses	For example, email, internet and via agents or brokers	For example, international: SE Asia, including China	
For example, cybercrime, such as hacking accounts to obtain value, used by state actors	**2**	**1**	**1**	**1**	**1**	**1.20**
	For example, deposit accounts	For example, low total value, and low value of individual accounts	For example, individual	For example, face to face	For example, domestic	

Threat and Vulnerability Rating Levels	Consequences Rating Levels	Mitigation Strategy Options	Colour Coding Guide for Overall Vulnerability and Likelihood
High – 3	Severe	Prevent	2.1–3 High
Medium – 2	Moderate	Mitigate	1.1–2.09 Medium
Low – 1	Limited	Accept	0–1.09 Low

Vulnerabilities			Likelihood	Consequences	Risk Rating	Mitigation Strategies
Counter-Proliferation Financing and Other Regulatory Controls	**Operational and Other Controls**	**Overall Vulnerability Rating**				
2	**3**	**2.50**	**2.65**	**3**	**2.83**	**Mitigate**
For example, products provided by well regulated and supervised banks, no specific CPF preventative measures are required or guidance provided	For example, no CPF operational controls applied, AML/CTF controls are adequate			For example, products directly related to procurement of sensitive goods, banks a key industry, severe security and reputational impact		For example, bank supervisor responsible for: legislative amendments required to impose CPF preventative measures; issuance of CPF guidance to banks; CPF focus in next compliance monitoring. Timeframe: 4–9 months
1	**1**	**1.00**	**1.10**	**1**	**1.05**	**Accept**
For example, strong regulatory controls on banks as deposit-taking institutions	For example, strong anti-cyber attack/hacking operational controls in place; no known cases of cyber			For example, no direct link to proliferation activity, limited financial and reputational impact		For example, continue awareness raising and promotion of anti-cyber attack controls

Instructions

A new spreadsheet should be created for each sector such as banking, insurance etc.

Note

N/A should not be used in this spreadsheet.

Spreadsheet 5: Sectoral Risk Table

Sector	Risk Rating
Financial Institutions	**2.31**
Banking	1.94
Insurance	3.00
Money-transfer services	2.00
Designated Non-Financial Businesses and Professions	**0.00**
Company service providers	
Real-estate agents	
Other High-Risk Sectors	**0.00**
Vessel dealers	

Instructions

This table is intended as a quick reference table summarising the findings from the Sectoral Risk Workbook in Spreadsheet 4. This table needs to be completed manually. For each sector, insert the final sectoral risk rating, which is the average of the risk ratings across all threats. Colour code the rating cell accordingly. The spreadsheet will automatically calculate the rating for financial institutions, DNFBPs and other high-risk sectors. An example is given above.

DISCLAIMER: To access the Excel spreadsheets, please email CPF@rusi.org.