

Institutional Proliferation Finance Risk Assessment Guide

Noémi També

192 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 192 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

June 2023

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

Acknowledgements	iii
Executive Summary	1
Introduction	2
I. Setting the Scene	4
The Role of the Private Sector	4
What are Proliferation and Proliferation Finance?	4
Differences and Similarities Between PF, ML and TF	7
II. PF Risk Assessment Methodology	10
Risk Categories	10
Vulnerability to PF Risk and Next Steps	19
III. Risk Categories and Risk Factors	23
Conclusion	29
About the Author	30

Acknowledgements

The author would like to thank Dimple Rabadia and Mario Menz for their review and helpful comments on an earlier version of this document. Thanks are also due to all those who have generously offered their time to be interviewed for the purpose of developing this guide, as well as to the RUSI Publications team for their editorial work.

Executive Summary

The potential involvement of the private sector in supporting WMD programmes is broad. Proliferators need access to the private sector to generate money, transfer it and purchase dual-use goods. Furthermore, they need to leverage the private sector to trade with companies and, finally, import dual-use goods into their jurisdictions. Thus, while governments have a role to play in setting the regulatory and legal landscape to fight proliferation finance (PF), they need the cooperation of the private sector to achieve an effective global counter-proliferation finance (CPF) framework. Thus the private sector, including financial institutions (FIs), has an essential role in identifying activities that may be suspicious, alerting relevant authorities, freezing assets and implementing financial sanctions.

This guide is designed to provide multi-jurisdictional support to the private sector in identifying activities that may be higher risk, determining the levels of PF risks the sector faces, and developing strategies to tackle such risks. With the private sector conducting institutional risk assessments (RAs), national authorities will obtain an increasingly comprehensive understanding of PF risk at national level. PF RAs will help institutions better understand and define their risk appetite while being aligned to CPF laws and regulations.

The guide documents the ways that FIs should understand the inherent PF risks they face through their customers, products and services offered, jurisdictions operated in and with, transactions, delivery channels used, and cyber threats. It explains how FIs can assess the inherent risk of these categories by considering the likelihood of the risk materialising, alongside the impact of the event should it materialise.

Once the inherent risk is evaluated, the next step is to assess the institution's residual PF risks. This is achieved by assessing the effectiveness of the controls an FI has in place to tackle inherent risks. When the institution completes its PF RA, it can measure its residual risk and hence its vulnerability to PF risk. Institutions can then choose whether to accept this risk or to further mitigate or try to prevent such vulnerabilities and exposures to PF risk.

The guide explains that RAs should be a dynamic exercise, and that FIs need to ensure that emerging and/or future vulnerabilities to PF are identified. Furthermore, the RA should follow a risk-based approach that provides institutions with flexibility in relation to CPF efforts.

Introduction

Proliferators need access to the formal financial system to raise and disguise funds and procure WMDs. To prevent such activities, a number of United Nations Security Council Resolutions (UNSCRs) impose international legal obligations related to proliferation financing (PF): UNSCR 1540 on the non-proliferation of WMDs, UNSCR 2231 on the implementation of the Joint Comprehensive Plan of Action related to Iran, and the expanded requirements of UNSCRs related to North Korea.¹

The Financial Action Task Force (FATF), the global standard-setter for combating money laundering and terrorist financing, included counter-proliferation financing (CPF) standards in its mandate in 2012. Its Guidance on CPF explains that understanding PF risks will ‘positively contribute to a jurisdiction’s ability to prevent persons and entities involved in WMD proliferation from raising, moving and using funds’.²

Since November 2020, FATF member states have been required to undertake national PF risk assessments (RAs). Financial institutions (FIs) and Designated Non-Financial Businesses and Professionals are also required to undertake PF RAs at institutional level to ‘to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks’.³ This requirement is reinforced in the FATF’s 2021 ‘Guidance on Proliferation Financing Risk Assessment and Mitigation’, which states:

Identifying, assessing, and understanding proliferation financing risks on a regular basis is essential in strengthening a country’s or private sector’s ability to prevent designated persons and entities involved in Weapons of Mass Destruction (WMD) proliferation from raising, storing, moving, and using funds, and thus other financial assets. The implementation of [targeted financial sanctions] related to proliferation and its financing is essential for a stronger Counter Proliferation Financing (CPF) regime.⁴

-
1. Anagha Joshi, Emil Dall and Darya Dolzikova, ‘Guide to Conducting a National Proliferation Financing Risk Assessment’, RUSI, May 2019.
 2. 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’, 2018, p. 4.
 3. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations’, 2012, Recommendation 1, p. 10.
 4. FATF, ‘Guidance on Proliferation Financing Risk Assessment and Mitigation’, June 2021, p. 7.

The national implementation of CPF requirements, including PF risk assessments, will be assessed in the next round of mutual evaluations.⁵

This guide is designed to provide multi-jurisdictional support to the private sector in identifying and determining the levels of PF risks it faces, and to develop strategies to tackle such risks, as per FATF Recommendations 1, 2, 7 and 15.⁶ The RA should follow a risk-based approach (RBA) which will provide institutions with flexibility in relation to CPF efforts. An RBA is not a zero-failure policy and does not prevent institutions from engaging with customers or establishing business relationships that may have a higher exposure to PF risk. Rather, it expects institutions to manage and target their efforts in areas that represent higher PF risk.

Chapter I of this guide discusses the role of the private sector in CPF and introduces PF, while Chapter II suggests a possible approach to PF RA, covering risk categories, the inherent risks of such categories, controls to mitigate inherent risks, control effectiveness and residual risk. Chapter III maps risk factors against risk categories and documents how each of these risk factors is relevant to PF. It also documents criteria to determine jurisdictions' exposure to PF risks.

This document should be read in conjunction with RUSI's 'Guide to Conducting a National Proliferation Financing Risk Assessment'.⁷ Together, these guides will help institutions to understand the types of PF threats and vulnerabilities their jurisdictions face.

-
5. FATF, 'Public Statement on Counter Proliferation Financing', press release, 23 October 2020, <<https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html>>, accessed 15 October 2022; see also FATF, 'Procedures for AML/CFT/CPF Mutual Evaluations, Follow-Up and ICRG', April 2022, <<https://www.fatf-gafi.org/content/dam/fatf/documents/methodology/5th-Round-Procedures.pdf>>, accessed 15 October 2022; 'The mutual evaluation ... is a cornerstone of the international framework to combat financial crime. It is a multi-year, peer-review process where the robustness of a jurisdiction's anti-financial crime framework is analysed for both its technical compliance with the FATF Standards and its overall effectiveness at combating financial crime. The product of the [mutual evaluation] is the mutual evaluation report (MER), a highly influential document that sets out the findings of the assessment team'. See Isabella Chase and Maria Sofia Reiser, 'Lessons Learned from the Fourth Round of Mutual Evaluations', RUSI Policy Brief, February 2022, p. 2.
 6. Recommendation 1 requires countries, FIs, 'designated non-financial businesses and professions', and virtual asset service providers to identify, assess and understand their PF risks, and take commensurate action to mitigate these risks. Recommendation 2 requires effective national cooperation and coordination mechanisms to combat PF. Recommendation 7 requires the implementation of UNSCR-based targeted financial sanctions on PF (for instance, asset freezes) and requires ensuring that 'no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the [UNSC] under Chapter VII of the Charter of the United Nations'. Recommendation 15 (revised in June 2021) requires the conducting of a PF risk assessment and mitigation to be established in respect of virtual asset activities and service providers; see FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation'.
 7. Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment'.

I. Setting the Scene

This chapter highlights the importance of the private sector in CPF, provides a definition of proliferation and PF, and outlines the differences and similarities between PF, money laundering (ML) and terrorist financing (TF).

The Role of the Private Sector

To develop WMDs, proliferators need access to the private sector to generate money, transfer it, purchase dual-use goods,⁸ trade with companies and, finally, import dual-use goods to their jurisdictions. Hence the potential involvement of the private sector in supporting WMD programmes is broad. Thus ‘private sector’ in this context not only means FIs, but also ‘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’.⁹

Indeed, while governments have a role to play in setting the regulatory and legal landscape to fight PF, they need the cooperation of the private sector to achieve an effective global CPF framework. The private sector, including FIs, is essential to identifying activities that may be suspicious, alerting relevant authorities, freezing assets and implementing financial sanctions. With the private sector conducting institutional RAs, national authorities will obtain an increasingly comprehensive understanding, at national level, of PF risk.

What are Proliferation and Proliferation Finance?

Proliferation in this context is the ‘manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling

-
8. Dual-use goods are goods, software and/or technologies that can be used for both commercial and military purposes. Such goods include nuclear materials, electronics, computers, sensors and lasers, for example. The export, transit and brokering of dual-use items is controlled to preserve international peace and security and prevent the proliferation of WMD. For more on dual-use goods, see Joshi, Dall and Dolzikova, ‘Guide to Conducting a National Proliferation Financing Risk Assessment’; see also John Varesi, ‘Wassenaar Arrangement Control Lists’, presentation to BIS 2018 Annual Conference on Export Controls and Policy, 2018, <<https://www.bis.doc.gov/documents/bis-annual-conference-2018/2212-multilateral-regime-control-lists-wassenaar-nsg-ag-mtcr-rev-13may2018/file>>, accessed 10 December 2022.
 9. Joshi, Dall and Dolzikova, ‘Guide to Conducting a National Proliferation Financing Risk Assessment’, p. 34.

or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual-use goods used for non-legitimate purposes)'.¹⁰ It includes technology, goods, software, services and expertise.¹¹ 'WMD' refers to nuclear, chemical, radiological or biological weapons,¹² all weapons that can inflict mass casualties and destruction.

Threats of WMDs come both from state groups (for example, Iran, North Korea and Syria) and non-state groups. 'Non-state groups' refers to any individual or entity that is not acting under the lawful order of a state, such as terrorist groups or proliferation networks of brokers, financiers, suppliers or trans-shippers.¹³

Although there is no international consensus on the definition of PF, the FATF defines PF as 'raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)]'.¹⁴

The Centre for a New American Security has identified and documented three stages of PF:

- **Fundraising:** the proliferator sources funds from state budgets, or from illegitimate or legitimate commercial or criminal activities conducted overseas by or on behalf of state actors.
- **Disguising and placing funds into the financial system:** proliferators rely on a network of businesses, front companies, opaque ownership structures and brokers to ensure that everything appears geographically separate from sanctioned countries.
- **Procuring materials and technology using those funds:** the proliferator accesses the international financial system to pay for goods, materials, technology and logistics needed for its WMD programme.¹⁵

10. FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', p. 8.

11. Gibraltar Financial Intelligence Unit, 'Counter Proliferation Financing: Guidance Notes', June 2020, p. 4, <<https://www.gfiu.gov.gi/what-is-proliferation-financing>>, accessed 6 January 2023.

12. The White House, 'National Security Strategy of the United States of America', December 2017, p. 8, <<https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>>, accessed 10 April 2023.

13. For details of non-state groups involved in PF, see *Al-Jazeera*, 'Abdul Qadeer Khan: Nuclear Hero in Pakistan, Villain to the West', 10 October 2021, <<https://www.aljazeera.com/news/2021/10/10/abdul-qadeer-khan-nuclear-hero-in-pakistan-villain-to-the-west>>, accessed 31 January 2023.

14. FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', p. 8.

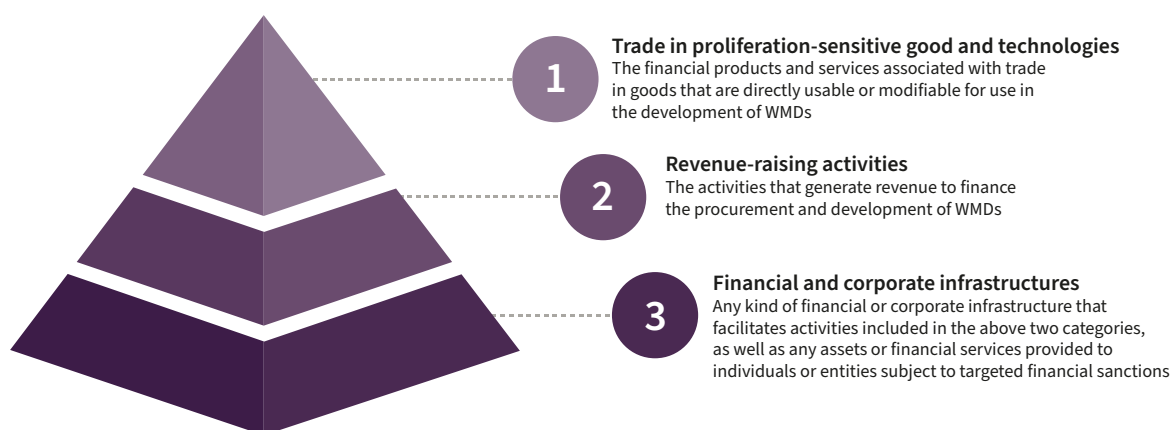
15. Jonathan Brewer, 'The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation', Center for a New American Security, 24 January 2018, p. 4, <<https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation>>, accessed 31 January 2023.

In sum, PF is not limited to the direct financing of WMDs or proliferation-sensitive goods and technologies, but encompasses a wide range of activities. For the purposes of this guide, the three categories of activity that may be considered to be PF and which could be captured within the scope of a PF institutional RA are:

- Financial products and services – such as trade finance, for example – that can directly support the trade in goods that are usable or modifiable for use in the development of WMDs.
- The revenue or assets generated or secured through licit or illicit activities to finance the procurement and development of WMDs and which will need to be placed into and moved through the financial system.
- Financial and corporate networks – such as correspondent banking – that can support the movement of finances and goods used to develop WMDs.¹⁶

Hence, for the purpose of their RAs, FIs should note that PF as defined by the FATF may not articulate the full range of financial activities that may support proliferation. These activities are encapsulated in the three categories of PF that are documented in Figure 1.

Figure 1: Categories of PF



Source: CPF and Sanctions team in RUSI's Centre for Financial Crime and Security Studies.

When conducting a PF risk assessment, institutions should consider the three categories of PF shown in Figure 1 and identify the PF exposure risk their customers can pose to the institution.

16. Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', p. 18.

Differences and Similarities Between PF, ML and TF

Existing CPF literature discusses the differences and similarities between PF, ML and TF. Like TF, PF involves a linear money trail: the end goal is not to secure laundered funds, but to facilitate further illicit activities. Similarly, PF, like ML, will require obfuscation tactics such as concealment of relationships with ultimate beneficial owners (UBOs), complex routing and re-routing of international payments, and concealment of both end use and end users of dual-use goods. Yet, ‘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’.¹⁷

Table 1: PF, ML and TF: A Comparison

	Proliferation Finance	Money Laundering	Terrorism Financing
Purpose	<ul style="list-style-type: none"> To support states and non-state actors in their illicit development of WMD programmes. 	<ul style="list-style-type: none"> To launder proceeds of crime in order to make them look legitimate. 	To finance terrorism, terrorists, and terrorist organisations.
Use of formal financial systems?	<ul style="list-style-type: none"> Yes, as well as cross-border smuggling of cash, gold or other high-value goods by ‘mules’ to support state and non-state proliferation activities. 	<ul style="list-style-type: none"> Yes, as well as informal financial conduits such as <i>hawala</i>, currency exchange houses, cash couriers and smuggling. 	<ul style="list-style-type: none"> Yes, as well as informal financial conduits such as <i>hawala</i>, currency exchange houses, cash couriers and smuggling.
Transactions	<ul style="list-style-type: none"> Transactions appear legitimate and aligned to traditional commercial activity, structured as in ML to hide the nexus with state and non-state actors involved in PF, or to hide the end use or the end user of dual-use goods purchased. 	<ul style="list-style-type: none"> Complex web of transactions, involving the use of funds, real estate, shell or front companies, offshore centres, banking secrecy havens, and complex layers of legal entities (including trusts and foundations, for example). 	<ul style="list-style-type: none"> Multiple methods, including the use of traditional payment methods and banking activities, informal value transfer systems, cash and precious metals and stones smuggling.
Sources of funds	<ul style="list-style-type: none"> Often based on state-sponsored programmes that foment fundraising activities that are traditionally legitimate but considered illegitimate because of the nexus with, for example, Iran and/or North Korea. 	<ul style="list-style-type: none"> Criminal activities. 	<ul style="list-style-type: none"> Illegal as well as legal activities. For example, funds may come from donations, from employment, or from criminal activities.

17. *Ibid.*, p. 5.

	Proliferation Finance	Money Laundering	Terrorism
Size of transactions	• Medium	• Small to large	<i>Small to medium</i>
Activities and sectors	<ul style="list-style-type: none"> • Complex structuring to hide the origin of the funding as well as what funds/assets are ultimately intended to be used for. • Establishment of corporate networks that facilitate but may not be solely involved in PF activities. Ultimate beneficial ownership, connections and control structures are opaque. • Exposure to all sectors. For example, purchase of dual-use items such as engine parts, raising of funds through network of overseas works, exploitation of construction companies or fisheries. 	<ul style="list-style-type: none"> • Complex structuring and web of transactions that may involve using front companies. • These can include, for example, cash-intensive businesses (such as restaurants, convenience stores and nail bars), bearer shares¹⁸ and the use of secrecy havens. • Exposure to all sectors. For example, purchase of luxury items with tainted/criminally obtained funds. 	<ul style="list-style-type: none"> • Multiple, varied methods, for example, formal banking systems, informal value transfer systems, smuggling of valuables (precious metals and stones, antiquities) and cash. • Exposure to all sectors. For example, procurement of weapons (including knives) and vehicles (including car hire businesses).
Money trail	Linear: movement of finances and/or trade in proliferation-sensitive goods to state and non-state actors.	Circular: the funds tend to eventually end up back with the person who generated them once the funds have been sufficiently distanced from the crime.	Linear: funds are used to promote and finance terrorists and their activities, as well as their infrastructure, by raising, storing, moving and using funds. None of these stages need be associated with violence.
Detection	<ul style="list-style-type: none"> • Specially designated entities and/or nationals, jurisdictions of proliferation and/or diversion concern, trade in proliferation-sensitive goods, and known revenue-raising activities for proliferation. 	<ul style="list-style-type: none"> • Suspicious transactions, such as deposits uncharacteristic of customer's wealth or expected activity. 	<ul style="list-style-type: none"> • Suspicious relationships, such as transactions between seemingly unrelated parties.

18. Bearer shares are shares that are not registered and are owned by the individual or entity that holds the physical share.

	Proliferation Finance	Money Laundering	Terrorism Financing
Cross-border activities?	<ul style="list-style-type: none"> • Yes. Likely to involve nationals or legal entities associated with jurisdictions of proliferation and/or diversion concern, as well as countries with weak export control laws or weak enforcement of export control laws. Use of organised or transnational crime networks, particularly their transport corridors and intermediaries in their networks for goods and/or funds. 	<ul style="list-style-type: none"> • Yes. Likely to involve use of smaller correspondent banks located in countries with weak anti-money laundering laws. 	<ul style="list-style-type: none"> • Yes. Likely to involve the use of organised or transnational crime networks, particularly their transport corridors and intermediaries in their networks.

Sources: Author generated, drawing on Jonathan Brewer, 'Study of Typologies of Financing of WMD Proliferation', Project Alpha, Centre for Science and Security Studies, King's College London, 13 October 2017, p. 35, <<https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf>>, accessed 16 November 2022; see also Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', p. 18; Jersey Financial Services Commission, 'Comparison: Terrorism Financing, Money Laundering and Financing the Proliferation of Weapons of Mass Destruction', 14 April 2022, <<https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/>>, accessed 16 November 2022.

II. PF Risk Assessment Methodology

FIs could incorporate PF RAs into their existing ML/TF RAs. This would enable institutions' Financial Crime Prevention (FCP) departments to easily add PF risk categories, risk factors and scoring methodologies to their existing ML/TF RA frameworks. However, some jurisdictions may mandate institutions to have standalone PF RA frameworks. This should be discussed with the relevant supervisory and regulatory authorities.

In addition, while developing an institutional PF RA, it is strongly recommended that FIs consider the PF National Risk Assessments (NRAs) available in their jurisdiction or relevant to their jurisdiction. ML and TF NRAs can be a good source of information, because PF typically does not arise in a vacuum, but leverages existing ML and TF threats and vulnerabilities within a jurisdiction. The UN Panel of Experts (UNPoE) reports on North Korea should also be consulted.

Finally, it should be noted that the matrices documented below are for guidance, and FIs will need to calibrate them to reflect existing scoring methodologies, risk appetite and types of controls, among other things. The RA methodology should be validated by relevant stakeholders across the FI.

Risk Categories

In line with the FATF's guidance for the banking sector,¹⁹ FIs should identify the PF risks they face. These risks may be categorised as follows:

- Customers.
- Products and services offered.
- Jurisdictions operated in and with.
- Transactions.
- Delivery channels used.
- Cyber threats to the systems and software used.²⁰

19. FATF, 'Guidance for a Risk-Based Approach: The Banking Sector', October 2014, p. 13, <<https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>>, accessed 2 February 2023.

20. North Korea engages in malicious cyber activities to collect intelligence, threaten its perceived enemies and raise revenue. Dolzikova and Joshi note that 'North Korea has adapted its operations to take advantage of the now-ubiquitous use of computer-based systems and telecommunications technology by financial

Each of these risk categories will be PF risk-assessed by reviewing their underlying risk factors (this is discussed in more detail in Chapter 3) and evaluating the PF residual risk they represent. This then feeds into FIs' PF RAs. For example, consideration of customer risk factors will typically include 'business activity/occupation/industry' and 'legal structure'. Similarly, products and services risk factors may typically include 'correspondent banking relationships' or 'open account trade'.

Inherent Risks

Inherent risks are the PF risks an institution faces before taking into account the controls and mitigation strategies that have been applied. Once risk categories have been identified, FIs should assess the inherent risk of these categories by considering the likelihood of the risk materialising, alongside the impact of the event should it materialise. This is typically assessed based on five levels of impact, cross-referenced with five levels of likelihood (see Table 2).

For example, an FCP team may, through a review of PF typologies or consultation of the UNPoE reports, identify that in the 'product risk category', open account trade might be used for PF. Thus, the likelihood of this product being used for PF could be classified as 'possible'. The FCP team would then judge the impact to be 'major' should the identified risk materialise and result in sanctions violations, reputational damage and financial losses as a consequence of share price drops and regulatory fines.²¹

Cross-referencing the impact ('major') with the likelihood ('possible') of the product being used for PF (see Table 2) creates the product's inherent PF risk rating of 'medium-high'. The FCP team must then consider whether existing control measures reduce the inherent risk and thus result in a residual risk that is in line with the institution's tolerance or appetite for risk, or whether additional mitigants will need to be put in place to reduce the risk of an event occurring.

institutions, as well as the expanding popularity of cryptocurrencies, to evade sanctions and generate revenue for the regime. Detailed information on North Korean cyber or crypto operations is not widely available, as cyber attacks can be hard to trace and attribute. However, the August 2019 PoE report estimated that, to date, North Korea had illegally acquired \$2 billion through cyber means. Some of the best-known cyber operations which are widely suspected to have been carried out by North Korean actors include the 2016 Bank of Bangladesh heist (which attempted to steal nearly \$1 billion from the bank's account at the Federal Reserve Bank of New York). See Darya Dolzikova and Anagha Joshi, 'The Southern Stratagem: North Korean Proliferation Financing in Southern and Eastern Africa', *RUSI Occasional Papers* (April 2020), p. 30.

21. For example, in 2019, Standard Chartered bank paid \$657 million to the US Department of the Treasury's Office of Foreign Assets Control to resolve sanctions violations, mainly relating to Iran. There were additional sanctions violations relating to Cuba, Sudan, Burma, Syria and Zimbabwe. See US Department of the Treasury, 'U.S. Treasury Department Announces Settlement with Standard Chartered Bank', press release, 9 April 2019, <<https://home.treasury.gov/news/press-releases/sm647>>, accessed 10 May 2023.

Table 2: Inherent Risks

		Impact				
		Insignificant	Minor	Moderate	Major	Severe
		Inherent Risk				
Likelihood	Certain	Medium–Low	Medium–Low	Medium–High	High	Extreme
	Almost certain	Medium–Low	Medium–Low	Medium–High	High	High
	Possible	Low	Medium–Low	Medium–Low	Medium–High	Medium–High
	Unlikely	Low	Low	Medium–Low	Medium–High	Medium–High
	Rare	Low	Low	Low	Medium–Low	Medium–High

Source: Author generated. Adapted from various enterprise risk management frameworks and guides. FIs may adapt this table to fit their internal processes.

Open Account Trade and Proliferation Finance

As global trade in goods and services has expanded over the years, so has open account trade:

Open account terms [are where] the buyer and seller agree to the terms of the contract and goods are delivered to the buyer followed by a clean or netting payment through the banking system. Under such open account terms, unless the FI is providing credit facilities, the FI's involvement will be limited to the clean payment and it will not generally be aware of the underlying reason for the payment. As the FI has no visibility of the transaction, it is not able to carry out anything other than the standard anti-money laundering (AML) and sanctions screening on the clean or netting payment.

In sum, open account trade enables goods to be shipped and delivered before payment is due, with the exporter sending shipping documents directly to the exporter. This process does not involve the bank. As a result, while the bank has access to the customer due diligence (CDD) files of its direct customers – reviewing information regarding beneficial owners, business activities and past transactions – it does not have key information relating to the goods being shipped, the identity and jurisdiction of either buyer or seller, the vessel name, the shipping company, or the shipping routes. This is also the case for intermediary banks that only have payer and payee information in a wire payment message. The importer and exporter of goods will only use a bank as a means of transmitting money.

FIs offering open account trade may not:

- Understand whether the merchandise being shipped consists of dual-use goods.
- Know who is transporting the goods.
- Know whether the ship or individuals involved in the trade are sanctioned.

- Know whether the shipment is stopping in a sanctioned or high-risk jurisdiction.

As such, although the importer and/or exporter may be proliferators, transactions may not be flagged as suspicious and might appear to be legitimate.

Unlike open account trade, letters of credit require banks to obtain documentation, including details of counterparties, consignees and shipping information. This enables FIs to use this information to conduct thorough due diligence, extract information and screen the transaction and associated data points. For example, shipments financed with a documentary letter of credit allow banks financing the transaction to have access to information relating to the goods being shipped, the identity and jurisdiction of both buyer and seller, the vessel name and the shipping company, as well as shipping routes.

Note: A letter of credit is a bank's guarantee that the correct payment will be received within the agreed timeframe. If the paying entity cannot make the payment to the selling entity, the bank agrees to pay the full amount.

Source: Wolfsberg Group, ICC and BAFT, 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles', 2017, p. 7, <https://www.icc-france.fr/wp-content/uploads/2021/04/TradeFinance_icc-wolfsberg-trade-finance-principless-2017.pdf>, accessed 30 May 2023.

Identifying Controls and Assessing the Effectiveness of Controls

Once the inherent risk has been evaluated, the next step is to assess the institution's residual PF risks, i.e., risks that remain after controls and mitigation strategies to tackle inherent risks have been applied. It should be noted that controls in place to mitigate ML and TF risks also help FIs mitigate the PF risks they may face.

Indeed, at onboarding and as part of the ongoing business relationship, FIs traditionally obtain and maintain customer information to understand, assess and document ML and TF risks. The following information should also be gathered to understand, assess and document PF risks:

- Who the customer is, and the identities of UBOs, significant controllers, intermediary entities within an ownership chain, and signatories (to establish whether there are any links to a sanctioned party or sanctioned jurisdiction).
- What the customer does, which sector they operate in, and the nature of their business.
- The identity of the parties the customer is doing business with, along with any other relevant connected parties.

- Whether the customer deals in dual-use goods, nuclear, research or military goods.
- The purpose of the business relationship.
- The expected activity on the account.

In addition, understanding whether the customer is purchasing, selling, importing or exporting dual-use or other controlled goods (nuclear or military) is essential to CPF. More specifically, institutions need to know:

- Whether the customer is licensed to trade in such goods.
- Whether there is a link to a sanctioned jurisdiction or to an area that borders a sanctioned jurisdiction.
- Whether trades involve the transshipment of goods.

Similarly, FIs will screen new and existing customers (as well as related parties and/or counterparties) against sanctions lists, adverse media and watchlists in order to identify any links to sanctioned entities or nationals, or Politically Exposed Persons (PEPs). Any alerts and true matches should be managed as per the FI's existing escalation processes. Customers (and relevant related parties) should be subject to ongoing screening throughout their relationship or the lifecycle of the trade. In addition to 'name screening', screening on all cross-border payments (inbound and outbound) must be undertaken to ensure compliance with relevant sanctions regulations.

Furthermore, FIs' transaction monitoring tools should include typologies indicative of PF activities. Where such transactions are identified, an investigation must be undertaken as per the FI's existing processes to identify sanctions evasion and/or PF. Any suspicion arising will need to be reported to relevant sanctions authorities as well as to financial intelligence units, depending on jurisdictional requirements.

Finally, all members of staff should complete relevant training appropriate to their role and jurisdictions. More specifically, staff who perform customer onboarding, risk assessments, ongoing monitoring, or name and transaction screening should be given targeted training on PF risks, typologies and risk indicators.

In summary, existing controls that support FIs in mitigating PF risks include:

- Governance arrangements.
- Management information.
- CPF policies.
- CDD/Know Your Customer (KYC) arrangements (including ongoing due diligence and enhanced due diligence).

- Know Your Employee checks.
- Customer risk scoring.
- PEP, sanctions and watchlist screening.
- Ability to freeze assets of designated entities and/or nationals.
- Transaction monitoring.
- Independent controls testing and quality assurance of existing systems and controls.
- New product approval processes, including, where applicable, committee decisions.
- Staff training.
- Restrictions on operating in certain markets.
- Suspicious activity reporting.
- Business-wide RAs.

The above list is not exhaustive, and there are additional elements that should be introduced so as to specifically target PF. These are:

- Calibrating transaction monitoring tools to reflect existing PF scenarios.²²
- Reviewing UNPoE reports for North Korea and Iran to identify natural persons and entities associated with PF, and adding these to internal watchlists.
- Reviewing UNPoE reports for North Korea and Iran to identify emerging PF typologies and trends.²³
- Providing export/import controls training to employees.
- Providing dual-use goods training to employees.

The effectiveness of controls is determined by two considerations: whether the control is well designed to mitigate inherent risks, and whether the control is being adequately operated to mitigate those risks. The combined design effectiveness and operating effectiveness of a control indicates whether the control is ineffective, partially effective, effective or highly effective (see Table 3). The determination as to whether controls are designed and operated effectively should be based on control testing.

22. For more on PF typologies, see Brewer, 'Study of Typologies of Financing of WMD Proliferation'; FATF, 'FATF Guidance on Counter Proliferation Financing'.

23. Security Council Report, 'UN Documents for DPRK (North Korea): Sanctions Committee Documents', <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=DPRK%20%28North%20Korea%29&cbtype=dprk-north-korea>, accessed 18 May 2023; Security Council Report, 'UN Documents for Iran: Sanctions Committee Documents', <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=Iran&cbtype=i>, accessed 5 January 2023.

Table 3: Control Effectiveness

		Operating Effectiveness			
		Ineffective	Partially effective	Effective	Highly effective
Design Effectiveness	Ineffective	Ineffective	Ineffective	Ineffective	Ineffective
	Partially effective	Ineffective	Ineffective	Partially effective	Effective
	Effective	Ineffective	Partially effective	Effective	Effective
	Highly effective	Ineffective	Effective	Effective	Highly effective

Source: Author generated. Adapted from various enterprise risk management frameworks and guides. FIs may adapt this table to fit their internal processes.

For example, in the case of the above example, where an open account trade was assessed as having a medium–high inherent risk, the FI would assess the effectiveness of the controls in place to mitigate the risks of the products involved being misused for PF purposes.

The controls and risk-mitigation measures that are typically used to reduce the likelihood and impact of PF risk associated with open account finance include:

- Due diligence both on customers and other relevant parties to transactions to understand the customer profile (including expected activity) and identify unusual and potentially suspicious activity.
- Screening names, entities, persons, suppliers and countries against official sanctions and prohibited persons lists to identify sanctions or other concerns with respect to a relationship or transaction.
- Transaction monitoring of completed or live transactions to detect the presence of unusual or potentially suspicious activity aligned to known PF typologies.²⁴

24. Wolfsberg Group, ICC and BAFT, ‘The Wolfsberg Group, ICC and BAFT Trade Finance Principles’, p. 70.

Chinpo Shipping Case Study

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

In 2014, the UNSC added OMM to the list of Specially Designated Entities for facilitating the July 2013 shipment of conventional arms from Cuba to North Korea. The shipment was on the *Chong Chon Gang* vessel, where the following items were found hidden under bags of sugar: two MiG-21 aircraft and engines; six trailers of SA-2 and SA-3 surface-to-air missiles; ammunition, rifles and night-vision equipment; and a total of 240 tons of military equipment.

During the trial in Singapore of Chinpo's founder, Tan Cheng Hoe, the prosecution's expert witness indicated that such military equipment could be used to protect North Korea's nuclear sites. In addition, the court confirmed that OMM had instructed Chinpo Shipping to pay the vessel's Panama Canal fees (\$54,270 and \$72,017 for outbound and inbound passages) on its behalf. To conceal the prior activities of *Chong Chon Gang*, OMM had also instructed Chinpo to falsely document the vessel name – as *South Hill 2* – in wire transfer documentation.

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

The Bank of China, which provided Chinpo with banking services, failed to implement robust KYC and CDD checks. It did not identify either Chinpo's close ties with North Koreans in Singapore, or its direct ties with North Korea. This included failing to identify, for instance, that Chinpo shared its address with the North Korean embassy in Singapore.

In addition, Singapore's District Court found that the bank may have failed to perform adequate transaction monitoring – which may have been a consequence of its poor KYC and CDD checks. For example, Chinpo's freight decreased from 57 to 4 vessels between 2010 and 2013. However, Chinpo's outward remittances totalled more than \$40 million between 2009 and 2013. Such transactions are inconsistent with the profile of such a shipping agent. It is unclear whether the Bank of China's ongoing transaction monitoring generated alerts, and whether analysts investigated the transactions to establish whether they were legitimate.

Sources: James Martin Center for Nonproliferation Studies, 'Chinpo Shipping Case Study', November 2017, <<http://www.nonproliferation.org/wp-content/uploads/2017/12/op35-presentation-chinpo-shipping-case.pdf>>, accessed 10 May 2023; Colum Lynch, 'U.N. Panel: North Korea Used Chinese Bank to Evade Nuclear Sanctions', Foreign Policy, 7 March 2016.

Residual Risks: Combining Inherent Risk and Control Effectiveness Scores

If all three controls are assessed as effective, then overlaying this assessment with an inherent risk rating of medium–high would result in a residual risk score of medium–low (see Table 4). It is important to note that such frameworks need to be flexible, and that the expertise and knowledge of the FCP team feeds into such evaluations. FCP teams should apply a risk-based approach. For example, in a case where the controls are evaluated as effective, the FCP team may estimate that the residual risk should be medium–high, owing to elements that may not have been qualitatively or quantitatively captured in the assessment. Hence, 'technical assessments performed by risk analysts can be overridden, enabling analysts to use heuristic techniques often influenced by "gut instinct", or sensitivity to a particular topic or ethics, when assessing certain risks associated with a particular event'.²⁵ Such factors need to be clearly documented and articulated, and should be reviewed and assessed via adequate governance arrangements (for example, risk and audit committees) to justify decisions.

25. Noémi També Bearpark, *Deconstructing Money Laundering Risk: De-Risking, the Risk-Based Approach and Risk Communication* (New York, NY: Springer, 2022), p. 23.

Table 4: Residual Risk

		Inherent Risk				
		Low	Medium-Low	Medium-High	High	Extreme
		Residual Risk				
Control Effectiveness	Ineffective	Low	Medium-Low	Medium-High	High	Extreme
	Partially effective	Low	Medium-Low	Medium-High	High	Extreme
	Effective	Minor	Low	Medium-Low	Medium-High	High
	Highly effective	Minor	Minor	Low	Medium-Low	Medium-High

Source: Author generated. Adapted from various enterprise risk management frameworks and guides. FIs may adapt this table to fit their internal processes.

Vulnerability to PF Risk and Next Steps

Once institutions have completed their PF RA, they can measure their residual risk, and hence their vulnerability to PF risk (in terms of potential non-compliance with regulations or too much risk exposure, for instance). Institutions can subsequently choose whether to accept, further mitigate or prevent such vulnerabilities and exposures to PF risk.

Institutions may want to strengthen and enhance existing controls to tackle the highest-rated inherent risks identified ('extreme' in Table 2), and modify other controls deemed to be ineffective or partially ineffective. Operating under a risk-based approach, institutions should aim to target the highest-rated identified inherent risks. In this spirit, institutions may also decide to review certain controls that may be seen as disproportionate in terms of mitigating lower inherent risks.

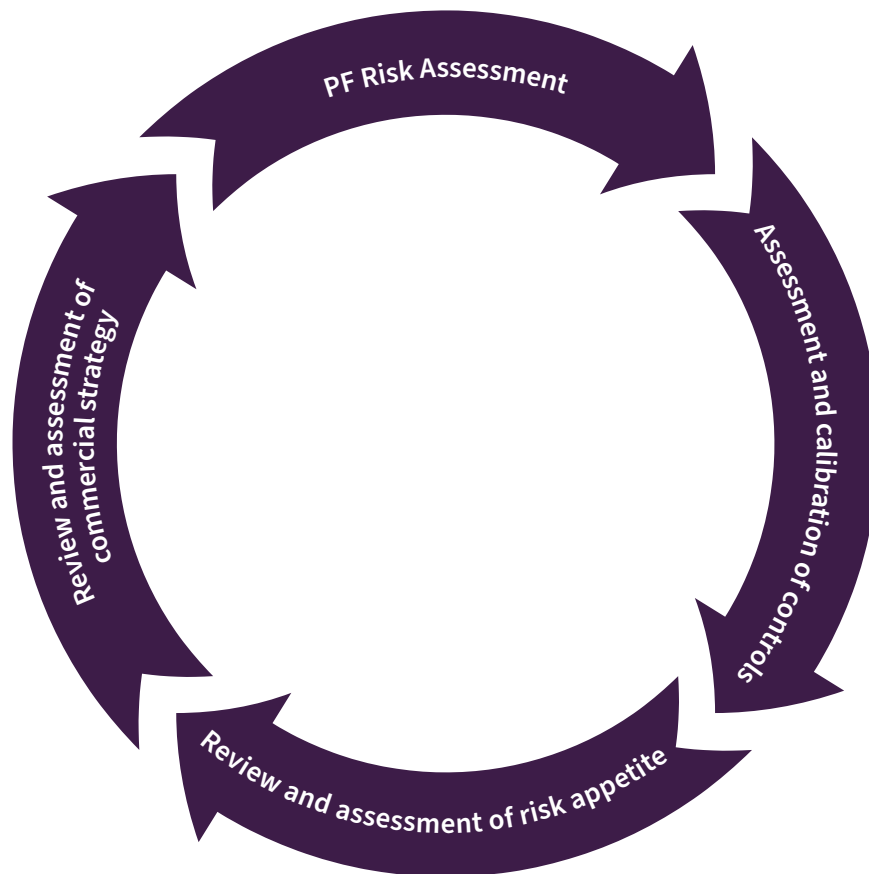
Furthermore, the PF RA will help institutions better understand and define their risk appetite while being aligned to CPF laws and regulations. Institutions may therefore decide to review and assess their existing commercial strategies.

This may result in the institution:

- Stopping certain activities in certain jurisdictions.
- Terminating certain business relationships.
- Launching new commercial ventures.
- Developing governance and controls arrangements to strengthen alignment to risk appetite.

RA should be a dynamic exercise, and the approaches outlined above can feed into a new PF RA to ensure that emerging and/or future vulnerabilities to PF are identified. This is illustrated in Figure 2 below.

Figure 2: The RA Cycle



Source: Author generated. Adapted from various risk assessment frameworks and guides.

Understanding Inherent and Residual PF Risks in Practice

The case of Corman Construction and Commerce (CC&C) illustrates the inherent PF risks of banking customers who display elevated PF risk factors. The March 2021 UNPoE report indicates that CC&C is a front company for the Mansudae Overseas Project Group of Companies sanctioned by the UN in 2017. The company was registered as a Senegalese company with Choe Song Chol, a known North Korean national, identified in the company's legal status documents as the controlling person. The UNPoE report indicates that contracts and financial transactions show that CC&C managed several projects in Dakar in Senegal.

In addition, it banked with two different financial institutions and regularly made payments to the North Korean embassy. Both CC&C and the FIs that provided CC&C with banking services violated UN sanctions by supporting programmes of WMDs: the former through revenue-raising activities, and the latter by providing financial services and infrastructure (see Figure 1).

In addition, in September 2019 a journalistic investigation found that a minimum of 31 North Korean nationals were working at the firm. This was a potential breach of UN sanctions that prohibit UN member states from allowing new North Korean workers into their jurisdictions, and which required any existing North Korean workers to be expelled from UN member states' territories by the end of 2019.

It is not possible to establish from the UNPoE whether the FIs that provided financial services to CC&C knowingly violated UN sanctions. However, the following facts could have indicated that CC&C has elevated PF risk factors:

- Geographic risk:
 - The company operates in Senegal, a jurisdiction that was rated as non-compliant with Recommendation 6 during the 2018 FATF mutual evaluation process.
 - Senegal has historical ties with North Korea, with diplomatic ties since 1972. In addition, Mansudae Overseas Projects, a North Korean company, built the African Renaissance monument in Dakar.
- Customer risk:
 - The company is controlled by a North Korean national.
 - The legal entity operates in the construction industry, a sector that poses elevated PF risk, as it can be leveraged to raise revenue through labour exploitation and profits from payment of contracts, which form part of North Korea's revenue-raising activities.

- Transaction risk:
 - The company sends revenue to the embassy of North Korea.

With these inherent risks identified, it might have been expected that the following controls would have been applied:

- An employee training programme to ensure there is robust CPF awareness within the FI.
- A CDD and KYC framework to establish the UBO and/or other controlling persons.
- A CDD and KYC framework to identify that CC&C is a front company for a sanctioned legal entity.
- A CDD and KYC framework to identify and assess the geographic spread of CC&C's activities and establish the purpose and nature of the account, including expected activities.
- Sanctions and adverse media screening to establish whether there is a match with sanctions lists.
- Transaction monitoring to identify illicit transactions, such as the ones made to the North Korean embassy.

Adequate implementation of these controls would have indicated that:

- The provision of financial services and/or products to CC&C is a clear violation of UN sanctions.
- The residual PF risks of providing banking to such a customer are therefore severe.
- To prevent exposure to severe PF risks, the customer should not be taken on.

Sources: UN Security Council (UNSC), 'Security Council 1718 Sanctions Committee Amends 44 Entries on its Sanctions List', SC/14983, press release, 26 July 2022, <<https://press.un.org/en/2022/sc14983.doc.htm>>, accessed 10 May 2023; UNSC, 'UN Panel of Experts Report', S/2021/211, 4 March 2021, pp. 51, 53, 322, <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf>, accessed 13 December 2022; Council of the European Union, 'Council Directive 2011/64/EU of 11 August 2017', Official Journal of the European Union (C 2016/849, 11 August 2017), <[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XC0811\(11\)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XC0811(11))>, accessed 13 December 2022; Ham Ji-ha and Kim Seon-myung, 'Despite UN Sanctions, North Koreans at Work in Senegal', VOA, 24 September 2019, <https://www.voanews.com/a/africa_despite-un-sanctions-north-koreans-work-senegal/6176412.html>, accessed 10 May 2023; Inter-Governmental Action Group against Money Laundering in West Africa, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Senegal: Second Round Mutual Evaluation Report', May 2018, <<https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-senegal-2018.html>>, accessed 10 May 2023.

III. Risk Categories and Risk Factors

Building on a fuller understanding of an RA methodology, Table 5 sets out the five PF risk categories whose inherent PF risks must be considered: customers; geographic exposure; products, services and transactions; delivery channels; and cybercrime.

There may be other risk categories that an institution wishes to add to ensure that all the risks it faces are adequately captured. Fraud, for example, may be identified as a revenue-raising method used by North Korea or Iran in a particular jurisdiction.

FIs will then need to consider each risk against the ‘risk factors’ (shown in the second column of Table 5) relevant to their business activities. The prominence of specific risk factors will vary across institutions. A small insurance company, for example, would not have the same business exposure as an international FI, or a virtual asset service provider. Risk factors will vary depending on the type of markets the institution services, its customers, the products it offers, delivery channels and platforms used. Note that Table 5 does not offer an exhaustive list of risk factors. The third column in Table 5 maps risk factors against the corresponding categories of PF activities illustrated in Figure 1 of this guide.

Table 6 provides a guide to the criteria to consider when evaluating the PF risks that jurisdictions may be exposed to.

Table 5: PF Risk Categories and Risk Factors

Risk Categories	Risk Factors	Potential Acts of Proliferation Finance
Customer risk (including legal entity type)	<ul style="list-style-type: none"> • Residency and nationality • Complex ownership structure involving several jurisdiction and entity types • Use of international corporate vehicles • Virtual currency providers or customers investing via such providers • Companies with nominee shareholders 	<ul style="list-style-type: none"> • Use of a country's vulnerability to PF as a result of historical legacy, poor regulatory and legal framework, social and political factors, or economic and technological factors. • Jurisdictions providing accounts to, or otherwise facilitating, financial activities of proliferation states. • Use of local branches of banks and financial institutions based in countries of proliferation concern. • Use of complex structures (such as multi-layered trusts, foundations), nominee directors and/or shareholders to hide a UBO or significant controller and their association with sanctioned entities or jurisdictions. • Use of cryptocurrencies to avoid the formal financial system. • Establishment of corporate networks that facilitate but may not be solely involved in PF activities. Ultimate beneficial ownership, connections and control structures are opaque. • Use of front companies, shell companies or brokers to obtain trade finance products and services, or as parties to clean payments. • See Table 6 for more on the criteria that should be considered when assessing a jurisdiction's vulnerability.
Business activity/ occupation/ industry of customer	<ul style="list-style-type: none"> • Money services businesses • Manufacturing • Agriculture • Research • Suppliers, buyers and trading partners in WMD technology/dual-use goods/nuclear/defence industries • Maritime/shipping industry • Providers of shadow banking • Money-exchange businesses • Embassies and consulates • PEPs • Corporate service providers and intermediaries 	<ul style="list-style-type: none"> • Use of universities or research centres to procure dual-use goods and/or for payment of funds, including Iranian and Syrian institutions. • 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. • 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 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 activities²⁶ as well as facilitating financial products or services related to trade in goods. • Use of PEPs who are vulnerable to corruption and may leverage their position of power to access land rights, mining rights or exploit businesses (such as fisheries) to raise revenue for sanctioned countries and actors. • Use of professional intermediaries and corporate service providers to mask parties to transactions and end users associated with PF.

26. This guide does not offer a comprehensive list of activities that North Korean and Iranian nationals and entities have been reported to – or could theoretically – engage in to raise funds. There are several well-established or emerging patterns of fundraising activities, such as cybercrime and abuse of cryptocurrencies, provision of military assistance, construction of statues and monuments, illegal wildlife trade, and overseas labour across different types of industries. Revenue-raising activities will differ across

Risk Categories	Risk Factors	Potential Acts of Proliferation Finance
Geographic risk	<ul style="list-style-type: none"> • Jurisdictions known for diversion • High-risk jurisdictions and high-risk third countries • Countries subject to sanctions or embargos; countries identified as lacking appropriate AML/CFT laws and regulations • Offshore financial centres and non-cooperative tax jurisdictions • Jurisdictions identified as having significant levels of corruption or organised crime, or other criminal activity • Jurisdictions identified as providing funding or support to terrorist activities 	<ul style="list-style-type: none"> • Use of local branches of banks and financial institutions based in countries of proliferation concern. • Use of third countries with weak CPF frameworks or elevated risks of corruption and bribery to channel financial transactions related to dual-use goods. • Use of offshore jurisdictions that offer the possibility of easily creating front and/or shell companies to disguise UBOs and/or end users associated with WMD programmes. • Use of trade or other economic relations with countries with links or significant exposure to a proliferating country. Often facilitated by a complex corporate network.
Products, services and transactions risk	<ul style="list-style-type: none"> • Open account payments/ letters of credit • International payments • Shadow banking • Correspondent banking relationships • Foreign accounts • Provision of precious metals and stones services • Provision of maritime insurance products • Provision of virtual assets trading 	<ul style="list-style-type: none"> • Use of trade finance products and services and clean payment services in procurement of proliferation-sensitive goods. • Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance. • Use of international wire payments with limited oversight of CDD performed on payers and payees. • Use of shadow banking, characterised by limited disclosure of the value and nature of assets. • Use of correspondent banking to transfer value across the international financial system to and from proliferators to pay for dual-use goods, or to transfer proceeds of revenue-raising activities. • Use of foreign-denominated accounts to make international payments for dual-use goods, or to transfer proceeds of revenue-raising activities. • Purchase or sale of precious metals and/or stones to transfer value across jurisdictions or to raise revenue to support WMD programmes. • Provision of maritime insurance to shipping companies involved in sanctions violations. • Use of cryptocurrencies to leverage anonymity and avoid the formal financial system and associated controls that may more easily identify sanctions violation.

jurisdictions, as they depend on jurisdictions' specific vulnerabilities. See Dolzikova and Joshi, 'The Southern Stratagem'.

Risk Categories	Risk Factors	Potential Acts of Proliferation Finance
Delivery channel risk	<ul style="list-style-type: none"> • Face-to-face origination • Non-face-to-face origination 	<ul style="list-style-type: none"> • Use of non-face-to-face account opening facilities to mask the identity of the UBO. • Services that are capable of concealing beneficial ownership from competent authorities (for example, nominee director risk).
Cybercrime risk	<ul style="list-style-type: none"> • Hacking • Ransomware • IT contractors with access to sensitive material 	<ul style="list-style-type: none"> • Hacking accounts to obtain value, largely used by state actors. • Use of systems with malicious software that freezes or encrypts devices that are unblocked after ransom is paid to state actors. • Use of criminal IT employees embedded in organisations involved in subject matter potentially related to WMDs or dual-use goods training or development.

Source: Author generated. The ‘Potential Acts of Proliferation Finance’ column is based on Joshi, Dall and Dolzikova, ‘Guide to Conducting a National Proliferation Financing Risk Assessment’; see also Brewer, ‘Study of Typologies of Financing of WMD Proliferation’.

Table 6: Country Risk Scoring

Scoring	Description
Restricted	<ul style="list-style-type: none"> • Country is subject to UN sanctions (North Korea and Iran). • Country is subject to other sanctions (for example, China, Syria, Russia and Pakistan). • Country has significant corporate/trade network of PF state/ties with sanctioned country/countries. • Country offers shipping flags of convenience or passports of convenience. • Country is on the FATF’s ‘high-risk country list’ and/or the FATF’s ‘grey list’. • Intelligence suggests that country may consider developing nuclear capability through illicit procurement.
Medium–High	<ul style="list-style-type: none"> • Known country of diversion, country scored with a low level of effectiveness in mutual evaluation reports, including on Immediate Outcome 11.²⁷ • Geographical proximity to a proliferating country. • Country named by the UNPoE/Office of Foreign Assets Control/mainstream media as either trading with sanctioned states or lacking sufficient visibility/transparency on trade patterns. • Country does not respond to UNPoE enquiries. • Country outside the Nuclear Non-Proliferation Treaty and/or country is maintaining or improving, or is expected to maintain or improve, its nuclear capabilities. • Proliferating state has diplomatic presence in the country.
Medium–Low	<ul style="list-style-type: none"> • Country neighbours a proliferating state. • Country has a large diaspora from a state of proliferation concern. • Country hosts a financial, trade centre, or transshipment hub that is attractive to proliferation financiers. • The jurisdiction is home to a manufacturing sector that produces goods controlled by international supplier regimes related to WMD and/or their delivery vehicles. • The jurisdiction has weak controls and/or enforcements in relation to ML, TF and PF.

27. ‘Immediate outcomes’ assess to what extent a country meets the objectives of FATF standards. Immediate Outcome 11 requires preventing persons and entities involved in WMD proliferation from raising, moving and using funds. For more information, see FATF, ‘Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems’, updated October 2021, <<https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>>, accessed 10 May 2023.

Scoring	Description
Low	<ul style="list-style-type: none"> • Country has strong regulation and enforcement mechanisms that are recognised by the FATF, and/or are not assessed in any of the risk category reports, and/or country is not on FATF lists. • Country has robust company registry system. • Country has performed national risk assessment (NRA) for ML/TF/PF (note that this is a FATF requirement and may be an indicator of low risk) and has identified and implemented mitigating controls to tackle high-risk issues raised in NRAs.

Source: Author generated, drawing on Jonathan Brewer, ‘The Financing of WMD Proliferation: Conducting Risk Assessments’, Center for New American Security, 30 October 2018.

Case Study: Congo Aconde SARL

In 2018, two North Korean businessmen, Pak Hwa Song and Hwang Kil Su, formed Congo Aconde SARL, a construction services firm in the Democratic Republic of the Congo (DRC). They opened a foreign-currency-denominated corporate bank account at Afriland First Bank. The Sentry, an investigative and policy organisation, identified ‘the Paris branch of BMCE Bank International, headquartered in London, as the correspondent bank designated to process US dollar and euro transactions for Congo Aconde’s account at Afriland First Bank’.

The company delivered construction projects in the DRC. One project involved erecting statues, a North Korean revenue-raising activity prohibited by the UN. Under UNSCR 2321 (2016), member states cannot directly or indirectly procure statues from North Korean individuals and entities. In addition, North Korean citizens are barred from supplying, selling or transferring statues.

The 2021 UNPoE Report on North Korea documents that Pak Hwa Song and Hwang Kil Su provided North Korean passports during the process of company incorporation. In addition, their passports indicated that they were employees of the Ministry of Foreign Affairs on official government business. Furthermore, their nationalities were recorded as ‘DPR Korea’ or ‘Korean’. Finally, a residential address was listed in Congo Aconde’s letters of incorporation.

In response to the Panel’s inquiry about the financial activities of Congo Aconde SARL:

one financial institution described its due diligence procedures, which included cross-referencing names and passport numbers against United Nations designation lists. The financial institution explained that Messrs. Pak Hwa Song and Hwang Kil Su are not designated entities. They also provided the Panel with documentation that the two men had signed an acknowledgment that the accounts would not be used for prohibited activities, inter alia, sanctions evasion.

The controls that would have been expected to be applied by both Afriland First Bank and BMCE Bank International are:

- An employee training programme to ensure there is robust CPF awareness within the FI.
- A robust CDD and KYC framework to establish that Pak's and Hwang's nationalities were North Korean.
- A CDD and KYC framework to identify that Congo Aconde SARL is controlled by North Korean nationals and therefore presents an elevated risk of being a front company for a sanctioned legal entity.
- Sanctions and adverse media screening to establish whether there is a match with sanctions lists.
- When providing correspondent banking services, enhanced due diligence on transactions of institutions operating in certain jurisdictions.
- When providing correspondent banking services, review and assessment of respondent banks's AML/CTF/CPF framework.

Sources: The Sentry, 'Overt Affairs: How North Korean Businessmen Busted Sanctions in the Democratic Republic of Congo', August 2020, <<https://thesentry.org/wp-content/uploads/2020/08/OvertAffairs-TheSentry-August2020.pdf>>, accessed 27 March 2023; UNSC, 'Resolution 2321 (2016)/ Adopted by the Security Council at its 7821st Meeting, on 30 November 2016', S/RES/2321, 30 November 2016; UNSC, 'UN Panel of Experts Report, S/2021/211', March 2021, p. 54, fn 129.

Conclusion

This guide aims to support the private sector on the necessary methodological foundation and tools for developing and conducting an institutional PF RA. To this end, the guide suggests approaches to performing a PF RA, identifying PF risks and risk factors to evaluate an institution's vulnerability to PF, and identifying mitigating controls and strategies.

While the guide will provide a useful starting point for conducting an institutional RA, institutions are ultimately responsible for analysing and applying these guidelines in a way that produces a reasonable judgement of their institutional risk. If conducted diligently, an institutional RA, as well as the information collected over the course of the process, should be a critical first step in better understanding vulnerability to PF, proactively addressing gaps in FIs' CPF frameworks, and mitigating the impact of PF activity through the private sector, and on the national economy and society more broadly.

About the Author

Noémi També is an Associate Fellow at the Centre for Financial Crime and Security Studies at RUSI. She is also an independent financial crime consultant and researcher with over 20 years of professional experience across the academic, public and private sectors – more particularly the private banking industry. She is an Associate Professor at the Luxembourg School of Business.