COUNTERING PROLIFERATION FINANCING

INDUSTRY PERSPECTIVES ON BEST PRACTICES

25 MARCH 2025

CONTENTS

Glossary 4

1. **Introduction**

1.1 Background & Objectives 5

1.2 Introduction to Proliferation Financing ("PF") 6

2. PF Risks and Typologies in Singapore

2.1 PF Risks 7

2.2 PF Typologies in Singapore – Observed/Detected by the Banking Industry 8

2.3 Other PF Typologies in Singapore (featured as key PF threats for Singapore in Singapore's PF NRA) 9

3. Conducting PF Risk Assessment

3.1 Key Purpose of the Risk Assessment 10

3.2 Methodology Framework Pillars 11

4. Risk Mitigation

4.1 Risk Governance 13

4.2 Policies and Procedures 15

4.3 Customer Due Diligence and Controls 17

4.3.1 Case Study 1 – Managing PF Risks through Negative News Screening and Other Analysis 19

4.4 Transactional Due Diligence and Controls 19

4.4.1 Case Study 2 – Using Internal Watchlists to Supplement the Robustness of Transaction Screening Databases/Filters 22

4.5 Incident Management and Investigations 23

4.6 Risk Awareness Programme 25

4.6.1 Case Study 3 – Benefits of Customer Education 26

4.7 Compliance Monitoring and Testing 27

CONTENTS

4.8 Data Analytics Applications for Risk Mitigation 30

4.8.1 Case Study 4 – Lookback Mechanism Revealing Sanctions Evasion Risks 31

4.8.2 Case Study 5 – Counterparty Trawl Revealing Sanctions Risks Exposure 32

5. Higher Risk Focus Areas

5.1 Open Account Trade and Dual-Use Goods 33

5.2 Correspondent Banking and Countries/Geographical Risk 35

5.3 Shell & Front and Broking Companies 36

5.4 Maritime Activities 37

6. Role of Public-Private Partnerships and Importance of Information Sharing to Combat PF

6.1 Background 38

6.2 Importance of Information Sharing 38

6.3 Existing Partnerships and Information Sharing Initiatives 39

6.4 Benefits for the Industry 39

7. Managing PF Risks for Non-Banks

7.1 Background & Introduction 40

7.2 Suggested Best Practices based on Observations 40

7.3 Measures for Risk Mitigation 41

8. Conclusion 43

Appendices

Appendix A: List of PF Risk Factors and Indicators 44

Appendix B: List of Potential Sources for Threats Identification 46

Appendix C: List of Considerations for Vulnerabilities Identification 47

Appendix D: Working Group Members and Other Contributors 48

Appendix E: References 50

Glossary

Acronym	Description
1LoD	First Line of Defence
ACIP	AML/CFT Industry Partnership
AIS	Automatic Identification System
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
BSM	Board of Directors and Senior Management
CDD	Customer Due Diligence
COSMIC	Collaborative Sharing of ML/TF Information & Cases
CPF	Counter-Proliferation Financing
CSPs	Corporate Service Providers
DA	Data Analytics
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
DPTSPs	Digital Payment Token Service Providers
EDD	Enhanced Due Diligence
EWRA	Enterprise-Wide Risk Assessment
FATF	Financial Action Task Force
IMO	International Maritime Organisation
IP	Internet Protocol
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
MRP	Material Risk Personnel
OFAC	US Treasury’s Office of Foreign Assets Control
P&Ps	Policies and Procedures
PF	Proliferation Financing
PF-TFS	PF Targeted Financial Sanctions
PoE	Panel of Experts
STRs	Suspicious Transaction Reports
TF	Terrorism Financing
TM	Transaction Monitoring
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions
WMD	Weapons of Mass Destruction

1. Introduction

1.1 Background & Objectives

Background

In 2022, a Counter-Proliferation Financing (“CPF”) Working Group was established under the Anti-Money Laundering/Countering the Financing of Terrorism (“AML/CFT”) Industry Partnership (“ACIP”), which included representatives[1] from participating banks (Citibank, DBS, Deutsche Bank, HSBC, JPMorgan, OCBC, SCB, UOB), non-banks, the Commercial Affairs Department (“CAD”), the Monetary Authority of Singapore (“MAS”), and Ernst & Young ("EY").

The objective of the CPF Working Group is to share best practices on the management of PF risks to further strengthen the industry’s collective defence against PF.

The development of this paper stemmed from thorough discussions amongst the CPF Working Group members, alongside an analysis of survey feedback from industry participants, encompassing both banks and non-banks, and complemented by focus group sessions. This paper draws on existing publications[2] from the Financial Action Task Force (“FATF”), United Nations (“UN”), MAS, and other relevant regulatory bodies and authorities.

Singapore gives effect to the United Nations Security Council Resolutions ("UNSCR") relating to the Democratic People's Republic of Korea (“DPRK”) and the Islamic Republic of Iran (“Iran”) through the Financial Services and Markets DPRK and Iran Regulations (applicable to financial institutions in Singapore) and the United Nations DPRK and Iran Regulations (applicable to individuals and entities, including designated non-financial businesses and professions but excluding financial institutions, in Singapore and Singapore citizens outside Singapore). Singapore’s status as an international financial centre and key trading and transhipment hub makes it susceptible to PF risks. Countering these risks has been identified as a priority area for both Singapore and its financial sector. As stated in Singapore's 2024 PF National Risk Assessment and Counter-PF Strategy ("Singapore's PF NRA")[3], the PF risks posed by the DPRK and Iran continue to be a concern for the international community.

1 Please refer to Appendix D for the full list of representatives as of the date of this publication. JPMorgan participated in the initial stages of the Working Group discussions but had to drop out subsequently due to other commitments.
2 Please refer to Appendix E for full list of publications that were leveraged during the development of this paper.
3 Published on 30 October 2024 on the websites of MAS, the Ministry of Home Affairs and the Ministry of Finance - for more details, please refer to: https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/proliferation-financing-national-risk-assessment-and-counter-pf-strategy.

1. Introduction

1.1 Background & Objectives

Objectives

This paper provides banks with a foundational guidance to advance their understanding and management of PF risks in the Singapore context by:

a) providing an overview and increasing industry awareness of the PF risks and typologies in Singapore;

b) providing guidance on how a PF risk assessment can be conducted with examples of methodology frameworks, information sources, and risk indicators that can be used to facilitate the assessment;

c) providing guidance on PF risk mitigation measures, including but not limited to, risk governance structures, customer/transactional due diligence, and related controls;

d) highlighting higher PF risk areas and best practices that banks can adopt to address these risks;

e) highlighting the role of public-private partnerships and relevant information sharing, and its importance in combatting PF; and

f) understanding both commonalities and differences between the banking and non-banking sectors, specifically focusing on corporate service providers ("CSPs"), digital payment token service providers ("DPTSPs"), law firms, maritime insurers, and remittance agents, which have been identified as higher-PF risk sectors in Singapore's PF NRA.

Whilst intended to provide guidance for the management of PF risks to banks in Singapore, similar principles and practices set out in this paper could also be applicable to non-banks. This paper will serve as a good starting point in providing non-banks with a common framework to support their assessment and management of PF risks.

1.2 Introduction to Proliferation Financing ("PF")

What is Proliferation and PF?

A. Proliferation of weapons of mass destruction ("WMD")

FATF defines the proliferation of WMD as the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual-use goods used for non-legitimate purposes).[4]

B. PF

FATF defines this as the raising, moving, or making available of 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).[5]

PF Targeted Financial Sanctions ("PF-TFS")

The implementation of PF-TFS is crucial for a robust CPF regime. This paper covers TFS related to the financing of proliferation of WMD. It should be noted that the relevant UNSCR are much broader and prescribe other types of sanctions (e.g., travel bans, activity-based financial prohibitions, category-based sanctions). Where appropriate, the paper also references these sanctions.

4 Please refer to FATF's Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021), footnote 7.
5 ibid.

2. PF Risks and Typologies in Singapore

This section outlines PF risk factors for evaluating PF risks and PF typologies in Singapore.

2.1 PF Risks

The existence of risk indicators suggests the likelihood of the occurrence of suspicious activity. A single standalone indicator in relation to a customer or transaction may not alone warrant suspicion of PF, nor will a single indicator necessarily provide a clear indication of such activity, but it could prompt further monitoring and examination, as appropriate.

Non-exhaustive examples of potentially higher risk situations for consideration when evaluating PF risks relating to types of customers, countries or geographic areas, products, services, transactions and delivery channels include:

Risk Category	Higher PF Risk Factors[6]
Customer Risk	• Customer or counterparty is listed on lists issued by international organisations and governments featuring persons of PF concern • Customer with main source of revenue/income/wealth from a country of proliferation concern • Customer or counterparty engaged in the manufacturing, supply, purchase or sale of proliferation-sensitive items, dual-use goods, or military goods • Customer or counterparty is featured in news or reports from credible sources (e.g., the United Nations Security Council (“UNSC”)’s Panel of Experts ("PoE")), or is subject to formal investigations by domestic or foreign authorities for sanctions and related reasons • Customer or counterparty has a history of violations of sanctions or export controls laws
Country or Geographic Risk	• Commercial relationship or business ties with a country of proliferation concern • Commercial relationship or business ties with countries that have diplomatic, trade or corporate links, or are near to a country of proliferation concern such as countries identified by credible sources (e.g., the UNSC PoE) as involved in proliferation networks • Countries subject to sanctions, embargoes, or similar measures imposed by regulatory bodies or international organisations (e.g., the UNSC) • Links with countries identified by credible sources as being subject to proliferation restrictions/countries of proliferation concern or having high rates of terrorism, organised crime involving WMD, arms trafficking or cybercrimes (including cybercrimes relating to virtual assets)
Product and Service Risk	• Payment received from unknown or unrelated third parties not identified in supporting documentation • Transfer of dual-use goods, proliferation-sensitive items, and materials to a country of proliferation concern • Customer sends and receives digital assets to and from external digital assets wallets that are tagged or have linkage to sanctioned individuals/entities • Illegal exportation of luxury and non-luxury goods such as commercially traded goods, which contravene Singapore’s sanctions against the DPRK
Transaction Risk	• Project financing of sensitive industries in a country of proliferation concern • Trade finance services, transactions, and insurance products involving countries of proliferation concern • Anonymous transactions, which may involve cash • Non-face-to-face business relationships or transactions where appropriate risk mitigation measures have not been implemented • Wire transfer activity that shows unusual pattern or has no apparent purpose
Delivery Channel Risk	• Maritime insurance and re-insurance services to those who own, operate, and/or provide services to vessels operating in regions identified as having higher risk of sanctions evasion

6 Please refer to Appendix A for more examples of PF Risk Factors and Indicators.

2. PF Risks and Typologies in Singapore

2.2 PF Typologies in Singapore – Observed/Detected by the Banking Industry

The CPF Working Group identified several PF typologies concerning the DPRK and Iran. The following are examples of top PF typologies detected via ongoing monitoring such as transaction monitoring ("TM"), transaction screening, customer reviews, and intelligence received, which are most relevant in the Singapore context. Some of these PF typologies have been identified as key PF threats for Singapore within Singapore's PF NRA.

A. Use of shell and front companies, and complex ownership and control structures

- Illicit actors may utilise shell or front companies to conceal their true identities and nature of their activities. Due to the speed and ease of set up, such companies are often used for brief periods to move monies and are usually part of an extensive network of similar companies. Shell companies may be used to move funds and assets across borders, and to evade sanctions whilst front companies are operating companies often used as a front to obscure the illicit actors' involvement in PF activities. Such companies may also be used to move dual-use goods to a country of proliferation concern (or goods in general that are prohibited to be exported to such countries), as well as facilitate the movement of funds or assets across borders.
- Illicit actors may complicate ownership or control structures by using multiple layers of ownership or control and/or nominee directors or shareholders, and incorporating entities in offshore jurisdictions with strict secrecy laws.

B. Ship-to-ship transfers of prohibited goods and falsification of information on vessel identities

- Illicit actors use various methods to evade detection during ship-to-ship transfers at sea. They may physically alter the vessel's appearance, name, and International Maritime Organisation ("IMO") number or falsify information via the Automatic Identification System ("AIS") to misrepresent the vessel's identity. Additionally, they may falsify details regarding the country of origin, country of destination, cargo, or vessel to conceal the true details, aiming to evade detection by banks and disguise prohibited transactions.
- Illicit actors may facilitate ship-to-ship transfers of prohibited goods using vessels registered in countries, which are not fully compliant with international sanctions regimes. These vessels may fly the flags of countries perceived to have less robust maritime regulations. Additionally, illicit actors may use flags of convenience or shell companies to obscure vessel ownership and may sometimes re-flag or rename vessels to evade detection.
- Illicit actors may also use transhipment hubs bordering sanctioned countries or ports perceived to have weak or inadequate customs and border control procedures.

C. Use of third-party suppliers and/or bank accounts

- Sanctioned individuals/entities may utilise deceptive practices to procure goods or use pass-through entities in third countries to conceal the ultimate beneficiary. For example, in 2019, the US Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory outlining deceptive practices employed by Iranian entities aimed at circumventing US sanctions. Iranian persons bypassed sanctions by obtaining US-origin aircraft parts through third-party suppliers across various jurisdictions.
- To conceal the origin of the transactions and the intended beneficiary of the funds, sanctioned individuals/entities may use third-party bank accounts or accounts involving third-party payments to avoid detection.

2. PF Risks and Typologies in Singapore

2.2 PF Typologies in Singapore – Observed/Detected by the Banking Industry

D. Use of correspondent banking services involving higher-risk banks

- Illicit actors may utilise correspondent banking services to gain access to the global financial system. Sanctioned individuals/entities may incorporate shell or front companies in countries that are perceived to have weaker AML/CFT regimes and accordingly, greater ease of opening accounts.
- Cross-border payments can be made more complex when transacted through multiple intermediaries before reaching the beneficiary bank.

E. Transhipment of prohibited goods via third countries

- Sanctioned countries and countries of proliferation concern may utilise third countries, usually entrepot zones or those which are located in close proximity, to obtain prohibited goods. Specifically, the DPRK was reported to have received imports of luxury and commercially traded goods via such means.

2.3 Other PF Typologies in Singapore (featured as key PF threats for Singapore in Singapore's PF NRA)

A. Movement of dual-use goods

- Countries of proliferation concern require dual-use components and technologies for their WMD activities/programmes. To procure these, illicit actors often use complex trade networks with numerous overseas third-party intermediaries (e.g., procurement agents, front companies, and suppliers) and route dual-use goods through several jurisdictions, creating layers to obscure the end-user. They may also falsify end-user documentation and shipping details to conceal the end-user and use deceptive tactics to access the international financial system. All these actions help them to evade export controls and sanctions.

B. Misuse of virtual assets

- Virtual assets/cryptocurrencies could be misused by illicit actors because of the pseudonymity (or in some cases, anonymity) they offer, convenience they provide as an instantaneous value transfer medium, and cross-border nature of virtual asset transactions. The UNSC PoE on the DPRK has noted that DPRK cyberactors had engaged in trading multiple forms of virtual assets, with the DPRK specifically targeting anonymity-enhanced cryptocurrencies. The FATF noted in 2024 that virtual assets continue to be used to support the proliferation of WMD, and that the DPRK continues to steal or extort virtual assets from victims. The DPRK also employs increasingly sophisticated methods to launder illicit proceeds, involving anonymity-enhancing coins, mixers, decentralised finance arrangements, and cross-chain bridges before converting stablecoins into fiat currencies at over-the-counter brokers concentrated in certain jurisdictions. Singapore's PF NRA noted that the misuse of virtual assets was featured in around 17% of PF investigations initiated by Singapore authorities from 2019 to 2023.

3. Conducting PF Risk Assessment

This section highlights the key elements to be taken into consideration when undertaking a PF risk assessment.

3.1 Key Purpose of the Risk Assessment

What is a PF Risk Assessment?

The aim of a PF risk assessment is to identify, analyse and understand PF risks, with a view to developing appropriate measures to mitigate or reduce an assessed level of risk to a lower or acceptable level.

There is no single risk assessment methodology as there is no one-size-fits-all approach in assessing risks. An effective approach for one jurisdiction or one private sector firm will not necessarily be effective for others.

Understanding PF risks on an ongoing basis is essential in strengthening the ability to prevent sanctioned individuals/entities involved in WMD proliferation from raising, storing, moving, and using funds and/or other financial assets.

Pursuant to FATF Recommendation 1, FATF recommends countries to identify, assess, and understand the PF risks for the country and take commensurate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose.

Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate PF risks are commensurate with the risks identified. In implementing a risk-based approach, banks, other financial institutions (including virtual asset service providers) and Designated Non-Financial Businesses and Professions (“DNFBPs”) should have processes in place to identify, assess, monitor, manage and mitigate PF risks.

Undertaking a PF Risk Assessment for your bank

Banks are recommended to assess their aggregate risks, including PF risks, periodically (e.g., annually) through their Enterprise-Wide Risk Assessment (”EWRA”) process, to identify, assess and quantify the inherent and residual PF risks as well as to evaluate the robustness of their systems and controls.

Banks are not required to have a standalone risk assessment for PF if pre-existing Money Laundering (“ML”), Terrorism Financing (“TF”) or sanctions risk assessment methodologies already incorporate PF risks or can adequately incorporate PF risks. PF risk management and controls can be part of existing enterprise-wide risk management programmes and processes.

Entities undertaking a PF risk assessment may consider the following factors:

I. preliminary scoping;
II. planning and organisation;
III. identification of threats and vulnerabilities;
IV. analysis; and
V. evaluation and follow-up.

3. Conducting PF Risk Assessment

3.2 Methodology Framework Pillars[7]

I. Preliminary Scoping

Banks may consider conducting a scoping exercise to determine the objectives, scope and focus of the assessment. Banks may focus their analysis on reviewing various recent methods, trends, and typologies of the breach, non-implementation or evasion of PF-TFS identified in various sources[8].

II. Planning and Organisation

Banks may consider adopting a systematic and consistent process to prepare a project plan, involve relevant stakeholders, devise a structured mechanism for data collection, conduct subsequent analysis, document findings, compare findings over time, and continuously refine the methodology.

III. Identification of Threats and Vulnerabilities

1. Threat

Banks may start their identification process by compiling a list of major known or suspected threats such as:

- sanctioned individuals/entities associated with the risk of PF (direct), or parties acting on their behalf (indirect), whether actual or potential;
- key sectors, products, or services that have been exploited;
- activities that sanctioned individuals/entities have engaged in; and
- primary reasons why sanctioned individuals/entities are not deprived of their assets or identified.

Banks should keep in mind that whilst the methodology of identifying PF threats could be similar to that of ML/TF, there are unique differences that should be considered in a PF threat assessment. Particularly, banks must be alert to the unique PF threats/typologies (and associated financing channels) relevant to the markets that they operate in, and the financing needs/methods in relation to sanctioned individuals/entities as part of their threat assessment. For example, a bank may need to assess its exposure to virtual assets and to facilitating the movement of dual-use goods, ship-to-ship transfers and the export of luxury goods.

As the risk profile and appetite vary between banks, considerations should be taken based on other factors for a holistic approach when gathering threat information, and to draw on available information sources relating to domestic, regional, and international PF threats.

Potential information sources[9] may include:

- sanctioned individuals/entities targeted by relevant UNSCR PF-TFS;
- actual or known typologies (including PF and related cases investigated/prosecuted by local authorities); and
- summaries of case types, schemes or circumstances involved in the breach, non-implementation or evasion of PF-TFS identified by banks internally or from reports published by national or international organisations.

7 Please refer to FATF's Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021), section 1.
8 Please refer to Appendix B for examples of sources banks can leverage during their PF assessment.
9 Please refer to Appendix B for the list of potential sources for the identification of threats.

3. Conducting PF Risk Assessment

3.2 Methodology Framework Pillars

2. Vulnerabilities[10]

Banks are encouraged to adapt their methodology used for identifying ML/TF vulnerabilities for PF purposes. Vulnerabilities refer to matters that can be exploited by threats, or that may support or facilitate non-compliance with TFS.

Vulnerabilities may be based on various factors. Examples of such factors and their corresponding considerations to note are set out below:

Vulnerability	Considerations
Structural	Firm's nature, scale, diversity, and geographical footprint; target markets and customer profiles; and the volume and size of transactions
Sectoral	Relative complexity and reach of funds movements
Product or Service-specific	Complexity, reach, accessibility, corresponding customer base, and offering across the firm
Customer and Transaction	Number of high-risk customers, parties and countries involved in cross-border transactions, multiple shell or front companies, and customer due diligence ("CDD") information

IV. Analysis

In addition to threats and vulnerabilities, banks may consider other general risk factors[11] that can make a jurisdiction vulnerable to PF. Risk can be considered as a function of threat, vulnerability, and consequence. This stage involves the consideration of the likelihood and consequences of specific PF risks materialising.

Banks are recommended to assign a relative value or importance to each of these risks and prioritise identified risks by considering their likelihood and consequences.

Likelihood includes the consideration of known cases, intelligence, typologies, strengths of CPF controls, and capabilities and intent of sanctioned individuals/entities whilst consequences include potential impact. Consequences refer to the outcome where sanctioned parties misuse funds or assets that are made available to them and consequently expose the firm to various risks including reputational risk, amongst others. Banks should bear in mind that not all PF methods have equal consequences.

V. Evaluation and Follow-Up

Banks are recommended to establish a structured process for evaluating PF risks or any concerns and weaknesses and determining priority risk areas. Process should incorporate a mechanism for consistently identifying areas of improvement throughout the lifecycle of the risk assessment.

Regular updates to the assessment of PF risks are crucial, constituting an evolving process that factors in present threats, compliance with sanctions requirements, and the potential for non-compliance or circumvention.

An update of the PF EWRA may be triggered due to (i) changes to UN designations against countries as specified in the relevant UNSCRs; (ii) local regulatory requirements; (iii) country's PF national risk assessment outcomes; and (iv) increased PF risk exposure for the country/banks operating in the country etc.

10 Please refer to Appendix C for the list of considerations for the identification of vulnerabilities.
11 Please refer to Appendix A for more examples of PF Risk Factors and Indicators referenced in this paper.

4. Risk Mitigation

Banks are encouraged to consider the following key areas when developing and establishing a risk mitigation framework to ensure that it also covers PF risk mitigations.

4.1 Risk Governance

Oversight

A bank's board of directors and senior management ("BSM") are accountable for ensuring that the bank has a sound risk mitigation framework that includes mitigating PF risks. The responsibilities of the BSM may include ensuring that:

- the allocation of sufficient compliance resources is made across all lines of defence and that the compliance function remains independent;
- policies and procedures ("P&Ps") addressing PF-related risks are in place, regularly updated to address emerging risks and readily accessible, effective and understood by all relevant staff;
- clear roles and responsibilities are in place across all lines of defence for detecting, monitoring and managing PF-related risks and staff accountability is enforced;
- staff are adequately trained to effectively detect, review, and assess/advise on PF risks, typologies and red flags; and
- there are established risk metrics/an escalation process to ensure that material PF risks are escalated to BSM expeditiously and any deficiencies are adequately addressed.

Roles and Responsibilities

The "Three Lines of Defence" model is defined in the Guidelines to MAS Notice 626 that sets out the responsibilities pertaining to each line of defence. The following are specific to PF risks.

First Line of Defence ("1LoD") (Front Office and Business Compliance)

- Have good knowledge of prospect and existing customers (including each customer's business model, trading profile, sources of raw materials, locations of trading counterparties etc.) to assess the PF risks posed by these customers and their transactions
- Keep abreast of PF typologies and red flags shared by regulators, authorities and/or the second line of defence
- Be vigilant in detecting, assessing and escalating PF red flags in transactions/ documentation

Second Line of Defence (Compliance)

- Have PF and sanctions expertise to review, assess and provide feedback on PF red flags identified by the 1LoD
- Devise procedures to guide 1LoD on escalation of suspicious transactions to compliance
- Establish procedures for periodic review of Suspicious Transaction Reports ("STRs") to identify any PF-related trends which may be an indication of control gaps and/or new PF typologies, and take follow-up action to proactively manage both existing and emerging PF risks
- Perform compliance testing on a regular basis to ensure timely identification of any weaknesses in PF controls
- To establish a process for updating BSM on PF-related escalations, weaknesses in controls, and plans for remedial actions
- Undertake training and awareness initiatives (in conjunction with AML/CFT training programme or otherwise) to keep all stakeholders apprised of PF-related red flags and typologies

Third Line of Defence (Internal Audit)

- Assess adequacy and operating effectiveness of the bank's PF risk mitigation policies and processes
- Incorporate testing of such controls in audit plan as required and ensure that staff performing such testing have adequate knowledge on PF

4. Risk Mitigation

4.1 Risk Governance

Best Practices

1. Timely reporting to BSM on PF risks for sound decision making

The BSM should receive timely reports on PF risks to enable them to regularly monitor and manage the risks on an ongoing basis.

Potential scope of reports

Examples of the risk metrics and information that can be reported include:

- PF EWRA and suspected cases of PF, along with associated typologies, which are identified during the bank's operations;
- effectiveness and adequacy of PF controls implementation;
- material updates on the bank's internal P&Ps/controls that address PF-related risks;
- analysis of PF-related risk metrics[12] such as:
  - backlog and aging reports for periodic customer account reviews or triggered ad-hoc reviews for PF risks
  - timeliness of review and closure of TM and name screening alerts
  - PF-related STR numbers/trends
  - rejected or blocked payments/trade transactions resulting from PF-related transaction screening hits (numbers/trends); and
- significant regulatory developments on PF, or notable new PF risk typologies and red flags highlighted by the regulators (e.g., case studies of PF-related enforcement actions or prosecutions by regulatory authorities), and the key takeaways or impact assessment on the bank.

2. Senior management committee to oversee management of PF risks

PF risks should be included in the Terms of Reference/scope of coverage of the bank's senior management committee[13] overseeing financial crime risks[14].

The senior management committee may execute sound decisions or be apprised of decisions made by Material Risk Personnel ("MRP")[15] on matters such as:

- requests to establish and/or retain high risk customer relationships of which PF is a risk contributor;
- requests to deviate from established P&Ps that address PF-related risks; and
- risk-based approaches to monitoring and mitigating risks which may be associated with PF, including whether the level of residual risks is acceptable.

12 PF-related risk metrics may be reported as part of sanctions-related risk metrics.
13 The committee may be established locally, regionally, or globally depending on the size and complexity of the bank.
14 The second line of defence should be represented in the committee to provide compliance perspectives and highlight potential PF risks.
15 Please refer to MAS Guidelines on Individual Accountability and Conduct (September 2020), section 4.

4. Risk Mitigation

4.2 Policies and Procedures

P&Ps to assess and combat PF risks should be established on a standalone basis or incorporated as part of a bank's wider AML/CFT and sanctions P&Ps. The objectives are to ensure effective implementation of targeted UNSCRs and other international sanctions on PF (primarily levied on the DPRK and Iran), and combat against evasion of such sanctions.

Bank's P&Ps that address PF-related risks should broadly cover, without limitation, the following key areas:

Areas	Recommended measures to address PF-related risks
Risk Appetite/ Assessment 	• Clearly set out the bank's risk appetite and any restrictions, on customer relationships and transactions, involving sanctioned individuals/entities and high PF risk/sanctioned jurisdictions • PF-related deviations should be approved by the relevant approving authorities (including relevant business risk owners, compliance stakeholders and the appropriate senior management risk committees, where relevant) under each bank's governance framework • Regularly review and update the bank's risk appetite to ensure alignment with changing regulatory requirements and emerging risks
Sanctions and CPF programmes 	• Put in place sanctions and CPF programmes, which should be in strict compliance with the relevant Financial Services and Markets Regulations for TFS in effect, TFS under the UNSCRs and other international sanctions on PF • Countries which are subject to comprehensive sanctions (e.g., the DPRK and Iran) or other targeted sanctions or are considered high PF risk countries should be risk-classified accordingly by the bank. The bank may consider stipulating the consequent policy implications (e.g., strict prohibition, enhanced due diligence ("EDD") or other specific conditions) on onboarding/retaining customers and processing transactions with a nexus to such countries
Customer Acceptance, Onboarding and Exit 	• Banks may find it useful to incorporate PF-related queries to assess PF risk exposure as part of the CDD process and document any potential PF risk exposure of the customers. This can either be applied for all customer onboardings or on a risk-based approach • In cases where a customer has a known or newly identified PF exposure, it is essential to assess whether appropriate risk mitigation measures are in place, including exiting the customer relationship, if necessary
Screening 	• Conduct screening on the bank's customers and their connected parties and declared major counterparties on a risk-based approach (refer to section 4.3 below on Screening)
Alerts Management and Escalation Protocol 	• Establish clear guidelines for prioritising and resolving higher risk screening alerts, including sanctions/PF alerts, with expedited resolution timelines and for prompt filing of STRs where necessary, in accordance with the relevant regulatory requirements • P&Ps can include actions required in relation to a confirmed true match such as blocking, freezing or restricting accounts, rejecting or blocking transactions, escalation for decisions, and regulatory reporting

4. Risk Mitigation

4.2 Policies and Procedures

Areas	Recommended measures to address PF-related risks
Ongoing Customer and Transactional Due Diligence and Controls 	• Conduct periodic CDD reviews on existing customers, particularly following a PF trigger event or when a customer's profile has significant changes. CDD information should be refreshed and documented • Ensure CDD reviews identify any new PF risk exposure and/or validate that the existing PF risk exposure remains in line with the bank's risk appetite, and that the bank's actions do not tip-off the customer • Set out procedures on transactions handling including on the following: (i) transactions involving dual-use goods or other "high PF risk" goods and services based on published typologies; (ii) filing of STRs for rejected or blocked transactions; (iii) timely follow-up reviews on customers: with transactions rejected or frozen by the bank or correspondent banks due to potential sanctions/PF-related concerns, with sanctions/PF-related STRs filed on their major counterparties or related parties, or which are observed to be regularly involved in initiating or receiving transactions involving third party payment arrangements; and (iv) assessment if interim controls are required for cases pending completion of review or investigation
Incident Management and Investigations 	• Implement and maintain P&Ps to identify, escalate, investigate and report potential/actual evasions and breaches of PF-TFS • PF breaches should be documented and escalated to compliance for advice, and to senior management for awareness and notification. Banks should report PF breaches in a timely manner, which would include filing STRs and informing MAS as soon as possible
Risk Awareness Programmes 	• Enhance staff awareness, knowledge and competency in PF risks through its P&Ps, information channels and training programmes which should be refreshed regularly to ensure relevance • Develop and maintain PF-specific typologies, trends, red flags risk indicators, methodologies, best practices, information from regulators/authorities, and applicable publications from relevant accredited bodies
Compliance Monitoring and Testing 	• Utilise a risk-based approach to conduct compliance testing, incorporating PF and other financial crime related risk factors, to assess the robustness and effectiveness of the bank's systems, controls, and compliance with its P&Ps, and applicable laws and regulations
Data Analytics Applications for Risk Mitigation 	• Leverage on artificial intelligence, blockchain, data analytics ("DA"), and automation to assess and combat PF risks (e.g., vessels tracking tools and maritime AIS data to detect illicit shipping practices relating to ship-to-ship transfers of goods to/from DPRK-flagged vessels)
Record-keeping 	• Ensure procedures and controls are in place for the retention, maintenance, and deletion of PF-related records per relevant record retention periods
Review and Update of P&Ps 	• Ensure P&Ps are reviewed and approved periodically (e.g., annually, bi-annually, or when material changes are required) by the BSM and regularly updated to remain consistent with regulatory requirements, industry guidelines and typologies, whilst considering emerging PF risks

4. Risk Mitigation

4.3 Customer Due Diligence and Controls

CDD ensures an appropriate level of knowledge and understanding of the bank's customers. The focus of this subsection lies in PF risk-related inquiries.

Banks should ensure that CDD reviews identify any new PF risk exposure for their customers, connected parties and declared counterparties of their customers and/or the customers' existing PF risk exposures remain in line with the banks' risk appetites.

Identification, Verification and Scrutiny of High PF Risk Customers

Banks should assess their customers using a customer risk assessment methodology based on a risk-based approach, and existing customer information from CDD/Know Your Customer ("KYC") processes, applicable laws and regulations, DA and information from competent authorities to identify high PF risk customers.

Due diligence measures, including verifying ownership, control structures, source of funds, and cross checking against sources which may contain entities of potential PF concerns (e.g., entities listed on export control lists for PF concerns), should be implemented to detect and monitor entities, along with scrutinising addresses associated with sanctioned entities (where feasible).

Upon the identification of high-risk customers of which PF is a risk contributor, banks should implement EDD, including the gathering of additional KYC information and enhanced ongoing monitoring, to assess if the customer relationship should be prohibited. If the bank has a reasonable basis to suspect or believe that a customer is involved in PF activity, follow-up action including escalation to compliance and senior management for decisions should be taken.

Banks may leverage publicly available, multi-disciplinary information to uncover complex efforts to evade sanctions. Banks may utilise AIS data with high-resolution satellite imagery to identify vessels and conduct network analysis using data from corporate registries, shipping databases, and ship certification documents. Banks may also perform network and transaction analysis to identify potential links to sanctioned individuals/entities.

Best Practices

Ongoing Monitoring

- Have in place ongoing monitoring controls such as TM along with underpinning processes such as TM risk assessment, designed to detect and escalate unusual activity patterns.
- Whilst these scenarios are generally not exclusively PF-focused, they include monitoring for a variety of PF-relevant behaviours.

Trade Finance Controls

- Examples: Scrutiny of shipping documents for PF risks and typologies, independent verification and tracking of shipping routes for higher risk ports, due diligence on transactions involving higher risk ports or known evasion hotspots.

Other Controls

- Leverage data, artificial intelligence and emerging technology driven tools to validate the legitimacy of supporting documents provided, where available and applicable.
- Implement specific controls that have relevance to aspects of PF risks and typologies.
- Examples: Internet protocol ("IP") blocking of online banking connections from proliferating and sanctioned countries, trade and receivables finance controls using vessels tracking tools and maritime AIS data to detect illicit shipping practices relating to ship-to-ship transfers of goods to/from vessels linked to high PF risk jurisdictions.

4. Risk Mitigation

4.3 Customer Due Diligence and Controls

Screening

Banks are encouraged to clearly set out the minimum screening standards, criteria and requirements in its P&Ps such as:

- the definitions of the critical data elements or fields to be obtained and screened;
- types of screening to be conducted; and
- screening systems to be used.

Banks can also consider (i) including AIS screening and vessel due diligence risk assessment clauses in loan agreements, letters of credit, and other financial instruments for global and regional commodity traders and brokers operating in higher risk markets for oil and petroleum products; (ii) conducting regular AIS screening and vessel due diligence checks on trading partners and vessels for higher risk transactions (e.g., in higher risk jurisdictions); (iii) setting clear risk tolerance thresholds and escalation procedures for higher risk vessel dealings; and (iv) providing training for relevant staff on AIS screening and vessel due diligence procedures.

The integration of AIS screening will augment risk detection capabilities by identifying vessels involved in suspicious or sanctioned activities, enabling banks to avoid high-risk vessel dealings. Additionally, the inclusion of vessel due diligence risk assessment clauses will ensure that traders conduct thorough checks on vessels to mitigate the risk of involvement in sanctions/PF-related or illicit activities and reduce the risk of non-compliance and associated reputational damage to the banks.

At minimum, customer name screening and negative news screening should be conducted for customers.

1. Customer Name Screening

- Banks should perform name screening on customers and their connected parties (for example, beneficial owners and authorised signatories) prior to onboarding, on an ongoing basis and when changes occur (including address updates, new beneficial owners, and updates to beneficial ownership)
- Screening should be conducted against the following up-to-date lists (non-exhaustive):
  - UNSC PF-TFS lists;
  - domestic lists (such as those referred to in MAS' Financial Services and Markets Regulations)
  - other PF-relevant lists that the bank assesses to be relevant and applicable, including those issued by authorities in jurisdictions where the bank has business operations or exposure (e.g., the United Kingdom, United States, and European Union authorities);
  - bank's internal lists; and
  - applicable global sanctions and local sanctions lists.

2. Negative News Screening

- PF risks can be managed through negative news screening using methods such as:
  - deploying automated screening where PF-related news categories are included as part of the bank's name screening tools' algorithms; or
  - collecting data from various sources (for example: regulatory databases, news articles, and relevant public information focusing on PF-related negative news such as UNSC PoE reports and the US Department of Justice indictments).

  These methods enable banks to (i) ascertain if any of their customers, connected parties and/or declared major counterparties of their customers exhibit potential PF risks; and (ii) detect adverse information linked to PF risks on these parties.

4. Risk Mitigation

4.3.1 Case Study 1 – Managing PF Risks through Negative News Screening and Other Analysis

A bank referenced a US indictment which disclosed that Entity A's network of front companies facilitated illicit financial activities for DPRK entities involved in WMD proliferation, and subsequently conducted a two-pronged approach to map a segment of Entity A's network.

Firstly, the bank analysed transactional activity involving entities named in the indictment to identify counterparties and transactional relationships. This approach allowed the bank to map out layers of counterparty relationships involving Entity A which the bank was exposed to.

Secondly, the bank supplemented its transactional analysis by integrating online customs data of exporters who had recorded shipments of potential dual-use goods to DPRK within a specific timeframe. The integration of customs data enabled the bank to spot name matches for counterparties initially identified through the transactional analysis, thereby facilitating a more precise filtering of customers and the subsequent prioritisation of targeted review investigations.

Note: The approach employed has certain inherent limitations, notably in detecting export controls concerns and accessing transactional level information on customers' international trade activities including imports, exports, and technology transfers. Banks should remain agile and adjust detection strategies based on available information and data to effectively identify and mitigate PF risks.

4.4 Transactional Due Diligence and Control

Transaction Screening (Cross Border Remittances and Trade Payments)

Transaction screening enables banks to identify, on a pre-transaction basis, transactions that may involve sanctioned individuals/entities or pose PF risks, allowing for further assessment on whether to process such transactions; taking into account regulatory obligations, the bank's internal risk policies and whether fund freezing obligations apply.

4. Risk Mitigation

4.4 Transactional Due Diligence and Controls

Transaction Screening (Cross Border Remittances and Trade Payments)

Banks may consider incorporating the following measures into their transaction screening framework and system to mitigate PF-related risks during transactions.

PF-related typologies should be incorporated into existing transactional screening framework and system with clear procedures setting out types of transactions that may require additional transactional due diligence before transactions may be processed.

Transaction Screening Framework and System
A. Pre-transaction screening
All incoming and outgoing cross-border wire payments and relevant information in trade documents[16] should be screened against the following lists to interdict and reject or block transactions, where required, that are assessed to be PF-related or to pose PF risks: (i) UNSC and other relevant sanctions lists; (ii) high PF risk[17]/sanctioned jurisdictions; and (iii) bank's internal watchlists.
B. Periodic reviews of screening protocols and algorithms
Establish a process to periodically review the adequacy of the transactional screening system which should include, without limitation: • types of payment messages and fields where screening must be applied, covering the ongoing and timely assessment of any subsequent changes to SWIFT message types and fields as well as new products/payment solutions or platforms which require transactional screening; • timeliness and frequency of updating screening lists; • robustness in the selection of sanctions/other lists applied for transactional screening to satisfy regulatory obligations and bank's internal policies. This includes the need to be aware and cognisant of the content and scope of the screening databases provided by external vendors, and to supplement those with the bank's internal watchlists where required; • degree of sensitivity of the match-rank or fuzzy logic algorithms applied and whether they are in line with the bank's risk profile, risk appetite and industry best practices; • adequacy of the controls or tools to address the risk of wire stripping; and • principles applied to screening of non-Latin alphabet data such as Chinese commercial codes and effectiveness of controls in place.
C. Transaction screening hit handling parameters
The hit handling parameters should be regularly reviewed and adjusted where necessary to take into account regulatory developments and pertinent PF/sanctions typologies and trends that the bank may identify from time to time from internal reviews or external sources and publications.
D. Post-transaction reviews
During periodic customer account reviews, conduct sampling-based, deep transactional reviews of past wire transfer transactions to identify customers with prior dealings involving individuals/entities of PF concern, that may not have been detected at the pre-transaction level.

16 Please refer to the ACIP Paper on Best Practices for Countering Trade Based Money Laundering, May 2018, Section 4.3.
17 The determination of high PF risk jurisdictions is at the discretion of the banks.

4. Risk Mitigation

4.4 Transactional Due Diligence and Controls

Best Practices

1. Transaction screening hit handling parameters

The hit handling parameters should be regularly reviewed and adjusted in line with regulatory developments and pertinent PF/sanctions typologies and trends identified periodically. Banks may:

- review IP address records of customers accessing their electronic banking channels and services or initiating transactions; and/or
- put in place controls to block or monitor customer activity from IP addresses in sanctioned jurisdictions.

2. Robustness of transaction screening databases/filters

Banks should be aware and cognisant of the content and scope of the screening databases provided by external vendors, and supplement those with their internal watchlists where required. Banks should identify, on a risk-based approach:

- individuals/entities of material PF concern which may not be designated but are featured in the following sources of information: (i) publicly available adverse news such as publicised law enforcement cases or regulatory enforcement actions (e.g., OFAC), UNSC PoE reports pertaining to PF, reputable think tank reports; (ii) maritime databases; (iii) intelligence shared by regulators or other banks; and (iv) Bank's in-house investigations into suspicious transactions involving sanctions evasions or other PF typologies; and
- individuals/entities deemed to be acting on behalf of or at the direction of UN/MAS designated persons/entities, where known.

3. Post-transaction review: screening of key/relevant parties in underlying documents

- Using a risk-based approach, establish a process for post-mortem review of controls to be conducted when STRs are filed on PF and sanctions related risks.
- Deeper retrospective reviews of wire transfer transactions on a sampling basis would be useful during periodic reviews of customer accounts to identify customers which had previously transacted with individuals/entities of PF concern, as this may not have been identified at a pre-transaction level. For example, supporting documents including the screening of key/relevant parties (e.g., counterparties, importer/exporter, vessels, carrier, charter, agent, freight forwarder, shipping company, consignee etc.)[18] and/or locations named in the supporting documents for the underlying transaction/activity can be obtained and reviewed to identify any PF-related red flags.

4. Periodic review/Back-test on transaction screening system

- Useful for banks to institute a periodic review/backtest to validate that the transaction screening system deployed by them, including the system parameters and rules, are working effectively and as intended to flag PF screening hits and that the residual risk identified is within the scope of their previously established risk appetite.
- Review should be performed by a party independent of the compliance function involved in deciding the screening filter and system rules. Review may cover topics such as timeliness and comprehensiveness in the implementation of new/changes in sanctions lists for transaction screening, the degree of sensitivity of the fuzzy logic algorithms applied, and any other matters relevant to the banks' specific circumstances.

18 Please refer to the ACIP Paper on Best Practices for Countering Trade Based Money Laundering, May 2018, Section 4.3

4. Risk Mitigation

4.4.1 Case Study 2 – Using Internal Watchlists to Supplement the Robustness of Transaction Screening Databases/Filters

XYZ Trading (Originator)

Bank's Customer P (Beneficiary)

2023: Attempted to send EUR payment to

Flagged by the Bank's transaction screening filter due to a hit on "NITC" and "Vessel X" in field 70 of the SWIFT message

National Iranian Tanker Company (NITC) and its affiliated Vessel X were re-designated by OFAC in 2020 for playing a significant role in oil deals used to generate revenue for Iran's Islamic Revolutionary Guard Corp-Qods Force and Hizballah.

XYZ Trading's response to the Bank's queries:

- The payment was for piloting services provided to Vessel X.
- NITC refers to "NEW INTERNATIONAL TRANSPORTATION CONTRACT".

Customer P provided supporting documents which indicated that NITC referred to **National Iranian Tanker Company** who manages the Iran-flagged OFAC SDN Vessel X.

Transaction was rejected by the Bank and **XYZ Trading** was placed on the Bank's Internal Watchlist for Name and Transactional Screening as it was potentially a front company acting on behalf of NITC.

Within the same month, another incoming EUR payment from XYZ Trading to a different customer of the Bank, Customer E, was flagged by the Bank's transaction screening filter. This transaction was rejected due to the following red flags noted:

- Goods in the purchase order were censored;
- Customer E was unable to provide the HS Code of the goods; and
- Customer E cited a Non-Disclosure Agreement with XYZ Trading to decline to provide shipping documents and provided other evasive responses to the Bank's queries.

Other red flags were subsequently noted from the review conducted on Customer E and the customer relationship was terminated.

The Bank was able to interdict the subsequent payment from XYZ Trading and thereafter identify the sanctions concerns on Customer E due to the inclusion of XYZ Trading on the Bank's Internal Watchlist deployed for transactional screening.

* All names have been redacted for the purpose of this case study.

4. Risk Mitigation

4.5 Incident Management and Investigations

Banks should implement and maintain appropriate processes and procedures to identify attempts to evade PF-TFS, escalate such incidents to compliance for advice and investigations, and notify senior management for awareness. PF breaches should be reported in a timely manner, which should include filing STRs promptly with the Suspicious Transaction Reporting Office and notifying the MAS as soon as possible. In particular, for positive sanctions hits against UN/MAS sanctioned individuals/entities, these should be reported to the relevant authorities without delay (and ideally within one business day).

Escalation Protocols

Formal escalation protocols which clearly set out the scenarios, responsible parties and timelines for handling of topics relevant to the management of PF risks should be established. Clarity on these would facilitate effective compliance across the bank, particularly given that some PF risk events are complex and time sensitive.

Banks may consider the following areas when incorporating PF risk management into their escalation protocols:

- **Scenarios which require mandatory escalation from business and operation units to compliance and expected timelines for escalation**

  - True or potential true sanctions/PF name screening hits (prioritised for review in view of potential asset freezing obligations);
  - Suspicious transactions;
  - Prospects onboarding rejected due to PF concerns;
  - Customers exited due to PF concerns;
  - Transactions with true PF screening hits; and
  - Blocked transactions/funds due to PF activity.

- **Approving authorities for policies that address PF-related risks or policy/control deviation requests**

- **Clearly defined escalation protocols and timelines for PF cases**

  The compliance function should be empowered to exercise a certain degree of judgement in deciding which cases require approval at a higher level, thereby ensuring that the senior management's attention is focused on higher risk cases.

- **Whistleblowing or employee disciplinary protocols**

4. Risk Mitigation

4.5 Incident Management and Investigations

Best Practices

1. Designate a point of contact

Incidents linked to PF which are unique and can be identified without ambiguity should be escalated in a timely manner to a designated point-of-contact. The point-of-contact should ideally be part of the second line of defence and have oversight over PF risks and compliance.

2. Investigative team: PF-related knowledge/expertise

As PF risks may overlap with other risk types (e.g., sanctions evasion, ML, TF) and illicit acts may fall into multiple financial crime categories, PF risks may not always be explicitly evident. Therefore, it is critical for the bank's investigative resources to have the capability to readily identify PF risks present in other incidents escalated to the second line of defence and handle them appropriately.

Regular training and refreshers for investigative resources on PF trends and typologies are important to ensure that PF risks are considered when there are PF-related red flags in a financial crime incident reviewed.

3. Investigative team: Resources/tools

The investigative teams should have access to resources and tools to facilitate the identification and mitigation of PF risks (e.g., IP blocking reports, AIS data, reviewing of cargo based on supporting trade documentation to ascertain potential dual-use items and prohibited goods).

4. Clearly defined process for handling PF-related cases

Banks should have a clearly defined process to handle PF-related cases, which may include inhibition of accounts, ringfencing of relationships pending the investigative reviews, and exit of the relationships.

5. Clearly defined escalation protocols and timelines for PF events

Escalation protocols and timelines for key PF-related incidents should be clearly defined, regularly communicated and periodically reviewed to assess the continued adequacy and effectiveness of controls.

4. Risk Mitigation

4.6 Risk Awareness Programme

A bank's BSM and relevant staff from all lines of defence[19] should undergo regular training on PF-related topics to heighten risk awareness and reinforce staff accountability for managing PF risks. PF training may be incorporated into the bank's existing sanctions training programmes or in wider AML/CFT training modules.

Example of a Risk Awareness Programme for Adoption by Banks

Annual training at minimum.

Can be delivered via a combination of e-learning and classroom training

Training materials should be refreshed periodically and tailored for relevance to the target audience

PF-related training for business units should consider the products or services offered, operational locations, customer types/ profiles, and the associated PF risks. Whilst training for operations units may include topics on identification of true or false screening hits and the escalation protocols.

The compliance function can cover policy/regulatory aspects whilst the business compliance function can provide training on the operational aspects of PF controls implementation.

Most effective when delivered by compliance (second line of defence) and business compliance functions (1LoD)

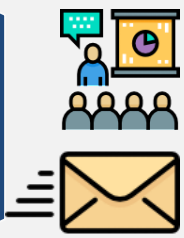
Include case studies on common PF typologies/ internal STR trends/high risk topics

Provide timely training to staff when deficiencies are detected in implementation of PF controls due to staff oversight or lack of understanding

Ad-hoc sharing on PF typologies and risks via email broadcasts or business meetings

PF training materials and resources should be made easily accessible and available to all staff

Customer education initiatives for higher PF risk customers via webinars or electronic direct mailers[20]



19 Particularly, staff involved in onboarding customers and maintaining customer relationships, processing, monitoring and screening transactions, operations, business compliance, compliance, compliance testing and audit functions.
20 See also MAS' Guidance Paper on Sound Practices to Counter Proliferation Financing, Aug 2018, Section 4.4.

4. Risk Mitigation

4.6.1 Case Study 3 – Benefits of Customer Education

AAA International Shipping ("AAA") (Bank's customer)

BBB Marine Services Pte Ltd ("BBB")

attempted to make a USD payment to

This attempted transaction was for the purchase of Marine Gas Oil from BBB which was ultimately delivered to an OFAC SDN "Vessel S".

Entity T had earlier been designated by OFAC for being the manager of a different flagged vessel of Country P, "Vessel U", which had engaged in ship-to-ship transfers of oil for the benefit of the DPRK.

The trade financing application was rejected by the Bank in view of the true sanctions hit on OFAC SDNs Vessel S and the vessel owner ("Entity T") whose names were noted in the Bunker Delivery Note document.

AAA advised the Bank that they did not knowingly violate sanctions regulations and were unaware that Vessel S and Entity T were designated by OFAC. The buyer of Marine Gas Oil was another Entity M, which was not their regular buyer.

After the Bank shared with them on sanctions risks, AAA took steps to improve their internal sanctions-related controls, for example:

- Implementing screening of their customers (buyers), and screening of all vessels and vessel ownership before delivering the marine fuel;
- Incorporating sanctions clauses in bunker fuel sales terms covering both list-based and activity-based sanctions.

AAA also provided the Bank with a sanctions representation letter.

There were no subsequent sanctions concerns noted from the Bank's review of AAA's transactions.

This case study illustrates the benefits of proactive customer education to reduce the Bank's exposure to sanctions risks.

* All names have been redacted for the purpose of this case study.

4. Risk Mitigation

4.7 Compliance Monitoring and Testing

Risk-based Compliance Testing Programme

The compliance testing function provides assurance that the bank's systems and controls are effective in meeting the requirement of its internal P&Ps and/or applicable laws and regulations and mitigating compliance risks, including PF risks.

Bank's risk-based compliance testing programme should test and evaluate the robustness of the bank's systems and controls through the compliance testing function. An appropriate testing approach (i.e., **thematic review** or **continuous monitoring**) based on the bank's approved testing methodology should be adopted to ensure adequate testing of key risk areas, including PF risks.

Compliance testing focus areas should be updated in line with changes to external regulations, risk assessments and in response to testing outcomes and shifting focus to new significant identified risks or control weaknesses.

1. Thematic Review

- May be planned to target key risk areas, including PF risks, identified during risk assessment
- Test and assess key processes and controls against applicable regulatory obligations and internal P&Ps to evaluate the design and operating effectiveness of the control environment
- Key PF control deficiencies identified through thematic reviews will be reported and escalated to management where appropriate. Issues should be recorded on the banks' risk management systems or equivalent registers to track remedial plan/action for completion

Conducting a thematic review

- Prior to commencement of a thematic review, the timing and test scope should be agreed upon by relevant stakeholders and test steps should be developed to target key risk areas, including PF risks identified
- Analytical tools and automation may be adopted where applicable to ensure efficient control testing, interrogate large and complex data sets to determine the effectiveness of a control environment, and enable compliance testing function to generate risk-based samples to focus on investigating exceptions

4. Risk Mitigation

4.7 Compliance Monitoring and Testing

1. Thematic Review

Case Study: Enhancing Compliance Testing through Data Analytics

Background: A bank sought to optimise its compliance testing process for TM alerts. Traditionally, the compliance testing team relied on randomised sampling, but this approach often resulted in non-material findings and inefficient use of resources.

Solution: The bank leveraged DA to interrogate large datasets and refine its sampling approach by overlaying the overall sampling population of TM alerts with a set of risk indicators and generating risk scores for every customer. Examples of such risk indicators include transactions involving higher risk geographic regions, customer segments, length of relationship with the bank, risk rating, total high-risk inward and outward transactions etc. This enabled the compliance testing team to identify higher quality samples for testing based on the risk scores of the customers.

Results and Benefits: The bank's adoption of DA in compliance testing led to significant improvements in reducing testing of lower risk TM alerts and focusing on higher risk and complex cases that potentially contain a higher likelihood of financial crime risks concerns. This data-driven approach enabled more effective allocation of resources and improved the ability to manage potential financial crime risks in a timelier manner.

2. Continuous Monitoring

Continuous monitoring is a formal activity in which a sample of control output is tested against pre-defined assessment criteria to determine if PF risks have been assessed and addressed sufficiently. It is conducted on a more frequent basis (e.g., monthly, quarterly) as compared to thematic reviews (e.g., annually) and is an alternative approach that may be adopted.

The key objective is to ensure quality and consistency in PF control throughput and performance. The consistent approach enables banks to keep a sound oversight through reporting of the PF risks that arise from the reviewed population.

4. Risk Mitigation

4.7 Compliance Monitoring and Testing

2. Continuous Monitoring

The continuous monitoring review consists of five steps. Each of the process steps should be undertaken and subsequently documented:

Sampling	Use of risk-based sampling allows the tester to better identify exceptions which could be more representative of the test population.
Assessment	Samples subject to continuous monitoring review are assessed based on the pre-defined assessment criteria. These criteria are developed in line with applicable regulatory requirements or internal P&Ps.
Feedback Loop	In order to foster knowledge sharing, continuous learning, and control improvement, sample testing results will be shared with appropriate stakeholders.
Reparation of Test Outcome	Upon receipt of test results, any identified shortcoming (with material issues) should be remediated by agreed action owners to drive quality improvement in the performance of PF controls.
Reporting and Management Information	The conclusive step of the continuous monitoring review is the reporting phase.

Best Practices

1. Designated person(s) in second line of defence

Designated person(s) with PF knowledge in the second line of defence should be appointed to conduct independent compliance testing using a risk-based approach to identify potential PF controls gaps. The designated person(s) should be independent from the execution of PF controls or processes and granted appropriate delegated authority to execute its testing, including access to relevant systems and information.

2. Determine appropriate sampling approaches based on objective and scope of review

Consider applying:

(i) statistical sampling which involves the use of techniques from mathematically constructed conclusions on the total population of control output; and

(ii) non-statistical sampling which may involve selecting samples based on PF risks, or data considering PF risks factors or criteria (e.g., number of transactions involving high PF risk jurisdictions, transactions involving parties whom the bank had filed a STR due to PF risk concerns etc.).

3. Analysis of recurrent issue

Consider conducting in-depth analysis of recurrent issues to identify root causes. Material issues may require a targeted remedial plan/action to be executed.

4. Clear reporting of testing results

Report on testing results should include trending (where relevant, specifically for continuous monitoring reviews), tracking of remediation actions, and reporting on overdue actions.

4. Risk Mitigation

4.8 Data Analytics Applications for Risk Mitigation

Investment in technology to use DA applications, including machine learning and artificial intelligence may help banks to identify previously unnoticed linkages and relationships, and to recognise patterns such as common adverse counterparties and geolocation that could have been difficult to recognise otherwise[21].

On 31 August 2023, MAS released a circular to banks in Singapore to encourage institution of a risk-based lookback mechanism to identify potentially higher risk customers based on past transactions, as they may in future seek to evade payment screening controls by using third-party transactions.

Banks may consider deploying DA on a tailored risk-based approach to detect sanctions and PF risks arising from customers and their transactions. Some examples include:

Applications	Description
Network and Transactional Link Analytics 	• Performing network and transactional link analytics upon specific trigger events or on a periodic basis to identify customers of the banks with relational (e.g., via common ownership, connected parties or common contact details) or previous transactional links to sanctioned persons or subjects of sanctions/PF concern, for further review
Thematic Data Slicing Scenarios 	• Developing and deploying thematic data slicing scenarios, which consider relevant PF trends and typologies to identify customers potentially posing PF/sanctions risks for a closer review by the banks • Data slicing scenarios may consider a combination of various customer profile or transactional attributes, in view of the typology identified
Macro-monitoring 	• Macro-monitoring of higher risk country to country payment corridors to identify potential spikes or unusual patterns for further investigation
Geo-location Data 	• Use of geo-location data, for example, for monitoring or blocking the operation of bank accounts from IP addresses in jurisdictions of higher PF risk

Best Practices

The risk-based DA programme should be formally documented and tailored according to the areas of material PF risks for the banks based on their business operations or customer base. The programme should consist of clear baseline parameters including, without limitation:

- scope of transactions to be reviewed and the lookback period to be applied for the analysis;
- frequency of running each DA scenario (e.g., annually, quarterly, or upon certain trigger events);
- risk-based approach towards reviewing accounts of customers flagged by the programme; and
- periodic review of the DA scenarios and techniques for continued effectiveness. The DA scenarios can be adjusted or decommissioned if they are no longer fit for purpose, or if the yield is low. Regular review will ensure that the bank's resources are effectively targeted to address areas of higher PF risk concern.

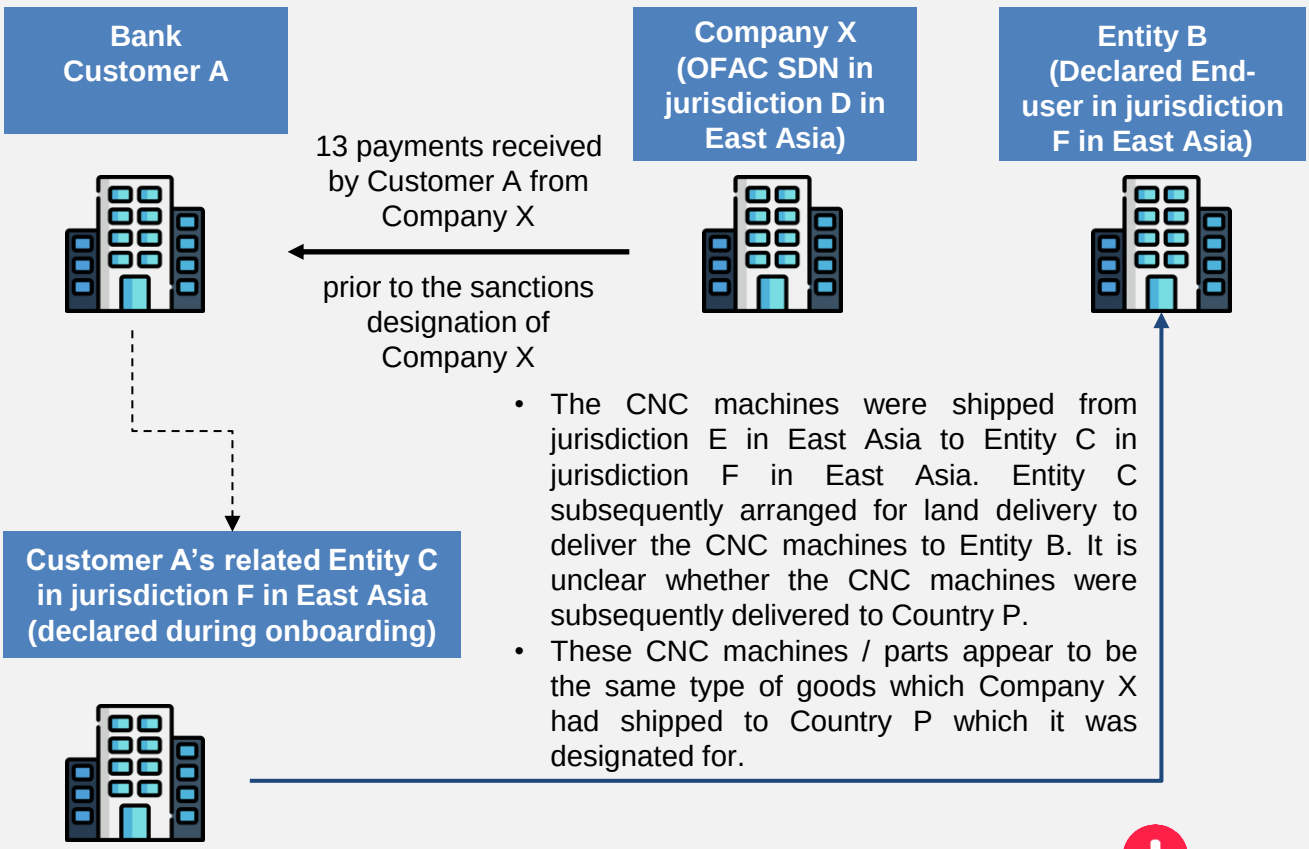
21 Please refer to FATF Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021), Para 73.

4. Risk Mitigation

4.8.1 Case Study 4 – Lookback Mechanism Revealing Sanctions Evasion Risks

In May 2024, Company X, an entity based in jurisdiction D in East Asia, was designated by OFAC for operating in the technology sector of Country P. Company X had shipped tens of millions of US dollars of foreign-produced CNC parts to a CNC distributor in Country P.

A Bank's Lookback Mechanism trawl identified Customer A which had 13 transactions with Company X in the year prior to its designation.



Additional checks on the corporate websites of Entity B (purported end-user) and Entity C (related entity of purported seller) revealed:

- Same Chinese name
- Same address in jurisdiction F in East Asia
- Common Ultimate Beneficial Owner

Customer A also provided questionable supporting documents and was not upfront in responding to the Bank's queries.

Relationship with Customer A was terminated and STR was filed given the red flags noted.

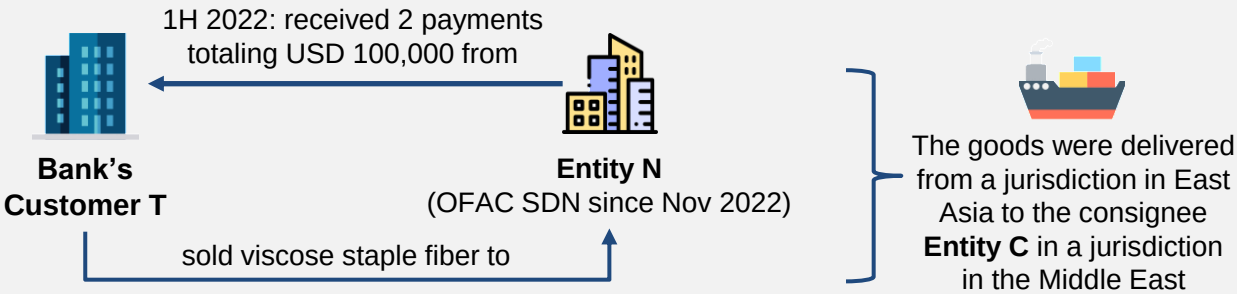
* All names have been redacted for the purpose of this case study.

4. Risk Mitigation

4.8.2 Case Study 5 – Counterparty Trawl Revealing Sanctions Risks Exposure

In November 2022, the US designated Entity N pursuant to US Executive Order 13846 for, on or after 5 November 2018, having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of sanctioned Iranian petrochemical brokers Persian Gulf Petrochemical Industry Commercial Co.

Via a counterparty trawl, the Bank identified its Customer T to have received 2 transactions from Entity N in 2022 prior to Entity N's designation.



The counterparty trawl enabled the Bank to uncover the Iran sanctions risk exposure from a deeper look at Customer T's counterparties named in the transactional documents.

Entity C (named as consignee in the Bill of Lading) was featured in adverse news (leaked documents from Iran's government agencies) to be a receiving / sending company for Iranian companies.

Several other counterparties named in the supporting documents for other transactions were similarly featured in adverse news for having:
(i) supplied goods to persons in Iran;
(ii) transacted with other potential Iranian front companies; or
(iii) been front companies for Iranian OFAC SDNs.

After a review, the banking relationship with Customer T was terminated and STR was filed in view of the PF/sanctions risks.

* All names have been redacted for the purpose of this case study.

5. Higher Risk Focus Areas

This section outlines higher risk focus areas that banks should consider in mitigating PF risks.

5.1 Open Account Trade and Dual-Use Goods

What are dual-use goods and open account trade?

- As defined in the Strategic Goods (Control) Act, "dual-use goods" are goods capable of being used for both a non-military purpose and a military purpose or relevant activity. The List of Dual-Use Goods is found in Division 2 of Part 2 of The Schedule to the Strategic Goods (Control) Order.
- Open account trade refers to "open account" settlement through wire transfers. Under open account trade, exporters ship the goods to the buyer and expect payment to be made under agreed terms at a future date, usually via remittances (i.e., without the use of documentary credits or collection).

Challenges in assessing dual-use goods and open account trade that may be of higher risk[22]

Dual-use goods	Open account trade

• It is challenging to determine if a particular good is dual-use given:
  • the technical aspect of the good;
  • vague description of the good;
  • uncertainty if the good will be used for non-civilian purposes; and
  • bank's staff may not necessarily possess the relevant technical qualifications and knowledge across a wide range of goods to allow them to understand the varying application of dual-use goods.
• For instance, metal sheets of certain specifications/characteristics are exported or transhipped to countries such as Iran or the DPRK, which can thereafter be used in the production of nuclear, chemical or biological weapons
	• Trade documents relating to a particular transaction may not be readily available to a bank, unlike in a documentary trade finance transaction where such documents are presented to the bank during the credit application process
	• The bank may have limited information on the underlying trade, such as the type and quantity of underlying goods, name and details of the buyer and seller, and the shipment

Heightened PF risks for dual-use goods with open account trade

PF risks vis-à-vis dual-use goods are elevated:

- when coupled with open account transactions to countries/geographical locations, which in the absence of any red flags are not being interdicted for payment and further due diligence on the transactions is not being performed to detect any PF risks; and
- for open account trade with underlying transactions involving dual-use goods, especially for cross-border trades.

<u>Other risk areas – Export/Import of goods from/to the DPRK</u>

- Despite a 2006 UNSCR prohibiting the export of luxury goods to the DPRK, the UNSC PoE on the DPRK observed that the DPRK has been able to obtain foreign goods (including luxury goods). Since 8 Nov 2017, Singapore has prohibited the import into, export from, transhipment in and transit through Singapore of all commercially traded goods from or to the DPRK. This goes beyond the DPRK-related UNSCR scope of prohibitions.

22 Refer to paragraph 6.6 of Singapore's PF NRA on challenges faced in identifying dual-use goods and ascertaining the use of dual-use goods for illicit purposes.

5. Higher Risk Focus Areas

This section outlines higher risk focus areas that banks should consider in mitigating PF risks.

5.1 Open Account Trade and Dual-Use Goods

Best Practices

Applying EDD on a risk-based approach as follows:

- Perform screening on additional parties involved in an open account trade[23] or transaction against individuals/entities listed in sanctions lists. These additional parties may be identified from documents or information obtained during the bank's inquiry into the said transaction. Banks may consider additional risk factors such as whether the flow of goods are to countries which are especially prone to being used as transhipment points to mask PF, as indicated by intelligence from authorities or those bordering sanctioned countries.
- Determine the end destination for the goods or services and if it involves jurisdictions which are susceptible to PF (e.g., Iran, DPRK), or under increased monitoring.

23 For the avoidance of doubt, screening on additional parties is also required for all other types of trade transactions.

5. Higher Risk Focus Areas

5.2 Correspondent Banking and Countries/Geographical Risk

What is correspondent banking?

- Correspondent banking involves one bank (the Correspondent) providing banking services to another bank (the Respondent). The Correspondent facilitates cross-border products and services for the Respondent's clients, acting as an agent or conduit. They execute payments or transactions for the Respondent's customers, such as individuals, companies, or legal entities.

Why correspondent banking is high risk and relevant PF risk

- As the Respondent's clients are typically not the Correspondent's own customers, they lack access to due diligence files of the originator/beneficiary, limiting understanding of transaction parties and activities.
- PF risks are elevated if the Respondent is linked to countries with weak AML/CFT controls or are not required by law to collect beneficial owner information. Additionally, a jurisdiction with a high level of crime, smuggling, fraud or other illicit activities also heighten PF risks.
- These geographies may also have less stringent export controls which conceal the true destination of the goods by seeking to establish themselves as the false end-user, obscuring the goods' true destinations and evading effective customs scrutiny. Goods may transit via smaller vessels, land, or air, complicating tracking.
- Correspondents face PF risks from processing payments for Respondents, exacerbating vulnerabilities.

Best Practices

Correspondent banking and geographical risk

- Aside from the higher ML/TF correspondent banking risk factors that will be considered as part of the CDD assessment, banks are also recommended to assess their Respondent's control framework on PF and decide whether these are within the bank’s own risk appetite.

- Banks may also consider supplementing the geographic risk assessment of PF with open-source information and/or published reports.

SWIFT message screening

- SWIFT’s messaging formats include certain optional general information fields in which ordering institutions may include additional information regarding the nature and purpose of the transaction, the identity of vessels or other related parties, and transport routes.

- Where practicable, correspondent banks should screen any additional information provided in optional payment message information fields by their respondent banks. This may include the name/IMO number of vessels or any other related parties, information regarding the type of underlying goods, and any ports (e.g., transhipment points).

5. Higher Risk Focus Areas

5.3 Shell & Front and Broking Companies

What is a shell and front company?

A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees. Typically, they serve as conduits or holding companies, whilst a front company is a fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit activity.

PF risk for shell/front and broking companies

- Shell/front companies may establish procurement networks for Iran/DPRK to acquire dual-use or restricted technologies used to obscure impending oil purchases and shipments to Iran/DPRK or are registered as ship owners where the vessels are ultimately controlled by Iran/DPRK.
- Brokers or intermediaries negotiate, arrange and facilitate transactions involving the transfer of goods or services under their ownership. This obscures the true ownership or destination of transactions concealing PF activities. Such complexity in TM and screening can obscure the involvement of sanctioned individuals/entities in transactions.

Common PF Red Flags Associated with Shell/Front and Broking Companies[24]

Banks can consider the following PF-centric red flags in its assessment for PF. The existence of a single standalone indicator in relation to a customer or transaction may not alone warrant suspicion.

a. Customer is incorporated, located or has connections with diplomatic offices or trade offices in a country that has weak export controls, financial regulation, or are known to be near countries with WMD programmes.

b. Certain customers' business types or activities may present inherent PF risk, such as manufacturers or suppliers of industrial materials, particularly dual-use goods. The PF risk may be higher if, for example, the company has a record of export-control violations or is a small trading company with limited information in the public domain.

c. If a customer is dealing with dual-use goods or goods subject to export control or complex equipment, consider whether the individuals in charge of the company have the technical background or expertise, that is aligned to the customer’s declared business activities.

d. Customer who is a manufacturing or trading firm uses cash to settle the purchase or sale of goods with its overseas suppliers or buyers, in an industry that is not known to be cash intensive or uncommon for settlement of commercial transactions to be done in cash.

e. Customer may receive payments from third parties with no connection to the underlying commercial transaction for settlement of sale and is not related to the buyer of the goods. Transactions may also be settled based on “ledger” arrangements which negate the need for cross-border fund transfers.

f. Customer does not have significant assets or business activities and presents itself as a wholesale trader of products such as electronics, textiles, and construction and industrial equipment, which may provide a cover for illicit cross-border fund transfers.

g. Customer demonstrates weak due diligence or awareness of its supply chain which may act as a conduit to obfuscate the true destination of the goods or counterparties involved.

24 Please refer to FATF Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021) and ACIP’s Legal Persons – Misuse Typologies and Best Practices Paper (May 2018) for further details on red flags and best practices when dealing with shell and front companies.

5. Higher Risk Focus Areas

5.4 Maritime Activities

Why is the maritime sector exploited?

The maritime sector has been observed to facilitate sanctioned individuals/entities' transport of components and materials for WMD or their delivery systems. Such individuals/entities could also misuse the maritime sector to generate revenue which can provide the underlying financing for a WMD programme.

What should banks look out for?

Banks should be aware of the common deceptive shipping practices which may be indicative of PF and employ due diligence measures to mitigate PF risks. Deceptive shipping practices which may be used to conceal illicit trade or prohibited activities encompass various methods such as:

a) vessel "spoofing" by falsely transmitting identity via AIS as different-flagged vessel using different IMO number;
b) disabling or manipulating the AIS;
c) vessel false flags/flag hopping;
d) ship-to-ship transfers and/or loitering in high-risk areas; and
e) voyage irregularities, such as highly convoluted vessel journeys such as indirect routes, unscheduled detours and transit or transhipment through low-risk third countries.

The presence of indicators do not necessarily imply that prohibited activity has taken place. There may be legitimate reasons for a vessel to not broadcast its identity via AIS or have gaps in its AIS broadcast (e.g., signal interruptions due to particularly dense traffic, fears of piracy), or conducting ship-to-ship transfers (e.g., vessel is too big for a terminal, avoiding port fees).

Best Practices

Banks should implement monitoring (including considerations of the following indicators) on a risk-based approach aligned with their compliance framework when reviewing transactions.

False flag/Flag hopping

To address potential risks associated with false flagging or flag hopping for vessels, banks may consider implementing EDD into their vessel review processes. This includes analysing and verifying vessel registrations and ownership details, conducting sanctions screening, tracking IMO numbers, monitoring vessel movements, and validating relevant documents, where available and applicable, through reliable resources such as industry partners in the maritime sector and credible data providers.

Manipulation or gaps in AIS

Repeated, prolonged, and unexplained AIS gaps, especially in higher risk locations should be investigated further. Banks should assess such activity on a case-by-case basis, considering the vessel type, its area of operations, its cargo, whether the AIS gap is a one-off occurrence or a sustained pattern, and the presence of other red flags.

Ship-to-ship transfers and/or loitering in high-risk areas

Banks should pay attention to vessels that are loitering in areas known for ship-to-ship transfers intended to bypass sanctions regimes[25], especially when there are also other red flag indicators such as disabling of AIS, vessel movement showing that it is repeatedly moving back and forth between a port and a known ship-to-ship transfer zone, or the vessel having draft changes at sea.

Voyage irregularities

Indirect shipping routes, unscheduled detour, or transhipment through a low-risk third country may be used to obfuscate the ultimate origin or destination of the cargo and/or the vessel. Banks should pay attention to voyages that deviate from the known business activities of their customers or the usual trade flows and ascertain whether there is an economic rationale for the shipping routes.

25 For example, STS involving the DPRK are known to take place in the Yellow Sea, Sea of Japan, East China Sea, and the Gulf of Tonkin. For sanctions concerning Iran, STS is known to take place in the seas off the UAE port of Fujairah.

6. Role of Public-Private Partnerships and Importance of Information Sharing to Combat PF

This section highlights the significance of information sharing and presents examples of existing partnerships and initiatives designed to promote public-private sector cooperation, thereby enhancing the effectiveness of managing ML/TF/PF risks.

6.1 Background

- Criminals adapt to existing CPF measures deployed by banks, adjusting their methodologies to circumvent controls from fund movement and goods transfer.

- As a result, in Singapore, there has been strong efforts in recent years to encourage information sharing and public-private sector cooperation to enhance ML/TF/PF risk management effectiveness and to bolster the AML/CFT system.

6.2 Importance of Information Sharing

- Through public-private partnerships, government agencies, banks, non-bank entities and other sectors can collaborate by sharing case studies to raise awareness of ML/TF/PF risks and publishing best practice papers for banks to adopt and implement in their AML/CFT/CPF framework. This collaboration aims to elevate the AML/CFT/CPF standards across the industry.

- Currently, all banks collect data and information on their customers. Some banks may have intelligence available only to them, whilst others lacking such data may be more vulnerable to exploitation by criminals employing PF methods. Criminals may attempt transactions through different banks, and those lacking intelligence may struggle to detect and disrupt illicit activities promptly.

- Establishing an information sharing platform is critical in combatting PF, enabling both public and private sectors to access data for effective detection of potential PF transactions and identification of entities or bad actors with PF concerns. Public-private partnership can enhance intelligence sharing mechanisms, enabling proactive ML/TF/PF risk management.

- An expanded, rapid information sharing mechanism amongst like-minded banks can curb potential circumvention efforts. Banks proficient in detecting PF sanctions evasion techniques can uplift smaller, local partners, non-bank entities, and public sector entities through enhanced engagement mechanisms, and industry outreach.

- Both public and private sectors should leverage on information sharing platforms and explore possibilities on using DA. By leveraging DA, entities across industries can enhance their detection capabilities of ML/TF/PF risk factors when dealing with customers, potentially uncovering broader criminal networks.

- Closer collaboration between public and private sectors facilitates the exchange of pertinent information with government agencies, aiding in the initiation and pursuit of investigations regarding potential violations of TFS. This strengthens the government's capacity to assess PF risk at a national level.

- Any changes to the relevant UNSC sanctions lists would be given immediate effect domestically. The obligations to freeze the assets of, and to not deal with, UNSC-designated individuals and entities would thus apply immediately, and any frozen assets should be reported to the relevant Singapore authorities as soon as possible.

6. Role of Public-Private Partnerships and Importance of Information Sharing to Combat PF

6.3 Existing Partnerships and Information Sharing Initiatives

- MAS publishes information and guidance papers to highlight key trends and practices in the financial industry, sharing best practices from reviews and inspections.

- In the public-private partnership space, ACIP collaborates across sectors to identify, assess and mitigate ML/TF/PF risks exposed to Singapore.[26] These initiatives involve establishing working groups and issuing ACIP Best Practice Papers to guide banks on implementing control measures to detect and prevent illicit financial activities.

Collaborative Sharing of ML/TF Information & Cases ("COSMIC")

- Through COSMIC, a secured digital platform managed by MAS, banks will be able to share risk information regarding suspicious customer behaviour and unusual transactions. This facilitates better identification of illicit networks, validation of customer explanations, and mutual warning of potentially suspicious activities amongst banks.

- Enabling banks to share information on customers surpassing specific risk thresholds helps dismantle "information silos" and enhances detection and disruption of criminal activities, reducing potential harm to the integrity of Singapore's financial centre.

6.4 Benefits for the Industry

3 Key Benefits

1. Sharing of insights from national risk assessments and typologies to strengthen the focus on key risks, hence enabling better effectiveness of risk-based controls and closing the gap on any vulnerabilities

2. Sharing of specific data/information on anomalous behaviours of clients

3. Collaborative information sharing and analysis between public and private sectors facilitate law enforcement agencies' efforts to derive actionable intelligence, enabling the disruption of any criminal attempts to exploit Singapore for PF

    - Since 2019, the CAD and MAS, through the ACIP partnership, have closely collaborated with major banks on specific cases and targets where intelligence and leads are exchanged using a hub-and-spoke model to uncover new leads and conduct further analytics.

    - These collaborative efforts have culminated in successful interceptions of about S$69 million, including more than S$19 million of incoming funds that were blocked through the banks' proactive identification of suspicious accounts.[27]

26 Refer to paragraph 7.3 of Singapore's PF NRA for details on how Singapore detects and shares information on emerging PF risks.

27 Keynote Speech by Ms Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime), MAS, at the ACAMS 12th Annual AML & Anti-Financial Crime Conference – APAC on 27 April 2021.

7. Managing PF Risks for Non-Banks

This section sets out the best practices observed in five non-banking sectors, which may be adopted by non-banks as appropriate in their course of business. These non-banking sectors were also identified in Singapore's PF NRA as being exposed to varying levels of PF risks.

7.1 Background & Introduction

Whilst this paper primarily focuses on understanding and managing PF risks within banks, it is worth noting that PF is a growing concern for other non-bank entities as well.

Non-bank entities might inadvertently engage in transactions or activities that facilitate proliferation or PF, particularly if they have global operations or deal with individuals/entities involved in sensitive industries such as defence, technology, or dual-use goods.

To gain a deeper understanding of PF risks within these non-banking sectors, a survey encompassing five sectors was conducted to gather insights into the current landscape. Workshops were also held with these participants to gain a better understanding of the responses provided. This section highlights the good practices observed from the contributions of the various sectors below.

Red flag indicators as provided by the non-bank entities were generally aligned with the banking sector. For the full list of indicators, please refer to section 2.1 and Appendix A.

Non-banking sectors that participated in the development of this section[28]:

- CSPs
- DPTSPs
- Law firms
- Maritime insurers
- Remittance agents

Sources

To aid in the detection of PF, non-bank entities, similar to banks, may rely on a list of sources for guidance on PF risks and list of sanctioned individuals/entities. These sources could originate from local regulatory bodies like MAS or from international organisations such as the UNSC. A non-exhaustive list of sources can be found in Appendices B & C.

7.2 Suggested Best Practices based on Observations

- Firms are encouraged to conduct PF risk assessments and implement the appropriate PF risk mitigation measures. If current methodologies for ML, TF and sanctions risk assessments adequately address PF risks, a separate assessment may not be necessary. PF risk management and controls can be integrated into the existing EWRA programmes and processes.

- Firms are encouraged to establish policies, procedures and frameworks to address PF risks. CPF policies, procedures and frameworks need not operate independently from existing AML, CFT or sanctions policies, procedures and frameworks, and some firms' existing AML controls already cover CPF (e.g., sanctions screening, EDD for higher-risk countries).

- Firms are encouraged to establish a periodic frequency of updating their P&Ps. The frequency of updates may be adjusted dependent on the size and risk appetite of the firm, taking into account its activities and customer profiles.

- Senior management are actively involved in the escalation process and approval of PF-related policies, procedures and frameworks.

28 Singapore's PF NRA listed precious stones and precious metals dealers as a sector to watch. Refer to section 6(F) of Singapore's PF NRA.

7. Managing PF Risks for Non-Banks

7.3 Measures for Risk Mitigation

Based on the survey and workshops conducted, these risk mitigation measures were commonly employed within the non-banking sectors. Below are examples of measures observed across the five sectors that other non-bank entities can apply when developing their PF controls:

Firms were observed to have implemented CDD and EDD measures, including identification and verification of the identities of customers and their beneficial owners, corroboration of source of funds/wealth, screening (e.g., adverse news screening, screening against UNSC and other unilateral sanctions lists, customer name screening, transaction screening), and ongoing monitoring of customers and transactions. Generally, firms conduct periodic reviews or trigger reviews as part of these measures. These were generally applied to customers, declared counterparties, directors, and beneficial owners.

In addition to the above measures, firms have also implemented other risk mitigation measures such as training programmes on PF, escalation to compliance/ML reporting officer ("MLRO")/senior management/risk committees for approval for high-risk PF cases, prohibition on dealings with sanctioned countries and sanctioned individuals and maintaining a firmwide country/product list for high PF risk items.

Furthermore, these are some non-exhaustive sector specific PF-related risk mitigation measures observed in the following sectors[29]:

Sector	Sector Specific PF-related Risk Mitigation Measures Observed
CSPs	• CSPs are required to flag out corporate entities that may have no real economic purpose or that may have been incorporated for the purpose of circumventing sanctions. These could include corporate entities involved in potentially higher-PF risk activities, which may include shipping and providing flags of convenience. From July 2024: • Business entities that carry on a business of providing corporate services from Singapore are required to register as CSPs and be subject to AML/CFT regulation by ACRA • ACRA has made explicit that CSPs have to comply with CPF obligations, including the requirement to conduct PF risk assessments
DPTSPs	**IP address:** • Using IP login data and other indicators of geographic locations to geolocate and determine if parties are covertly operating in prohibited jurisdictions with high sanctions and PF risks • Implementing geo-blocking solutions provided by service providers to evaluate potential loopholes through IP access to prevent the onboarding of users from sanctioned jurisdictions • Conducting video calls for non-face-to-face verifications, including the use of service providers for authenticity checks. Customers are required to turn off their VPNs for IP matching to identify any jurisdiction mismatches

29 Refer to section 6 of Singapore's PF NRA.

7. Managing PF Risks for Non-Banks

7.3 Measures for Risk Mitigation

Sector	Sector Specific PF-related Risk Mitigation Measures Observed
DPTSPs (continued)	**Blocklist(s):** • Regularly and promptly blocklisting blockchain addresses owned/controlled/ exploited by sanctioned actors and designated by relevant authorities • Maintaining a blocklist of wallet addresses which the firm prohibits from transacting **Crypto wallet addresses:** • Utilising in-house solutions to prevent sending to or receiving from a sanctioned crypto address • Impacted crypto assets are placed into a suspense account and reported • Real time crypto wallet address screening
Law Firms	• The Law Society of Singapore has issued a Practice Direction that provides guidance to lawyers on the discharge of their AML/CFT/CPF obligations • From February 2024, Ministry of Law has made explicit that lawyers and law practice entities have to comply with CPF obligations
Maritime Insurers	• In most cases, maritime insurers' contracts would have carve out clauses to void any insurance coverage should there be sanctions concerns (including those relating to UNSC sanctions as well as other relevant unilateral sanctions) **AIS:** • Checking of AIS history at onboarding • Continuously monitoring of fleet via AIS **Watchlist:** • For shipments involving watchlist territories, the insurers are required to refer each voyage declaration to the compliance team for approval prior to the provision of any coverage • Monitoring in general if any insured vessels are on any port calls to or near sanctioned jurisdictions
Remittance Agents	• Some remittance agents have built up DA capabilities and thus have been able to detect and block potential sanctions evasion

8. Conclusion

This paper is intended to help both banks and non-bank entities by setting out best practices to be taken into consideration when assessing PF risks. Banks and non-bank entities should review their existing practices against this paper and consider if there are areas that they can enhance to raise the effectiveness of managing PF risks.

Combatting PF activities in Singapore requires a collective effort as banks working independently may create vulnerabilities exploited by criminal networks skilled in evading detection. Evasion techniques such as transaction layering, shell entities, and cryptocurrency use contribute to this challenge.

Strengthening existing public-private partnerships and information sharing frameworks can enhance effectiveness in addressing these challenges.

Appendices

Appendix A: List of PF Risk Factors and Indicators

This section provides a non-exhaustive list of PF risk factors and indicators for both banks and non-banks to take into consideration when assessing PF risks for their firm/entity. Banks and non-banks are encouraged to refer to the Guidelines to MAS Notice 626, MAS' 2018 Sound Practices to Counter Proliferation Financing, FATF's 2018 Guidance on Counter Proliferation Financing, FATF's 2021 Guidance on Proliferation Financing Risk Assessment and Mitigation for more guidance on the identification of red flags.

General Risk Factors

- Non-party to relevant international conventions and treaties on WMD non-proliferation
- Lack of implementation of relevant UNSCR
- Presence of industries producing WMD components or dual-use goods
- Nature of the jurisdiction's export trade both in terms of volumes and geographical end-users
- Lack of working coordination between the customs authority and the export licensing authority of a specific jurisdiction
- A jurisdiction that has secondary markets for technology

Customer Risk

- Customer, particularly a trade entity, its owners, or senior managers, appears in sanctions lists or negative news related to ML/TF/PF activities
- Customer deals with dual-use goods incongruent with their stated line of activity or technical background
- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding
- A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control
- Ownership structure of the customer appears unusual or excessively complex given the nature of its business
- Customer or counterparty is involved in the maritime industry, particularly those who own, operate, and/or provide services (e.g., bunkering, ship-to-ship transfer, flagging) to vessels operating in regions identified as having higher risk of sanctions evasion
- Customer and/or beneficial owner(s) are from higher PF risk jurisdictions or nature of work involves higher PF risk industries
- Customer is a trade entity operating at an address which has been flagged for PF concerns, or where the operating address may not be congruent with the nature of business (e.g., a residential address).

Geographic Risk

- Movement of people and funds to/from high-risk countries may facilitate PF activities
- Geographic proximity, trade hubs, or free trade zones may be used for transhipment of dual-use goods to proliferation-prone countries
- Connections with high-risk jurisdictions engaged in WMD proliferation or PF activities (e.g., DPRK, Iran)
- IP hits from countries with weak AML/CFT controls indicate potential PF risks

Delivery Channel Risk

- Customer utilises a DPTSP or foreign-located money value transfer service provider in a high-risk jurisdiction of proliferation concern that lacks or is known to have inadequate, AML/CFT (including CPF/sanctions) regulations for DPTSPs, including inadequate CDD or KYC measures

Appendices

Appendix A: List of PF Risk Indicators and Factors

Transaction Risk

- The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern (i.e., DPRK and Iran)
- Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes
- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g., companies do not have a high level of capitalisation or display other shell company indicators. Countries or the private sector may identify more indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity
- Account activity or transactions where the originator or beneficiary of associated banks is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF standards or a weak export control regime (also relevant to correspondent banking services)
- Customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For banks, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals
- Transaction screening identifies negative keywords (e.g., ammunition)
- Transactions with indication of higher crime risks such as association with sanctioned parties, frauds, ML, and other criminal activities

Sector Specific PF Risk Indicators

Maritime Sector

- Shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet
- Insured vessel's AIS transponder has been turned off or manipulated
- AIS manipulation or gaps
- Flag of vessels from higher PF risk jurisdictions

Trade Finance Risk Indicators

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

Appendices

Appendix B: List of Potential Sources for Threats Identification

Banks can refer to the following list of potential sources for the identification of threats:

Internal Sources for Threat Identification

- Firm and group-wide databases containing CDD information collected during onboarding and ongoing due diligence - additional focus should be spent on the beneficial ownership of legal persons and arrangements
- Transaction records (if available) involving the sale of dual-use goods or goods subject to export control
- Internal controls rules designed to identify sanctioned individuals/entities and those acting on their behalf or at their direction may also be relevant
- TM and screening, as well as internal audit and regulatory findings

External Sources for Threat Identification

International & National Typologies / Case Studies

- Threat analysis reports/National PF risk assessments (from Singapore and other relevant jurisdictions where the bank operates)
- Supervisory circulars and guidance
- UNSC PoE reports (including cases involving possible proliferation/PF activities)
- Breach, non-implementation or evasion of PF-TFS

Data/Intelligence Information from Government Agencies

- Financial intelligence and law enforcement data
- Designated persons list
    i. MAS Lists of Designated Individuals and Entities
    ii. UNSC Consolidated List
- Customs documents
- Domestic and foreign intelligence on:
    i. Global, regional, and national proliferation threats
    ii. Source, movement, and use of funds by sanctioned individuals/entities, as well as those acting on their behalf or at their direction, and with close connections to countries of proliferation concerns (i.e., DPRK and Iran)
    iii. Intelligence on potential PF activities (including those from foreign intelligence agencies, where available)

Information from Competent Authorities (in relation to Customers & Transactions)

- Names of specific entities and persons potentially tied to proliferation networks, as well as end-users of particular concern regarding items, materials, equipment, goods and technology prohibited under the country-specific resolutions, including lists provided by national export control authorities, where applicable
- Available typologies of PF (not limited to those typologies identified by the private sector stakeholders)
- Lists and/or characteristics of persons who have been granted or denied export licences and associated transactional details (e.g., type of goods involved, export routes, methods of financing, and the rationale for denial)
- Information relating to the diversion of items, materials, equipment, goods and technology prohibited under country-specific resolutions

Public-Private Partnership

- Relevant information obtained through public-private information sharing initiatives

Appendices

Appendix C: List of Considerations for Vulnerabilities Identification

Banks can refer to the following list of considerations for the identification of vulnerabilities:

Considerations for Vulnerabilities Identification
• Number of customers already identified as high risk, especially those often carrying out cross-border transactions involving legal persons and arrangements, or multiple shell or front companies • Information on the type and identity of the customer, as well as the nature, origin and purpose of the customer relationship • Other considerations include the number, amount (especially in cash), and frequency of transactions • Originating from, transiting through, or designating for an overseas jurisdiction that has weak implementation of relevant UNSCR obligations and FATF standards, weak governance, law enforcement, and regulatory regimes • Involving individuals acting on behalf of a legal person or arrangement (e.g., authorised signatory, director) • Transactions unrelated to a firm's stated business profile • Vulnerabilities associated with products and services of banks such as correspondent banking services and trade finance

Appendices

Appendix D: Working Group Members and Other Contributors

Working Group Members	
Bank	**Representative**
Oversea-Chinese Banking Corporation Limited (OCBC)	Loretta Yuen (Co-Chair)
HSBC Bank (Singapore) Limited (HSBC)	Robert Oates (Co-Chair)
Oversea-Chinese Banking Corporation Limited (OCBC)	Fairlen Ooi
Oversea-Chinese Banking Corporation Limited (OCBC)	Abrie Lee
Oversea-Chinese Banking Corporation Limited (OCBC)	Koh Mun Keong
HSBC Bank (Singapore) Limited (HSBC)	Shane Godwin
HSBC Bank (Singapore) Limited (HSBC)	Angela Kwa
Citibank Singapore Limited (Citi)	Toh Ziki
Citibank Singapore Limited (Citi)	Hazel Cheok
DBS Bank Ltd. (DBS)	Christine Koh
DBS Bank Ltd. (DBS)	Joyin Leong
Deutsche Bank Aktiengesellschaft (DB)	Kevin Chua
Deutsche Bank Aktiengesellschaft (DB)	Chan Su Leng
Deutsche Bank Aktiengesellschaft (DB)	Gregory Tan
United Overseas Bank Limited (UOB)	Yu Beng Soon
Standard Chartered Bank (Singapore) Limited (SCB)	Murugesan, Anandan

Professional Services	Representative
Ernst & Young Advisory Pte. Ltd. (EY)	Radish Singh
Ernst & Young Advisory Pte. Ltd. (EY)	Nicholas Sebastian
Ernst & Young Advisory Pte. Ltd. (EY)	Janell Joseph
Ernst & Young Advisory Pte. Ltd. (EY)	Eunice Aw

ACIP Secretariat
Commercial Affairs Department (CAD)
Monetary Authority of Singapore (MAS)

Appendices

Appendix D: Working Group Members and Other Contributors

Working Group Members (Non-Banks)
Accounting and Corporate Regulatory Authority (ACRA)
Association of Small & Medium Enterprises (ASME)
QBE Insurance
Singapore Customs
The Law Society of Singapore

Appendices

Appendix E: References

1. Accardi, E. (2020, April 23). *A Hull in Their Story: Satellite Imagery, AIS, and the Ships Secretly Transporting Iranian Gas to China.* C4ADS. https://c4ads.org/commentary/2020-4-21-hull-in-their-story/

2. ACIP, 'Best Practices for Countering Trade Based Money Laundering', May 2018, Section 4.3. https://abs.org.sg/docs/library/best-practices-for-countering-trade-based-money-laundering.pdf

3. ACIP, 'Legal Persons – Misuse Typologies and Best Practices', May 2018. https://abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf

4. Albright, D. et al. (2021, September 22). *The Peddling Peril Index for 2021/2022*. Institute for Science and International Security. https://isis-online.org/uploads/isis-reports/documents/ThePeddlingPerilIndex2021_POD_wCover.pdf

5. Arterburn, J. (2018, August 2). *Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System*. C4ADS. https://c4ads.org/reports/dispatched/

6. Arterburn, J. et al. (2019, July 16). *Lux & Loaded: Exposing North Korea's Strategic Procurement Networks*. C4ADS. https://c4ads.org/reports/lux-loaded/

7. Bartlett, J. (2020, November 18). *Exposing the Financial Footprints of North Korea's Hackers.* Center for a New American Security. https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers

8. Boling, A. et al. (2021, September 9). *Unmasked: Vessel Identity Laundering and North Korea's Maritime Sanctions Evasion*. C4ADS. https://c4ads.org/reports/unmasked/

9. Byrne, J. et al. (2019, September 26). *Project Sandstone Report 4: Down and Out in Pyongyang and London*. RUSI. https://www.rusi.org/explore-our-research/publications/special-resources/project-sandstone-report-4-down-and-out-pyongyang-and-london

10. Byrne, J. (2020, September 4). *Project Sandstone Report 7: The Billion-Dollar Border Town: North Korea's Trade Networks in Dandong (Part 1)*. RUSI. https://rusi.org/explore-our-research/publications/special-resources/project-sandstone-report-7-billion-dollar-border-town-north-koreas-trade-networks-dandong-part-1

11. Erskine, S. (2022, January 5). *North Korean Proliferation Financing and Designated Non-Financial Businesses and Professions*. RUSI. https://rusi.org/explore-our-research/publications/emerging-insights/north-korean-proliferation-financing-and-designated-non-financial-businesses-and-professions

12. FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf

13. Kuo, L. et al. (2021, March 22). *Black Gold: Exposing North Korea's Oil Procurement Networks.* C4ADS. https://c4ads.org/reports/black-gold/

Appendices

Appendix E: References

14. MAS, 'Guidelines on Individual Accountability and Conduct', September 2020, Section 4. https://www.mas.gov.sg/-/media/mas/mpi/guidelines/guidelines-on-individual-accountability-and-conduct.pdf

15. MAS (2021, April 27). *Keynote Speech by Ms Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime).* ACAMS 12th Annual AML & Anti-Financial Crime Conference – APAC. https://www.mas.gov.sg/news/speeches/2021/acams-12th-annual-aml-and-anti-financial-crime-conference-apac

16. MAS, 'Singapore's 2024 Proliferation Financing (PF) National Risk Assessment and Counter-PF Strategy', 30 October 2024. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/proliferation-financing-national-risk-assessment.pdf

17. MAS, 'Sound Practices to Counter Proliferation Financing', August 2018, Section 4.4. https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/anti_money-laundering_countering-the-financing-of-terrorism/pf-guidance-13-aug-2018.pdf

18. UK HM Treasury, 'National risk assessment of proliferation financing', September 2024. https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing

19. United Nations Security Council, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2019/171', 5 March 2019. https://www.undocs.org/S/2019/171

20. United Nations Security Council, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2020/151', 2 March 2020. https://undocs.org/S/2020/151

21. United Nations Security Council, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2020/151', 4 March 2021. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf

22. US Department of the Treasury, 'Deceptive Practices by Iran with respect to the Civil Aviation Industry', 23 July 2019. https://ofac.treasury.gov/media/16611/download?inline

23. US Department of the Treasury, 'Guidance to Address Illicit Shipping and Sanctions Evasion Practices', 14 May 2020. https://ofac.treasury.gov/media/37751/download?inline

24. US Department of the Treasury, 'National Proliferation Financing Risk Assessment', February 2024. https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf

25. US Department of the Treasury, 'Risks for Businesses with Supply Chain Links to North Korea', 23 July 2018. https://ofac.treasury.gov/media/7721/download?inline