المكتب التنفيذي
للرقابة وحظر الانتشار
EXECUTIVE OFFICE FOR
CONTROL & NON-PROLIFERATION

Proliferation Finance Institutional Risk Assessment Guidance

For FIs, DNFBPs, and VASPs

Published: December 2023

Table of Contents

Acronyms

EOCN	The Executive Office for Control & Non-Proliferation
CPF	Counter Proliferation Financing
PF	Proliferation Financing
AML	Anti-Money Laundering
CTF	Counter Terrorist Financing
FATF	Financial Action Task Force
ML	Money Laundering
TF	Terrorist Financing
FIs	Financial Institutions
DNFBPs	Designated Non-Financial Businesses & Professions
VASPs	Virtual Asset Service Providers
CRS	Customer Risk Scoring
RA	Risk Assessment
STR / SAR	Suspicious Transaction Report / Suspicious Activity Report
FIU	Financial Intelligence Unit

RBA	Risk-Based Approach
UBO	Ultimate Beneficial Owner
PEPs	Politically Exposed Persons
OFAC	Office of Foreign Assets Control – US Treasury
UN	United Nations
WMD	Weapons of Mass Destruction
UNPoE	United Nation’s Panel of Experts
NRA	National Risk Assessment
KYC	Know Your Customer
CDD	Customer Due Diligence
SMOs	Senior Managing Officials
EDD	Enhance Due Diligence
DUGs	Dual-Use Goods
TCSPs	Trust & Company Service Providers
DPRK	Democratic People’s Republic of Korea

Section 1: Introduction and Purpose

1. The Executive Office for Control and Non-Proliferation (EOCN) has a central role to play in setting the regulatory and legal landscape, as well as in coordinating efforts to fight proliferation finance (PF) in the UAE. However, the cooperation of the private sector is essential to achieve an effective national and hence, global counter-proliferation finance (CPF) framework. To achieve this, the EOCN advises the private sector to leverage existing Anti Money Laundering (AML) and Counter Terrorism Financing (CTF) governance and frameworks to deliver effective CPF.

2. In 2020, the Financial Action Task Force (FATF) updated its recommendations to require FIs, DNFBPs, and VASPs to "identify, assess, and take effective action to mitigate"[1] their **proliferation financing risks**, in addition to their money laundering (ML) and terrorist financing (TF) risks.

3. This document is an addendum to the Guidance on Counter Proliferation Financing for Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs) and Virtual Assets Service Providers (VASPs) and aims to provide additional support to the private sector as to how to identify, assess and mitigate PF risk.

4. The document comprises of 5 sections, including the introduction. Section 2 provides a suggested methodology to assess PF risk. Section 3 provides an overview of controls in place within the private sector to support the mitigation of PF risk. Section 4 documents questions that the private sector is suggested to ask customers as part of the PF risk scoring process. Finally, Section 5 documents PF case studies and provides a walkthrough of how to complete the customer risk scoring (CRS) questionnaire as applied to the case studies.

5. Note that FIs, DNFBPs and VASPs may benefit from the documented PF risk assessment methodology and tailor their existing internal processes when conducting a risk assessment to include PF.

[1] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', 2012, Recommendation 1, p. 10.

Section 2: PF Risk Assessment Methodology

6. It is understood that each institution will have its own risk assessment (RA) methodology for ML and TF. It is therefore recommended that institutions leverage their existing RA methodology to assess PF risk.

7. The PF risk assessment methodology is based on three key steps:

   i. Evaluate the inherent risks;

   ii. Assess the effectiveness of existing controls in place to mitigate risk; and

   iii. Determine the residual risk.

Inherent risks

8. To conduct a risk assessment, the private sector should assess the inherent PF risk of the following categories:

   - Customers;
   - Business activity, occupation and/or industry of customers;
   - Geographic location;
   - Products, services and transactions (new and existing);
   - Delivery channels (new and existing); and
   - Cyber threats to the systems and software used.

9. Each of the abovementioned risk categories needs to be assessed based on a set of PF risk factors (those are discussed in more detail in Section 3). In order to understand how this is done, it is fundamental to first discuss how the inherent risk of each of those categories can be evaluated.

10. **Inherent risk** is the risk an institution is exposed to without considering the controls it has in place to mitigate such risks. Inherent risk is determined by:

    - **PF threats** and **vulnerabilities** of your institution: E.g., what threats do the jurisdictions you operate in face, what vulnerabilities do the jurisdictions you operate

in have. Factors that affect vulnerability of the business may include nature, scale, diversity and geographical footprint of the business, target market and customer profiles, volume and size of transactions.

- **New** and **existing issues** identified by internal and external audits, quality assurance, investigations and/or reporting of suspicious activity reports (SARs) and suspicious transactions reports (STRs) to the Financial Intelligence Unit (FIU);

- Your institution's **commercial strategy** and **risk appetite**: Decisions relating to jurisdictions you will operate in, customer types you will be servicing, products and services you will be offering;

- **Built-in constraints**: The inherent risk is determined by existing constraints (such as technical restrictions of delivery channels for instance or nature of products, services or delivery channels.)

11. The inherent risk can then be assessed based on three risk score levels as documented in Table 1:

Table 1: Inherent risks

Low	**Limited or no indicators of:** - Threats and vulnerabilities - New and existing issues - Risk appetite - Inherent high-risk constraints
Medium	**Some indicators of:** - Threats and vulnerabilities - New and existing issues - Risk appetite - Inherent high-risk constraints
High	**Numerous indicators of:** - Threats and vulnerabilities - New and existing issues - Risk appetite - Inherent high-risk constraints

Control effectiveness

12. The effectiveness of controls is determined by two considerations: whether the control is **adequately designed**, and whether the control is **effectively operated** by the institution to mitigate the inherent risks.

13. Testing the design of a control aims to validate whether the control would prevent or detect risk. For instance, an institution may state that there is a customer PF risk scoring process in place for all new customers. To test the design of this control, one would review evidence demonstrating that customer risk scoring has been implemented and has been designed in a way that accurately risk scores customers.[2]

14. An **adequately designed control** is not sufficient. The control also needs to be operated and performed effectively. Testing the **operating effectiveness of a control** aims to identify whether the control is performed and/or operated as it was intended to. In the case of the customer risk scoring example, a sample of customer risk score questionnaires will be selected, and the risk scoring be re-performed to determine whether the process was effectively followed as per the institution's existing procedures.

15. Once an institution has assessed both the design and operating effectiveness of its controls, it can determine overall control effectiveness. A score will be assigned as documented in Table 2.

Table 2: Criteria for design and operating effectiveness

Robust	- The control is adequately designed to mitigate inherent risks. - The control operates effectively to mitigate inherent risks.
Moderate	- The control has moderate gaps and/or deficiencies in its design and moderately mitigates inherent risks. - The control has moderate gaps and/or deficiencies in its operating effectiveness and moderately mitigates inherent risks.
Weak	- The control has major gaps and/or deficiencies in its design and is not fit for purpose to mitigate inherent risks. - The control has major gaps and/or deficiencies in its operating effectiveness and is not fit for purpose to mitigate inherent risks.

[2] For example, this may involve ensuring that all PF risk factors typically associated to a customer are accounted for and measured and all risk scores are completely and accurately recorded and escalated. The reader should note that a risk practitioner such as an auditor or compliance monitoring staff will typically establish how to best assess, review and test controls.

16. The combined design effectiveness and operating effectiveness of a control indicates whether the control is ineffective, partially effective, or effective as per Table 3 below.

Table 3: Control effectiveness

		Operating effectiveness		
		Weak	**Moderate**	**Effective**
		Control effectiveness		
Design effectiveness	**Weak**	Ineffective	Ineffective	Ineffective
	Moderate	Ineffective	Partially effective	Partially effective
	Effective	Ineffective	Partially effective	Effective

17. It is important to highlight that institutions have to periodically review and test their controls. Any weaknesses identified should be addressed.

Residual risks

18. The residual risk is the risk remaining after considering controls' effectiveness. Once both the inherent risk and the controls effectiveness have been assessed; the residual risk is determined as per Table 4:

Table 4: Residual risks

		Inherent risk		
		Low	Medium	High
		Residual risk		
Control effectiveness	Ineffective	Low	Medium	High
	Partially effective	Low	Medium	High
	Effective	Very low	Low	Medium

19. For illustration, if a customer segment's inherent risk is identified as "Medium" and the control effectiveness has been determined to be "Partially effective", the residual risk of the customer segment will be rated as "Medium".

20. It is important to note that institutions can adapt Table 4 and the scoring methodology to fit their internal processes.

Review Cycle

21. An institutional PF risk assessment is an evolving process and should be regularly updated, taking into consideration newly emerging threats and vulnerabilities that may arise following a trigger event.

22. In the institutional context, trigger events may include changes in the company's businesses strategy, targeted customer base, newly offered products, services, and delivery channels, and establishing business activities in a high-risk jurisdiction.

Section 3: Proliferation Finance Risk and Controls

23. Table 5 sets out the **six PF risk categories** whose inherent PF risks should be considered: 1) customers; 2) business activity, occupation and/or industry of customer, 3) geographic location, 4) products, services and transactions; 5) delivery channels and 6) cyber threats to systems and software.

24. Institutions will then need to consider each risk category against the ‘risk factors’ (shown in the second column of Table 5) relevant to their business activities. The prominence of specific risk factors will vary across institutions. A maritime insurance company will not have the same business exposure as an international bank, a virtual asset service provider or a dealer in precious metals and stones. Furthermore, risk factors vary depending on the type of markets the institution services, its customers, the products it offers, delivery channels and platforms used. The third column in Table 5 maps relevant PF activities against the risk categories. Note that Table 5 does not offer an exhaustive list of risk factors rather contains examples that assist Fis, DNFBPs, and VASPs in identifying the most relevant risk factors.

PF Risk categories and factors

25. The RA should follow a risk-based approach (RBA) which will provide institutions with flexibility in relation to the steps they take to combat PF. An RBA does not prevent institutions from engaging with customers or establishing business relationships that may have a higher exposure to PF risk. Rather, it guides institutions to manage and target their anti-financial crime efforts to areas that represent higher financial crime risk.

Table 5: Risk categories and risk factors[3]

Risk Categories	Risk Factors	Potential Acts of Proliferation Finance
Customer risk (including legal entity type)	Residency and nationality	• Use of a country's vulnerability to PF (this may be the result of historical legacy, poor regulatory and legal framework, social and political factors, or economic and technological factors). • Use of jurisdictions that provide accounts to, or otherwise facilitate, financial activities of proliferation states. • Use of local branches of banks and financial institutions based in countries of proliferation concern. • Use of complex structures (such as multi-layered trusts, foundations), nominee directors and/or shareholders to hide an Ultimate Beneficial Owner (UBO) or significant controller and their association with sanctioned entities or jurisdictions, especially those incorporated in offshore tax havens. • Use of cryptocurrencies to avoid the formal financial system. • Establishment of corporate networks that facilitate but may not be solely involved in PF activities. • Ultimate beneficial ownership, connections and control structures are opaque. • Use of front companies, shell companies or brokers to obtain trade finance products and services, or as parties to clean payments.
	Complex ownership structure involving several jurisdiction and entity types	
	Use of international corporate vehicles	
	Virtual currency providers or customers investing via such providers	
	Companies with nominee shareholders	
Business activity/occupation/industry of customer	Money services businesses	• Money-exchange businesses used for cash transfers in support of proliferation networks, where transfers involve individuals or entities owned or controlled
	Manufacturing	

[3] També, N. (2023) 'Institutional Proliferation Finance Risk Assessment Guide', p.24. Available online: https://www.rusi.org/explore-our-research/publications/special-resources/institutional-proliferation- finance-risk-assessment-guide.

	Agriculture	by proliferation actors. Can also involve structured payments to organized crime networks involved in revenue-raising activities. • Use of universities or research centers to procure DUGs and/or for payment of funds. This may be done under the guise of MOUs signed with other universities/research centers. • Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. Often combined with use of front companies with opaque ownership structures. • Use of diplomats, consular officers or diplomatic or consular missions of North Korea to build networks, including corporate networks, within a country. These networks then facilitate a range of revenue-raising activities[4] as well as facilitating financial products or services related to trade in goods. • Use of PEPs or their associates who may leverage their position of power to access land rights, mining rights or exploit businesses (such as fisheries) to raise revenue for sanctioned countries and actors. • Use of professional intermediaries and corporate service providers to mask parties to transactions and end users associated with PF.
	Research	
	Suppliers, buyers and trading partners in Weapons of Mass Destruction (WMD) technology/dual-use goods (DUGs) /nuclear/defense industries	
	Maritime/shipping industry	
	Providers of shadow banking	
	Money-exchange businesses	
	Embassies and consulates	
	Politically Exposed Persons (PEPs)	
	Corporate service providers and intermediaries	
Geographic risk	Jurisdictions known for diversion	• Use of local branches of banks and financial institutions based in countries of proliferation concern.
	Jurisdictions with weak export control laws	

[4] This guide does not offer a comprehensive list of activities that North Korean and Iranian nationals and entities have been reported to – or could theoretically – engage in to raise funds. There are several well-established or emerging patterns of fundraising activities, such as cybercrime and abuse of cryptocurrencies, provision of military assistance, construction of statues and monuments, illegal wildlife trade, and overseas labor across different types of industries. Revenue-raising activities will differ across jurisdictions, as they depend on jurisdictions' specific vulnerabilities. For more, see Darya Dolzikova and Anagha Hoshi, 'The Southern Stratagem: North Korean Proliferation Financing in Southern and Eastern Africa', *RUSI Occasional Papers* (April 2020), Available online: https://www.rusi.org/explore-our-research/publications/occasional-papers/southern-stratagem-north-korean-proliferation-financing-southern-and-eastern-africa.

	High-risk jurisdictions	• Use of third countries with weak CPF frameworks, export control laws, or elevated risks of corruption and bribery to channel financial transactions related to DUGs. • Use of offshore jurisdictions that offer the possibility of easily creating front and/or shell companies to disguise UBOs and/or end users associated with WMD programmes. • Use of trade or other economic relations with countries with links or significant exposure to a proliferating country. Often facilitated by a complex corporate network. • Use of jurisdictions with inadequate AML/CTF/CPF regulatory compliance measures which may provide opportunities for exploiting regulatory arbitrage. See Table 6 for more on the criteria that should be considered when assessing a jurisdiction's vulnerability.
	Countries subject to sanctions or embargos; countries identified as lacking appropriate AML/CFT/CPF laws and regulations	
	Offshore financial centers and non-cooperative tax jurisdictions	
	Jurisdictions identified as having significant levels of corruption or organized crime, or other criminal activity	
	Jurisdictions identified as providing funding or support to terrorist activities	
Products, services and transactions risk	Open account payments	• Use of trade finance products and services and payment services in procurement of proliferation-sensitive goods. • Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance. • Use of international wire payments with limited oversight of CDD performed on payers and payees. • Use of shadow banking characterized by limited disclosure of the value and nature of assets. • Use of correspondent banking to transfer value across the international financial system to and from proliferators to pay for DUGs, or to transfer proceeds of revenue-raising activities. • Use of foreign-denominated accounts to make international payments to procure
	Letters of credit	
	International payments	
	Shadow banking	
	Correspondent banking relationships	
	Foreign accounts	
	Trading in precious metals and stones	
	Provision of maritime insurance products	

	Provision of virtual assets trading services	DUGs, or to transfer proceeds of revenue-raising activities. ● Purchase or sale of precious metals and/or stones to transfer value across jurisdictions or raise revenue to support WMD programmes. ● Provision of maritime insurance to shipping companies involved in sanctions violations. ● Use of anonymity-enhanced virtual assets [privacy coins]. ● Use of unregulated virtual asset service providers to avoid the formal financial system and associated controls. ● Directly transferring or facilitating virtual assets for the benefit of sanctioned individuals or entities for the purposes of circumventing sanctions.
Delivery channel risk	Face-to-face origination	● Use of non-face-to-face account opening facilities to mask the identity of the UBO. ● Services that are capable of concealing beneficial ownership from competent authorities (for example, nominee director risk).
	Non-face-to-face origination	
Cyber threats to systems and software	Hacking	● Hacking accounts to obtain fund by proliferating states.
	Ransomware	● Use of systems with malicious software that freezes or encrypts devices that are unblocked after ransom is paid to proliferation actors.
	IT contractors with access to sensitive material	● Use of IT employees embedded in organizations involved in subject matter potentially related to WMDs or DUGs training or development.

26. Table 6 provides a guide to the criteria to consider when evaluating PF risks that jurisdictions may be exposed to. Note that this table is for guidance and provides examples of factors and/or elements to consider when developing your institution's country risk assessment. The reader should note that there are many lists that they may wish to consult to determine a country's risk assessment scores. Those are, for example:

- The FATF's list of jurisdictions under increased monitoring;[5]
- The EU high risk countries list;[6]
- The US Office of Foreign Assets Control (OFAC) sanctions programs and country information list;[7]
- The Basel AML index;[8] or
- The Transparency International's Corruption Perceptions Index.[9]
- Countries subject to United Nations (UN) Sanctions[10]

Table 6: Example of country risk scoring[11]

Restricted/Very High	• Country is subject to UN sanctions related to proliferation activities (North Korea and Iran)
High	• Country is subject to other unilateral sanctions. • Country has significant corporate/trade network with proliferating state or ties with sanctioned countries. • Country offers shipping flags of convenience or passports of convenience. • Country is on the FATF's list of jurisdictions under increased monitoring. • Intelligence suggests that country may consider developing nuclear capability through illicit procurement.
Medium–High	• Known country of diversion, country scored with a low level of effectiveness in FATF mutual evaluation reports, including on Immediate Outcome 11.[12] • Geographical proximity to a proliferating country.

[5] Available online: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2023.html.
[6] Available online: https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en.
[7] Available online: https://ofac.treasury.gov/sanctions-programs-and-country-information.
[8] Available online: https://index.baselgovernance.org/methodology#:~:text=The%20Basel%20AML%20Index%20measures,high%20risk%20of%20ML/TF.
[9] Available online: https://www.transparency.org/en/cpi/2022.
[10] Please see https://www.un.org/securitycouncil/sanctions/information
[11] També, N. (2023) 'Institutional Proliferation Finance Risk Assessment Guide', p. 26. Available online: https://www.rusi.org/explore-our-research/publications/special-resources/institutional-proliferation-finance-risk-assessment-guide
[12] 'Immediate outcomes' assess to what extent a country meets the objectives of FATF standards. Immediate Outcome 11 requires preventing persons and entities involved in WMD proliferation from raising, moving and using funds. More information can be sourced in the FATF's methodology for assessing compliance with the FATF recommendations and the effectiveness of AML/CFT systems, https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html. In addition, refer to the following link for the consolidated assessment rating: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html.

	• Country named by the UN Panel of Experts (UNPoE) / OFAC / mainstream media as either trading with sanctioned states or lacking sufficient visibility/transparency on trade patterns. • Country does not respond to UNPoE enquiries. • Country outside the Nuclear Non-Proliferation Treaty and/or countries that are maintaining or improving their nuclear capabilities. • Proliferating state has diplomatic presence in the country.
Medium	• Country neighbors a proliferating state. • Country has a large diaspora from a state of proliferation concern. • Country hosts a financial, trade center, or transshipment hub that is attractive to proliferation financiers. • The jurisdiction is home to a manufacturing sector that produces goods controlled by international export control regimes related to WMD and/or their delivery vehicles. • The jurisdiction has weak controls and/or enforcements in relation to ML, TF and PF.
Low	• Country has strong regulation and enforcement mechanisms that are recognized by the FATF, and/or country is not on FATF lists. • Country has robust company registry system. • Country has performed national risk assessment (NRA) for ML/TF/PF and has identified and implemented mitigating controls to tackle high-risk issues raised in NRAs.

Risk mitigating measures

27. Building on a fuller understanding of a RA methodology and PF risk categories and factors, there are multiple controls that are traditionally in place to combat ML and TF which will help the private sector in mitigating PF risks. These controls are mentioned below.

Client onboarding, Know your Customer (KYC) and Customer Due Diligence (CDD)

28. The information collated as part of KYC and CDD helps the private sector in understanding, assessing and documenting PF risks it is exposed to. Indeed, deep knowledge and understanding of the customer are established during the onboarding process where the necessary information to monitor, screen and assess the customer's potential PF risks is collated.

29. The objectives of the KYC and CDD process are:

- Identification and verification of the customer identity;
- To get a detailed description of the customer's background;
- To understand the customer's source of wealth and source of funds (the source of the assets that will be transferred to the institution);
- To understand the purpose, nature of the relationship, as well as the expected behavior of the account;
- To understand the ownership and control structure if the customer is a legal entity;
- To obtain identification and verification of UBOs, PEPs status and associations with PEPs;
- To understand who the customer does business with and where;
- To perform sanctions, watchlist, and adverse media screening.

30. In addition, understanding whether the customer deals in dual-use or other controlled goods (i.e., nuclear or military) is essential to CPF. As part of the KYC/CDD process, the private sector needs to assess:
    - Whether the customer is licensed to trade in such goods;
    - Whether there is a link to a sanctioned jurisdiction or to an area that borders a sanctioned jurisdiction;
    - Whether trades involve the transshipment of goods.
31. CDD and KYC performed on legal entities should also extend to associated natural persons, including the entity's beneficial owners, authorized signatories, individuals with power of attorney and/or senior managing officials (SMOs).
32. In addition, regulated entities are required to collate and store the information relating to their customers. This information should be reviewed periodically to ensure that customers' information remains accurate, complete, and valid and that the customers' circumstances have not changed. This is an essential control to mitigate PF risks as it will enable the institution to verify whether the customer's activities are aligned to their risk profile and the purpose of the business relationship.

Enhanced Due Diligence (EDD)

33. EDD refers to the additional steps an institution is required to undertake at onboarding as well as during the business relationship with a customer, to limit or manage higher inherent financial crime risks, including PF risk, posed by the customer. The following will determine whether a customer should be subject to EDD:

    - A politically exposed person (foreign or domestic);
    - A person or legal entity residing or incorporated in a high-risk jurisdiction as per UAE regulation[13] and the institution's high risk country list;
    - A customer who purchases products, services, privacy-enhancing tokens that are more vulnerable to PF;
    - A customer whose corporate ownership structure is highly complex and hence opaque;
    - A customer who uses international corporate vehicles in various offshore jurisdictions to structure assets and support their investment needs;
    - A customer who operates and/or is involved in a high-risk industry.

34. In cases where the CDD/KYC indicates the institution is dealing with a higher risk customer, EDD should be performed, with particular focus on the corroboration of customer information using independent and reliable sources of information. EDD requires:

    - Obtaining and corroborating additional KYC and CDD relating to the customer and the beneficial owner and, where necessary, updating it every 12 months. Examples of additional KYC and CDD may include requesting the passport copy in cases in which the client has only provided a national ID document (for individuals), or requesting the memorandum of association (MOA) in cases in which the client has only provided the trade license (for entities);
    - Understanding further the customer's business and documenting the research;

[13] Please see National Committee for Anti Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations (NAMLCFTC) – High Risk Countries https://www.namlcftc.gov.ae/en/more/jurisdictions/high-risk-countries/

- Lowering controlling ownership interest from 25% to 10%[14];
- Enhancing the monitoring of the business relationship and the transaction monitoring controls performed on the customer to identify any unusual or unexpected transactions behaviors that may result into suspicion of proliferation finance;
- Documenting the role of the PEP within the company in case of the involvement of a PEP within a corporate structure.
- Performing further searches such as criminal records, litigation history, financial history, adverse media to enhance the understanding of the customer's risk profile;
- Obtaining additional information on the customer's intended nature of business relationship, the reasons for and economic background of the transactions, on the plausibility of these transactions, on the customer's source of funds and/or source of wealth and/or crypto to confirm that they are not associated to PF;
- Obtaining sign off by the relevant customer acceptance committee and/or senior management, to start, continue or exit the business relationship.

Screening Customers for Sanctions and Adverse Media Risks

35. Existing client screening processes performed as part of the CDD/KYC process support in determining whether a client represents an elevated PF risk. It is expected that all customers, beneficial owners, authorized signatories, attorney holders, company directors and/or all other relevant individuals on an organization chart will be screened.

36. Screening the client will determine whether there are any matches with individuals and/or entities that:

- Have adverse press and/or reputation;
- Have been criminally prosecuted;
- Are PEPs or are relatives or close associates of PEPs;

[14] Note that this is best practice observed in some jurisdictions but is not a regulatory requirement under Cabinet Decision No. 58 of 2020 on Regulating the Beneficial Owner Procedures. For more information refer to Cabinet Decision No. 58 of 2020.

- Are sanctioned and/or are associated to sanctioned legal entities and/or natural persons;

- Are associated to PF, proliferation activities and/or proliferators.

37. Sanctions screening should be performed at a minimum in circumstances mentioned under Section 4 of the Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs and cross-border payments and securities transactions have to be screened in real-time against international and internal sanctions lists. Alerts with a higher probability for true matches need to be escalated to management as per the institution's internal processes.

38. The screening outcome may affect the risk level applied to a customer and may trigger either applying an enhanced due diligence process, the offboarding of the client and/or a STR/SAR logged with the FIU.

Ongoing monitoring and transaction monitoring

39. Once a customer is onboarded and a business relationship is established, institutions are required to re-perform CDD/KYC on all business relationships on a periodic basis or when a trigger event occurs. The frequency of the review is determined by the customer's risk profile as per the risk-based approach and in line with the institution's internal processes. As part of these periodic reviews, the institution will update all CDD/KYC information. For instance, a client re-classified from medium to high risk as a consequence of the periodic review will be subject to EDD.

40. In addition to CDD/KYC, the institution should review and analyze transactions throughout the course of a business relationship, including performing blockchain monitoring in the case of VASPs, to ensure that the transactions being conducted are consistent with customer profiles. Transaction monitoring tools used should include typologies indicative of PF activities. The institution will thus determine whether customers' behaviors, product use, deposits and transaction volumes are aligned with the expected transactions, nature and purpose of the business relationship and, if not, whether such activities have a robust business rationale or should be treated as suspicious.

Suspicious Activity Reports

41. Staff members should immediately report any alert of money laundering, terrorist financing or proliferation finance to compliance. If after investigation the alert cannot be discarded, a

SAR or STR should be reported to the FIU via the goAML platform. For more details on STR/SAR reporting, please refer to the UAE FIUs website.

Employee screening

42. Institutions should implement robust hiring processes in line with relevant regulations. Employees should be screened to safeguard against proliferation finance. Employees competence, good standing, and integrity to be assessed.

Employee Training

43. The institution should ensure that all relevant employees, contractors, senior management and any other relevant individuals are trained with regards to preventing the institution from being used for proliferation finance. Targeted training should be delivered to CPF staff or to staff that work directly with customers or whose responsibilities expose them to PF. More particularly staff who perform customer onboarding, risk assessments, ongoing monitoring, name and transaction screening should be given targeted training on PF risks, sanctions evasion typologies and risk indicators.

44. The EOCN recommends reviewing the above controls along with the following elements to ensure that CPF is an integral part of the institution's framework:

- **Governance framework.** This includes ensuring that CPF is part of the overall governance framework, including procedures on how CPF measures in the compliance function may affect/interact with other business-related functions.
- **Management information pack** distributed to SMOs. The MI pack may include, among other topics, information on CPF risks, policies and procedures, mitigating controls, and effectiveness of such controls.
- **CPF policies.** This may include policies on implementing targeted financial sanctions related to proliferation financing, process on dealing with DUGs, and reporting suspicious PF activities.
- **Adequate screening systems.** This includes ensuring that screening systems are adequate and fit for the purpose of detecting confirmed and partial name matches on sanctions lists, as well as for detecting possible DUGs in trade and other documents.

- **Process in place to freeze assets** of designated entities and/or nationals without delay. This includes both freezing of assets and prohibition to provide funds and other assets or services to the designated person and reporting to the EOCN where such measures have been taken.

- **Controls testing.** This includes tests of the CPF controls in place to measure whether those controls are effective. An example is a test to ensure that adequate information is being obtained during the CDD process to be able to accurately rate the PF risks of customers.

- **New product approval process.** CPF risks need to be taken into consideration before approving new products, especially those related to facilitating trade.

- **Customer acceptance process.** Onboarding or continuing a business relation with a high PF risk customer should be approved at senior management level.

- **Business-Wide Risk Assessments.** PF risks should factor into the overall Business-Wide Risk Assessment and is an integral part of the overall financial crime risks that an entity faces.

45. A final point is that it is fundamental to maintain a financial crime prevention framework that is proportionate to the institution's customer size, volumes of transactions, size of deposits or geographical footprint. Institutions should aim for proactive compliance and be focused on a RBA to effectively identify, evaluate and mitigate PF threats.

Section 4: Onboarding questionnaire, elevated PF risk factors and customer risk scoring

46. This section provides a template for FIs, DNFBPs, and VASPs to collect information related to customers' PF risk factors and helping them in assessing their customers' PF risk profile and risk score.

47. All institutions, including DNFBPs and VASPs[15], should go through sections A to D. Additional Section E is designed for DNFBPs while additional Section F is designed for VASPs.

[15] Note that some questions may not be applicable to DNFBPs and/or VASPs in Sections B and C. Under such circumstances, the N/A box should be selected.

Customer PF Risk Scoring Questionnaire

Customer Due Diligence (CDD) and Know Your Customer (KYC) questionnaire to determine customer PF risk score

Nationality:	Country of residency:	
Profession (including description):	Industry type:	Current/last employer (if relevant):
Estimated net wealth:		
PEP:		

Additional relevant information relating to customer, their occupation and description of relationship with customer:

A. Country risk	NO	YES	Comments
High risk or medium risk country as per your organization's internal policy for the following:			
1. Nationality			
2. Country of residence			
3. Country of business activity			

B. Customer risk	NO	YES	N/A	Comments
1. Origin of wealth and/or source of funds is easily identified or well described.				
2. Customer's profile (age, occupation, employment status, salary, level of education) is consistent with wealth, transactions and account turnover.				
3. Customers with valid reasons to open the account/establish the relationship in the requested jurisdiction.				
4. Walk-in customers have not been actively prospected by the institution or lacking an obvious connection with the institution.[16]				
5. Customers who have not been physically met.[17]				
6. Customer introduced by a trust and company service provider (TCSP) and/or uses an intermediary in all interactions including business relationships with no robust rationale.				
7. Politically Exposed Person (PEP) or related to a PEP.				

[16] Note that VASPs do not actively prospect customers and may wish to select the N/A option as this will not necessarily be a high-risk indicator.
[17] Note that VASPs that onboard customers remotely will not meet customers face to face. They may therefore wish to select the N/A option as this will not necessarily be a high-risk indicator.

8. Customer working in high-risk industry. This includes arms dealing, manufacturing, nuclear industry including research, construction, art and antiques dealer, auctioning house, shadow banking, currency exchange bureaus, money transmitters, oil, precious metals and stones and high-value goods dealers, wildlife trade, maritime and international shipping, import/export related business, freight transportation or industries linked to goods subject to export control and DUGs, diplomacy, VASPs. *Refer to Table 5 for details of industries with elevated PF risk factors.*				
9. Customer operating in gambling activities.				
10. Customer involved in crypto-mining or trading with crypto currencies.				
11. Customer operating from a complex, multi-layered business structure.				
12. Complex legal structure with no reasonable economic or wealth management purpose.				
13. Client is using companies where multiple, unexpected statutory changes have occurred. This may have been over a short period of time and may include, for example, the designation of new directors, a change in the country of registration to a high or medium risk country or the modification of the company's objective without an economic justification.				
14. Dormant customer with a sudden unexplained surge in activities.				
15. Customer operates within a company with nominee directors and/or shareholders and/or bearer shares.				
16. Missing ID documentation, invalid forms of ID, false and/or incomplete residential address, overall reluctance to provide CDD, KYC and ID documentation.				
17. The customer may be raising funds on behalf of designated individual/ entity. This includes holding a legal title to any asset, conducting transactions for the benefit of, or on behalf of, or at the direction of a designated individual or entity.				
18. The customer displays signs of acting on somebody else's instruction and/or has a disproportionate level of authority provided by the end client.				
C. Products, Services and Transaction risk	**NO**	**YES**	**N/A**	**Comments**
1. First transfer on the account made by cash deposit. For DNFBPs, this includes purchases done through multiple cash transactions or where seller insists on cash only payments.				
2. Commercial transaction at a price that is undervalued, overvalued or unjustified.				

3. Business relationship has no legitimate economic or legal grounds.			
4. Customer involved in trade finance or correspondent relationships.			
5. Transaction involves the sale or purchase of dual-use, proliferation sensitive or military goods, particularly with higher risk jurisdictions			
6. Transaction involves the shipment of goods incompatible with the technical level of the country to which it is being shipped.			
7. Transactions involve possible shell companies. Indicators of shell companies may be use of nominee directors, mass registration address, address of a TCSP, limited capitalization and/or assets.			
8. Transaction involves a person or entity in a foreign country of proliferation concern or a country with weak export control laws.			
9. Transaction involves jurisdictions known to have inadequate AML/ CTF/ CPF measures.			
10. The customer makes out of character payments (including in cash) and/or transactions (payment in precious metals and stones and/or VAs) to other companies, subsidiaries or entities that belong to the same group. Consideration should be given to payments made to other companies that have the same directors, shareholders and/ or beneficial owners.			
11. Use of bulk cash or precious metals (e.g. gold) in transactions aimed for purchase of unrelated items (e.g., industrial items, real estate, etc.).			
12. Payment from purchaser is financed through an unusual source (e.g., offshore bank located in a high-risk jurisdiction).			
13. Purchaser pays the initial deposit with a third-party cheque.			
14. The speed of the transaction (e.g., sale or purchase of a good) is particularly fast.			
15. The customer is using complex loans or opaque means of financing which do not appear to involve regulated financial institutions.			
16. Client owns assets located in other jurisdiction and do not appear to be declared in tax returns.			
17. Client is invoiced by organizations that are in jurisdictions known for strict bank secrecy laws, offshore and/or high-risk jurisdictions.			
18. Transactions involve transshipment of dual-use / controlled items to high-risk jurisdictions.			
D. Sanctions and adverse media screening	NO	YES	Comments
1. Customer, or purchaser, or seller, or UBO is a confirmed name match while screening through sanctions lists (UN, UAE Local Terrorist List, and other lists).			
2. Customer, or purchaser, or seller, or UBO is linked to negative news, crime and/or ML/TF/PF reports from watchlist screening tool.			

Additional questions specific to DNFBPs

E. DNFBPs	NO	YES	Comments
1. Customer's economic profile/business activity and purpose aligns with the cost of the good.			
2. Customer's source of funds can be identified and documented			
3. Customer is using an intermediary for interactions and conducting transactions with no logical reason. Consideration must also be given to a customer who appears to be acting on behalf of a third party whose identity is concealed. In addition, consideration must be given to the good standing of the intermediary and whether they are adequately supervised and trained. Finally, consideration must also be given to potential different geolocations between the customer and the intermediary and whether there is a rationale.			
4. Customer is purchasing the good in the name of a nominee, a relative, or on behalf of minors. Consideration must be given as to whether the customer hesitates or declines to put his name on documentation connecting them to the goods.			
5. The customer structures payments to ensure that transactions do not exceed DNFBPs' CDD thresholds as per FATF Recommendation 22.[18] More specifically, DNFBPs' thresholds are: • USD 15,000 in cash for dealers in precious metals & stones • USD 3,000 for casinos			
6. Purchaser/ seller is unconcerned about the economic or investment value of the good being purchased/sold.			
7. Purchaser/ seller buys/ sells multiple goods in a short period of time and has limited concerns or interests relating to the location and/ or price of the good.			
8. Lack of clarity of who the end user is and/or involvement of a third party (e.g., payment from third party or delivery of good to a third party who did not purchase the goods).			
9. The customer is not concerned with making losses where loss is avoidable.			
10. The customer offers to pay unusually high fees for a product or a service with no rationale.			

[18] Per Article 6 of the UAE's Cabinet Decision No.10 of 2019 (amended by Cabinet Decision No. 24 of 2022), DNFBPs should undertake CDD measures when "carrying out occasional transactions in favour of a customer for amounts **equal to or exceeding AED 55,000**, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked."

Additional questions specific to VASPs

F. VASPs	NO	YES	Comments
1. The source of crypto is easily identified.			
2. The customer is not sharing IP addresses and/or using VPN services from established providers.			
3. The customer wants to top up their wallet with high-risk payment methods.			
4. The customer performs transactions that enable fiat on-ramp and off-ramp.			
5. The customer engages in high-risk transactions such as arbitrage, gambling, mining.			
6. The customer uses self-hosted and/or non-custodial wallets to store crypto.			
7. The customer has a high wallet risk score as identified by Blockchain Analytics tools.			
8. The customer is a legal entity that is a high-risk VASP. Consideration should be given to whether the customer is a cryptocurrency ATM, Cryptocurrency Mining, Decentralized Cryptocurrency Exchange, Mixers, OTC Broker, Custodial Service, Decentralized Autonomous Organizations. In addition, consideration should be given to the types of tokens that the VASP accepts on its platform. Finally, consideration should be given as to the VASP's AML/CTF/CPF policies and practices. This can be assessed via a correspondent relationship type questionnaire.[19]			

48. Note that accurate completion of the CRS questionnaire enables the private sector to identify at onboarding as well as during the ongoing due diligence process, clients and/or entities that are high risk or need to be reclassified as high risk because of a change in circumstances (e.g., change of industry, PEP status, out of character transactions).

[19] The Global Digital Finance AML/KYC working group has developed an Anti-Money Laundering Due Diligence Questionnaire for Virtual Asset Service Providers (VASPs). It is available online: https://www.gdf.io/gdf-virtual-asset-due-diligence-questionnaire/.

Section 5: Case Studies and the Customer Risk Score (CRS) Questionnaire

Tsai Case Study

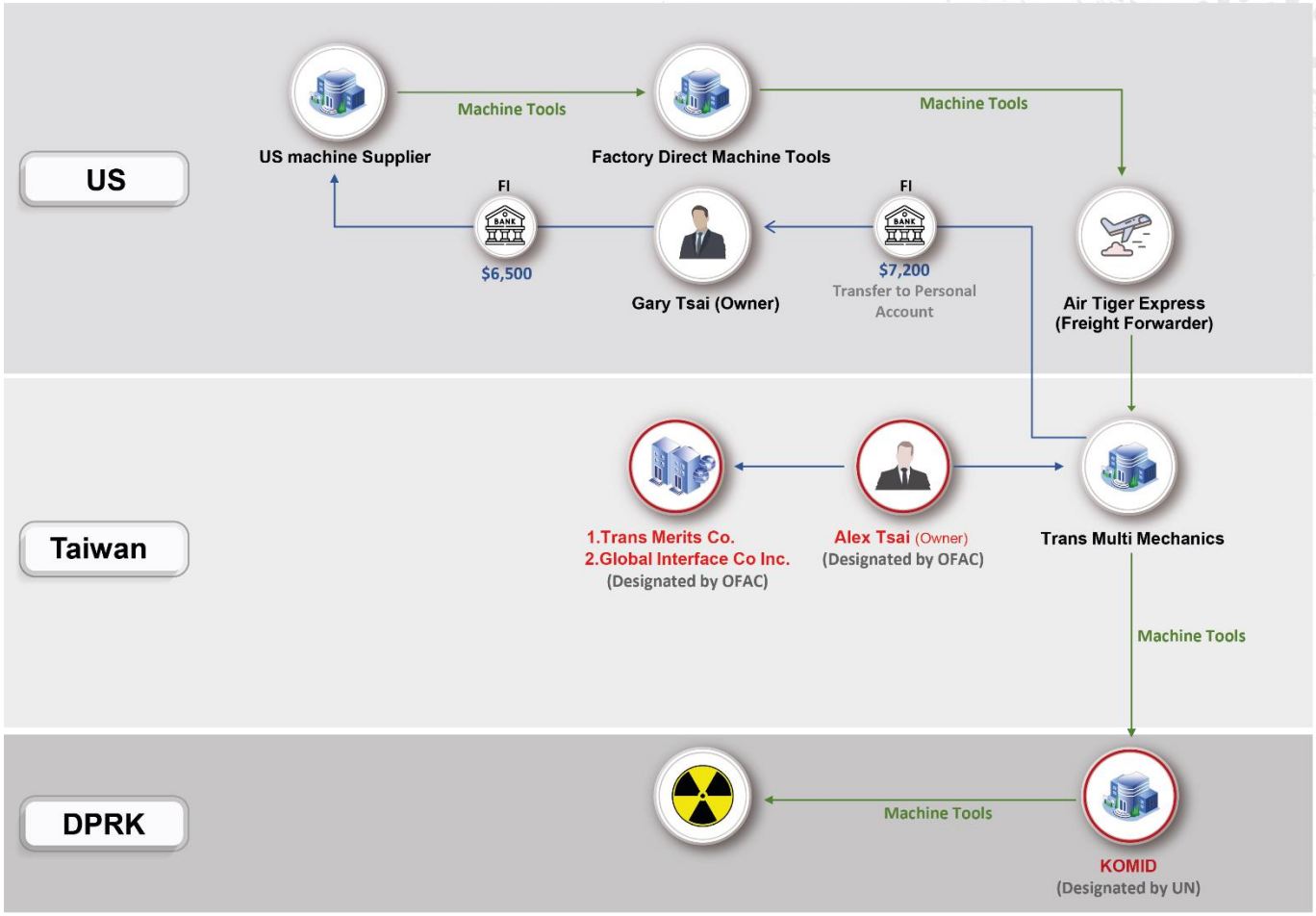
In 2009 the U.S. Justice Department announced the arrest of two Taiwanese nationals, Alex and Gary Tsai (father and son respectively) accused of conspiring to export from the U.S., machine tools that can manufacture weapons of mass destruction[20] (WMDs) to Taiwan. Due to Alex Tsai's activities prior to 2009, there are suspicions that the tools were subsequently shipped to North Korea.

Indeed, in June 2008, Alex Tsai (residing in Taiwan) and his company Trans Merits Co Ltd were indicted in Taiwan for "forging shipping invoices and shipping restricted materials to North Korea"[21]. In addition, in January 2009, the US Treasury (OFAC) sanctioned Alex Tsai and his companies Global Interface Company Inc and Trans Merits Co Ltd for supporting a UN sanctioned conglomerate, the Korea Mining Development Trading Corporation (KOMID). KOMID (which has now been rebranded as Greenpine corporation) is known as "Pyongyang's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons".[22] KOMID (KPe.001) is listed under UNSCR 1718 Sanctions Committee.[23]

To evade sanctions, Taiwan based Alex Tsai started operating through Trans Multi Mechanics, a non-designated company. Alex purchased U.S. manufactured machine tools via Factory Direct Machine Tools, his son's U.S. based company. Gary, his son, facilitated Alex's imports of machine tools from the U.S into Taiwan. For instance, in September 2009, Gary arranged the shipment of a machine for $6,500 from a US supplier to Trans Multi Mechanics via a freight forwarder (Air Tiger Express). Trans Multi Mechanics subsequently wired $7,200 to Gary's personal account who then wired $6,500 to the US tool supplier.

According to the US Department of Justice documentation,[24] the same pattern occurred many times whereby funds were sent from Trans Merits or Trans Multi Mechanic's accounts in Taiwan to Gary's U.S. personal bank accounts.

[20] Department of Justice Press Release U.S. Department of State, "Fact Sheet: United States Sanctions Individuals Linked to North Korean Weapons of Mass Destruction Programs," March 8, 2013.
[21] United States District Court in the Northern District of Illinois, Eastern Division, Indictment: United States of America v. Hsien-Tai Tsai aka Alex Tsai, October 23, 2012, p. 3.
[22] U.S. Department of State, "Fact Sheet: United States Sanctions Individuals Linked to North Korean Weapons of Mass Destruction Programs," March 8, 2013.
[23] For more detail reefer to: https://www.un.org/securitycouncil/sanctions/1718/materials/summaries/entity/korea-mining-development-trading-corporation.
[24] United States District Court in the Northern District of Illinois, Eastern Division, Indictment: United States of America v. Yueh-Hsun Tsai aka Gary Tsai, April 19, 2013.



Case Analysis

49. There is no indication as to whether the FIs transaction monitoring tools flagged the fund transfers from Trans Merits or Trans Multi Mechanic's (Alex Tsai's companies) accounts in Taiwan to Gary's U.S. accounts as suspicious. However, since the Department of Justice documentation indicates that the transactions associated to the purchase of the machinery were not particularly high in value nor out of character for Gary's machine tools import/export business, this is not indicative of a failing from the FIs.

50. While there is no public information relating to the controls that FIs had in place while providing banking services to Alex and Gary Tsai, the controls below would assist in identifying and reporting suspicious activities:

    - Following Alex's indictment and conviction for United Nations Security Council Resolutions 1718 (2006) violations, sanctions and adverse media screening would flag Alex and provide the institution with the opportunity to exit the business relation with Alex;

- For the purpose of this exercise, we assume the bank does not identify that Alex is sanctioned and he only appears on the adverse media list. Under such circumstances, the bank subjects Alex's account to EDD should it wish to maintain a business relationship with the customer;

- The bank flags transfers from Alex's account to the U.S. (especially those associated to the purchase of sensitive goods) as suspicious and has them, and other associated transactions investigated by trained anti financial crime staff members;

- The bank flags the transaction to its correspondent bank as high risk, leveraging the experience and systems and controls in place across large international FIs;

- As part of the sanctions screening, Gary's bank identifies Gary's surname as a match for an OFAC sanctioned individual;

- The investigation of the match establishes that Gary is the son of an OFAC designated person (Alex Tsai);

- Further due diligence on Gary indicates that:

    - His activity is import/export of machine tools;

    - He introduces himself as an employee of a known designated entities (it is documented that Gary distributed designated entity business cards to his US suppliers);

    - He uses designated companies' email accounts;

    - He sends sensitive goods to Taiwan where his father was indicted for his involvement with North Korea.

Assessing customer risk using the CRS questionnaire

51. Using the information documented in the Tsai case study, this section illustrates the way a financial institution is expected to complete the CRS questionnaire. Each 'YES' and 'NO' box selected will influence the customer's overall PF risk score.

52. Note that institutions wishing to adopt the questionnaire need to adapt and develop the scoring methodology to fit their internal processes and risk scoring process.

53. The following is a walkthrough of the CRS questionnaire for Gary Tsai at onboarding. Since no information relating to transactions are documented, questions relating to transactions will be responded to as 'NO'.

A. Country risk	NO	YES	Comments
High risk or medium risk country as per your organization's internal guidance for the following:	x		Taiwan is not on high-risk country list.
1. Nationality	x		Taiwan national
2. Country of residence	x		U.S.A
3. Country of business activity	x		U.S.A and Taiwan

B. Customer risk	NO	YES	N/A	Comments
1. Origin of wealth and/or source of funds is easily identified or well described.		x		Director of an import/export business. Website and company accounts support source of wealth.
2. Customer's profile (age, occupation, employment status, salary, level of education) is consistent with wealth, transactions, and account turnover.		x		
3. Customers with valid reasons to open the account/establish the relationship in the requested jurisdiction.		x		The customer needs correspondent banking to receive payments from Taiwan.
4. Walk-in customers have not been actively prospected by the institution or lacking an obvious connection with the institution.	x			
5. Customers who have not been physically met.	x			
6. Customer introduced by a TCSP and/or uses an intermediary in all interactions including business relationships with no robust rationale.	x			
7. Politically Exposed Person (PEP) or related to a PEP.	x			
8. Customer working in high-risk industry. This includes arms dealing, manufacturing, nuclear industry including research, construction, art and antiques dealer, auctioning house, shadow banking, currency exchange bureaus, money transmitters, oil, precious metals and stones and high-value goods dealers, wildlife trade, maritime and international shipping, import/export related business, freight transportation or industries linked to goods subject to export control and DUGs, diplomacy, VASPs. *Refer to Table 5 for details of industries with elevated PF risk factors.*		x		**High Risk indicator:** Director of Factory Direct Machine Tools, an Import/export business of machine tools that can manufacture weapons of mass destruction.

9. Customer operating in gambling activities.	x			
10. Customer involved in crypto-mining or trading with crypto currencies.	x			
11. Customer operating from a complex, multi-layered business structure.	x			
12. Complex legal structure with no reasonable economic or wealth management purpose.	x			
13. Client is using companies where multiple, unexpected statutory changes have occurred. This may have been over a short period of time and may include, for example, the designation of new directors, a change in the country of registration to a high or medium risk country or the modification of the company's objective without an economic justification.	x			
14. Dormant customer with a sudden unexplained surge in activities.	x			
15. Customer operates within a company with nominee directors and/or shareholders and/or bearer shares.	x			
16. Missing ID documentation, invalid forms of ID, false and/or incomplete residential address, overall reluctance to provide CDD, KYC and ID documentation.	x			
17. The customer may be raising funds on behalf of designated individual/ entity. This includes holding a legal title to any asset, conducting transactions for the benefit of, or on behalf of, or at the direction of a designated individual or entity.		x		**High Risk indicator:** Review of adverse media indicates that the customer's father has been indicted by authorities in Taiwan for potential involvement with North Korea.
18. The customer displays signs of acting on somebody else's instruction and/or has a disproportionate level of authority provided by the end client.	x			
F. Products, Services and Transaction risk	NO	YES	N/A	Comments
1. First transfer on the account made by cash deposit. For DNFBPs, this includes purchases done through multiple cash transactions or where seller insists on cash only payments.	x			
2. Commercial transaction at a price that is undervalued, overvalued or unjustified.	x			
3. Business relationship has no legitimate economic or legal grounds.	x			
4. Customer involved in trade finance or correspondent relationships.		x		**High Risk indicator:** Transfers from and to Taiwan expected. The customer needs a

			correspondent banking account.
5. Transaction involves the sale or purchase of dual-use, proliferation sensitive or military goods, particularly with higher risk jurisdictions.		x	**High Risk indicator:** Import/export of machine tools that can manufacture weapons of mass destruction.
6. Transaction involves the shipment of goods incompatible with the technical level of the country to which it is being shipped.	x		
7. Transactions involve possible shell companies. Indicators of shell companies may be use of nominee directors, mass registration address, address of a TCSP, limited capitalization and/or assets.	x		
8. Transaction involves person or entity in foreign country of proliferation concern or the country with weak export control laws.		x	**High Risk indicator:** Exports to Taiwan where the customer's father was indicted.
9. Transaction involves jurisdictions known to have inadequate AML/CTF/CPF measures.	x		
10. The customer makes out of character payments (including in cash) and/or transactions (payment in precious metals and stones and/or VAs) to other companies, subsidiaries or entities that belong to the same group. Consideration should be given to payments made to other companies that have the same directors, shareholders and/ or beneficial owners.		x	**High Risk indicator:** The client has received business related payments on his personal account.
11. Use of bulk cash or precious metals (e.g. gold) in transactions aimed for purchase of unrelated items (e.g., industrial items, real estate, etc.).	x		
12. Payment from purchaser is financed through an unusual source (e.g., offshore bank located in a high-risk jurisdiction).	x		
13. Purchaser pays the initial deposit with a third-party cheque.	x		
14. The speed of the transaction (e.g., sale or purchase of a good) is particularly fast.	x		
15. The customer is using complex loans or opaque means of financing which do not appear to involve regulated financial institutions.	x		
16. Client owns assets located in other jurisdiction and do not appear to be declared in tax returns.	x		
17. Client is invoiced by organizations that are in jurisdictions known for strict bank secrecy laws, offshore and/or high-risk jurisdictions.	x		
18. Transactions involve transshipment of dual-use / controlled items to high-risk jurisdictions.	x		

G. Sanctions and adverse media screening	NO	YES	Comments
1. Customer, or purchaser, or seller, or UBO is a confirmed name match while screening through sanction list (UNSC, UAE Local Terrorist List and other lists).		x	**High Risk indicator:** Gary's surname is a match for an OFAC sanctioned individual (Tsai).
2. Customer, or purchaser, or seller, or UBO is linked to negative news, crime and/or ML/TF/PF reports from watchlist screening tool.		x	**High Risk indicator:** Review of adverse media indicates that the customer's father has been indicted by authorities in Taiwan.

Recommendations

54. Gary Tsai has a high-risk profile. He matches a total of eight risk criteria, two of which relate to United Nations Security Council Resolutions (UNSCR) 1718 (2006) violations. His father supported KOMID, a UN sanctioned entity, and Gary Tsai who is in a business relationship with his father, may be acting for or on behalf of his father and KOMID. Indeed, while an entity may not be UN designated, it can still be subject to UNSCR provisions.[25] Based on this element, the FI should not onboard the customer and log a SAR/STR with the FIU.

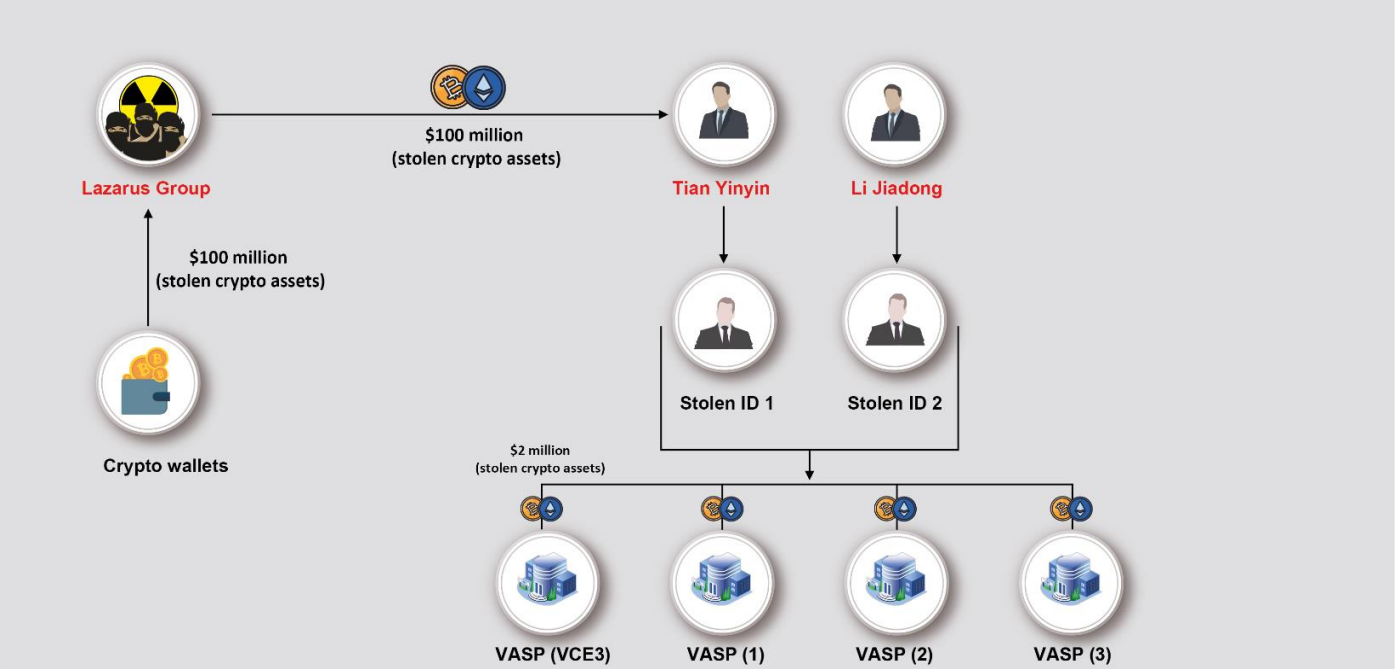
55. Under a scenario whereby elements relating to sanctions violations are not identified during CDD, the institution may decide to accept or reject the customer based on its risk appetite; however, implementation of EDD should be undertaken in the event the customer is onboarded.

[25] Operative Paragraph (OP) 6 of resolution 2087 (2013) calls upon "Member States to exercise enhanced vigilance including monitoring the activities of their nationals, persons in their territories, financial institutions, and other entities organized under their laws (including branches abroad) with or on behalf of financial institutions in the DPRK, or of those that act on behalf or at the direction of DPRK financial institutions, including their branches, representatives, agents and subsidiaries abroad". Available online: https://www.fatf-gafi.org/en/publications/Financingofproliferation/Unscr-proliferation-wmd.html, p. 13.
Gary Tsai's father, Alex Tsai, has been supplying goods with weapons production capabilities to Korea Mining and Development Trading Corporation (KOMID), a UN designated entity (refer to Security Council 1817 Sanctions Committee' s sanctions list for further detail. Available online: https://press.un.org/en/2022/sc14983.doc.htm).

VCE3 Case Study

Tian Yinyin and Li Jiadong, two Chinese nationals associated to the Lazarus group,[26] were charged by the US Department of Justice with laundering over $100 million in various cryptocurrencies on behalf of North Korea. The coins were obtained through hacks orchestrated by North Korea. Tian and Li moved the illegally acquired crypto assets through multiple VASPs.

To be successfully onboarded by VASPs, Tian and Li edited photos of individuals using stolen personal identifiable information. One VASP (referred to as VCE3[27]) was unsatisfied with the identification provided and requested a video call with the account holder. This was rejected by the account holder. Despite this, VCE3 accepted transactions from the account holder (i.e. Tian and Li), receiving almost $2 million of stolen assets.[28]



Case Analysis

56. While there is no public information relating to the controls that VCE3 had in place while providing services to Tian and Li, the documented controls below would assist in identifying and escalating suspicious activities:

[26] The Lazarus Group is a North Korean cybercrime organisation which is believed to be sponsored by North Korea. For more information, refer to: https://cointelegraph.com/top-people-in-crypto-and-blockchain-2023/lazarus-group.
[27] For further detail refer to: https://static.rusi.org/299_SR_CPF_VirtualAssetsGuide.pdf, p. 11 and 14.
[28] For further detail please refer to: https://home.treasury.gov/news/press-releases/sm924.

- The compliance department rightfully identified an issue with the identification documents provided by Tian and Li and requested a live video call to perform adequate KYC and CDD;

- The video call was denied, and Tian and Li were onboarded regardless. This indicates that had a live video call been a requirement, onboarding would not have happened, and the funds may not have been laundered through the VASP.

Assessing customer risk using the customer risk scoring questionnaire

57. Using the information documented in the VCE3 case study, this section illustrates the way a VASP onboarding a customer or performing ongoing due diligence checks on an existing customer, is expected to complete the CRS questionnaire. Each 'YES' and 'NO' box selected will influence the customer's overall PF risk score.

58. The following is a walkthrough of the CRS questionnaire for Tian and Li at onboarding. Accordingly, no information relating to transactions can yet be documented at this stage. Questions relating to transactions will be responded to as 'NO'. In addition, the reader should note that some information relating to what VCE3 knew or did not know is not available in the public domain. As a consequence, some sections have been documented as 'This information is not available in the public domain'.

A. Country risk	NO	YES	Comments
1. High risk or medium risk country as per your organization's internal guidance for the following:		x	**High Risk indicator:** Clients located in a country neighboring Democratic People's Republic of Korea (DPRK) and may be used for PF diversion.
2. Nationality		x	**Medium to High-Risk indicator depending on your institution's high risk country list:** Clients citizens of a country neighboring DPRK and may be used for PF diversion. This needs to be considered alongside other indicators.
3. Country of residence		x	**High Risk indicator:** Unsatisfactory identification provided. Client has rejected live video call.

4. Country of business activity		x		**High Risk indicator:** Unsatisfactory identification provided. Client has rejected live video call.

B. Customer risk	NO	YES	N/A	Comments
1. Origin of wealth and/or source of funds is easily identified or well described.	x			**High Risk indicator:** Not known as CDD is not complete
2. Customer's profile (age, occupation, employment status, salary, level of education) is consistent with wealth, transactions and account turnover.	x			**High Risk indicator:** Not known as CDD is not complete
3. Customers with valid reasons to open the account/establish the relationship in the requested jurisdiction.	x			**High Risk indicator:** Not known as CDD is not complete
4. Walk-in customers have not been actively prospected by the institution or lacking an obvious connection with the institution.	x			Not an issue as standard practice for VASPs. Robust KYC and CDD typically mitigates the risk.
5. Customers who have not been physically met.	x			Not an issue as standard practice for VASPs. Robust KYC and CDD typically mitigates the risk.
6. Customer introduced by a TCSP and/or uses an intermediary in all interactions including business relationships with no robust rationale.	x			
7. Politically Exposed Person (PEP) or related to a PEP.	x			
8. Customer working in high-risk industry. This includes arms dealing, manufacturing, nuclear industry including research, construction, art and antiques dealer, auctioning house, shadow banking, currency exchange bureaus, money transmitters, oil, precious metals and stones and high-value goods dealers, wildlife trade, maritime and international shipping, import/export related business, freight transportation or industries linked to goods subject to export control and DUGs, diplomacy, VASPs. *Refer to Table 5 for details of industries with elevated PF risk factors.*		x		**High Risk indicator:** Not known as CDD is not complete
9. Customer operating in gambling activities.		x		**High Risk indicator:** Not known as CDD is not complete

10. Customer involved in crypto-mining or trading with crypto currencies.		x		**High Risk indicator:** Not known as CDD is not complete
11. Customer operating from a complex, multi-layered business structure.		x		**High Risk indicator:** Not known as CDD is not complete
12. Complex legal structure with no reasonable economic or wealth management purpose.		x		**High Risk indicator:** Not known as CDD is not complete
13. Client is using companies where multiple, unexpected statutory changes have occurred. This may have been over a short period of time and may include, for example, the designation of new directors, a change in the country of registration to a high or medium risk country or the modification of the company's objective without an economic justification.		x		**High Risk indicator:** Not known as CDD is not complete
14. Dormant customer with a sudden unexplained surge in activities.	x			
15. Customer operates within a company with nominee directors and/or shareholders and/or bearer shares.		x		**High Risk indicator:** Not known as CDD is not complete
16. Missing ID documentation, invalid forms of ID, false and/or incomplete residential address, overall reluctance to provide CDD, KYC and ID documentation.		x		**High Risk indicator:** Missing ID&V and incomplete CDD.
17. The customer may be raising funds on behalf of designated individual/ entity. This includes holding a legal title to any asset, conducting transactions for the benefit of, or on behalf of, or at the direction of a designated individual or entity.		x		**High Risk indicator:** Not known as CDD is not complete
18. The customer displays signs of acting on somebody else's instruction and/or has a disproportionate level of authority provided by the end client.		x		**High Risk indicator:** Not known as CDD is not complete
C. Products, Services and Transaction risk	**NO**	**YES**	**N/A**	**Comments**
1. First transfer on the account made by cash deposit. For DNFBPs, this includes purchases done through multiple cash transactions or where seller insists on cash only payments.	x			
2. Commercial transaction at a price that is undervalued, overvalued or unjustified.			x	
3. Business relationship has no legitimate economic or legal grounds.		x		**High Risk indicator:** Not known as CDD is not complete

4. Customer involved in trade finance or correspondent relationships.			x	
5. Transaction involves the sale or purchase of dual-use, proliferation sensitive or military goods, particularly with higher risk jurisdictions.			x	
6. Transaction involves the shipment of goods incompatible with the technical level of the country to which it is being shipped.			x	
7. Transactions involve possible shell companies. Indicators of shell companies may be use of nominee directors, mass registration address, address of a TCSP, limited capitalization and/or assets.			x	
8. Transaction involves person or entity in foreign country of proliferation concern or the country with weak export control laws.		x		**High Risk indicator:** Potentially, as clients located in a country neighboring DPRK and may be used for PF diversion through use of front companies and import/export.
9. Transaction involves jurisdictions known to have inadequate AML/CTF/CPF measures.		x		**High Risk indicator:** Potentially, as clients located in a country neighboring DPRK and may be used for PF diversion.
10. The customer makes out of character payments (including in cash) and/or transactions (payment in precious metals and stones and/or VAs) to other companies, subsidiaries or entities that belong to the same group. Consideration should be given to payments made to other companies that have the same directors, shareholders and/ or beneficial owners.	x			
11. Use of bulk cash or precious metals (e.g. gold) in transactions aimed for purchase of unrelated items (e.g., industrial items, real estate, etc.).	x			
12. Payment from purchaser is financed through an unusual source (e.g., offshore bank located in a high-risk jurisdiction).	x			
13. Purchaser pays the initial deposit with a third-party cheque.	x			
14. The speed of the transaction (e.g., sale or purchase of a good) is particularly fast.	x			
15. The customer is using complex loans or opaque means of financing which do not appear to involve regulated financial institutions.	x			

16. Client owns assets located in other jurisdiction and do not appear to be declared in tax returns.	x		
17. Client is invoiced by organizations that are in jurisdictions known for strict bank secrecy laws, offshore and/or high-risk jurisdictions.	x		
18. Transactions involve transshipment of dual-use / controlled items to high-risk jurisdictions.			

D. Sanctions and adverse media screening	NO	YES	Comments
1. Customer, or purchaser, or seller, or UBO is a confirmed name match while screening through sanction list (UNSC, UAE Local Terrorist List and other lists).	x		
2. Customer, or purchaser, or seller or UBO is linked to negative news, crime and/or ML/TF/PF reports from watchlist screening tool.	x		

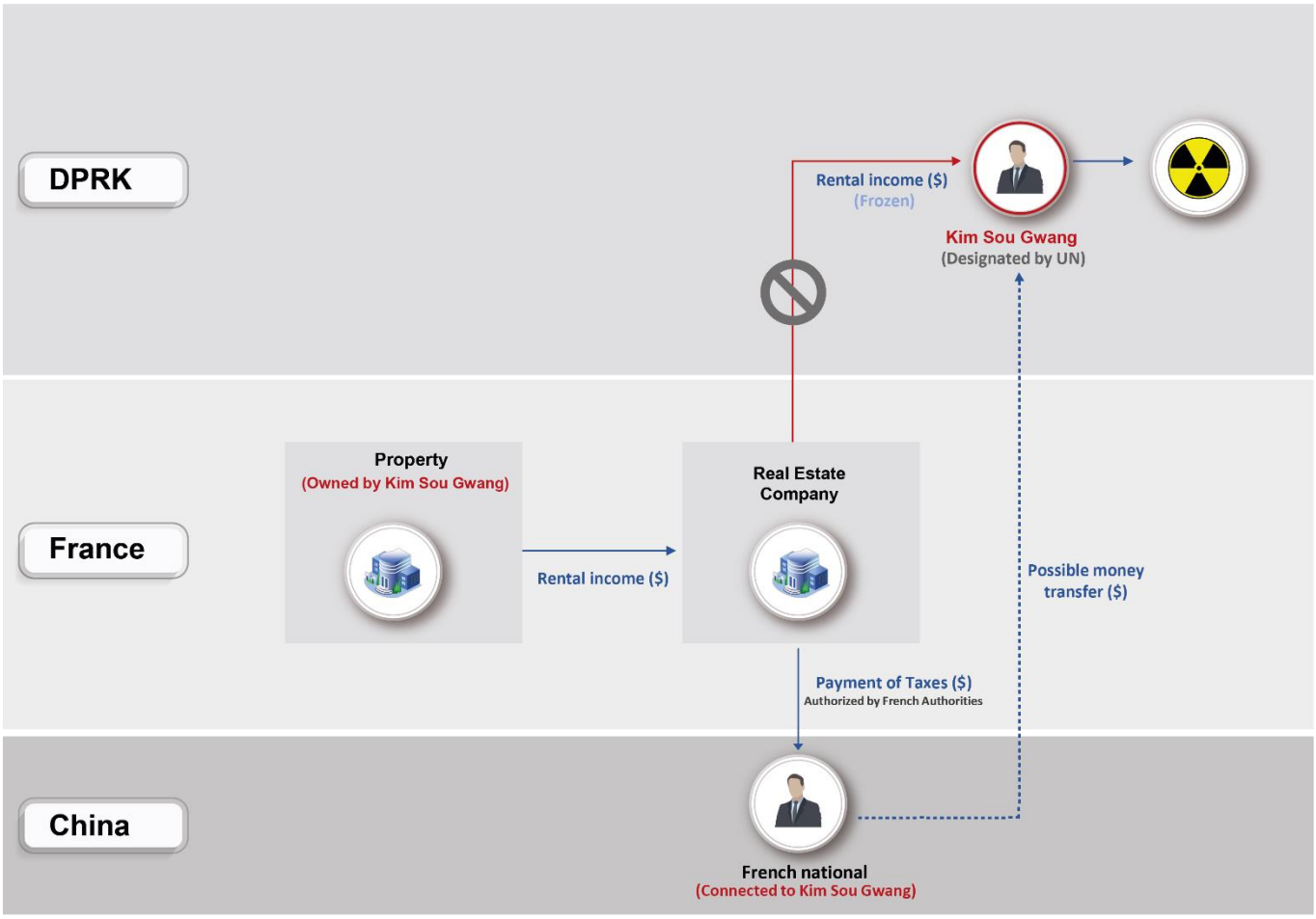
F. VASPs	NO	YES	Comments
1. The source of crypto is easily identified.	x		**High Risk indicator:** Blockchain analytics tool should identify that the source of crypto is associated to hacks.
2. The customer is not sharing IP addresses and/or using VPN services from established providers.			This information is not available in the public domain.
3. The customer wants to top up their wallet with high-risk payment methods.			This information is not available in the public domain.
4. The customer performs transactions that enable fiat on-ramp and off-ramp.			This information is not available in the public domain.
5. The customer engages in high-risk transactions such as arbitrage, gambling, mining.			This information is not available in the public domain.
6. The customer uses self-hosted and/or non-custodial wallets to store crypto.			This information is not available in the public domain.
7. The customer has a high wallet risk score as identified by Blockchain Analytics tools.		x	**High Risk indicator:** Blockchain analytics tool should identify that the source of crypto is associated to hacks.
8. The customer is a legal entity that is a high risk VASP. Consideration should be given to whether the customer is a cryptocurrency ATM, Cryptocurrency Mining, Decentralized Cryptocurrency Exchange, Mixers, OTC Broker, Custodial Service, Decentralized Autonomous Organizations. In addition, consideration should be given to the types of tokens that the VASP accepts on its platform. Finally, consideration should be given as to the VASP's AML/CTF/CPF policies and practices. This can be assessed via a correspondent relationship type questionnaire.		x	

Recommendations

59. Tian and Li have a high-risk profile. They match a total of 22 risk criteria as CDD was not adequately performed. Based on this element, the VASP should not have onboarded Tian and Li. Under circumstances where a potential client refuses to perform CDD, a SAR/STR should be logged with the FIU.

Kim Sou Gwang Case Study

Kim Sou Gwang, an agent for North Korea's Reconnaissance General Bureau, is a UN designated person who owns a property in Paris. Due to sanctions, the rental income on his Paris apartment was frozen. The French authorities allowed the real estate company to transfer a portion of the rental income for the payment of taxes to a French national residing in China. The transfers were not made to Kim Sou Gwang as he is a UN sanctioned individual but were made to the French national. However, the 2019 UN Panel of expert report indicates that "subsequent information revealed that this French national is connected to Kim and that the payments were likely still reaching him".[29]



Case Analysis

60. Although there is no further information in the public domain, we will assume for the purpose of the guide, that the real estate company did not consider this case as high risk because:

[29] Refer to the 2019 UN Panel of Expert Report. Available online: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf, p. 25.

- All funds were frozen;
- Relevant authorities had authorized the DNFBP to make transfers for the purpose of tax payments;
- Transfers were made to an individual who was not sanctioned.

61. While there is no public information relating to the controls that the real estate company had in place while setting up payments to the French national, the documented control(s) below would assist in identifying and escalating suspicious activities:

- Following Kim Sou Gwang's designation for United Nations Security Council Resolutions 1718 (2006) violations, sanctions and adverse media screening may have flagged the French national as being an associate acting for or on behalf of Kim Sou Gwang;

Assessing customer risk using the CRS questionnaire

62. Using the information documented in the Kim Sou Gwang case study, this section illustrates the way the DNFBP may decide to reclassify the customer file as high risk.

Each 'YES' and 'NO' box selected will influence the customer's overall PF risk score.

A. Country risk	NO	YES	Comments
1. High risk or medium risk country as per your organization's internal guidance for the following:		x	**High Risk indicator:** The owner of the property is a sanctioned North Korean diplomat.
2. Nationality		x	**High Risk indicator:** The owner of the property is a North Korean national
3. Country of residence		x	**High Risk indicator:** The individual receiving payments is based in a country neighboring DPRK and may be used for PF diversion.
4. Country of business activity	x		France

B. Customer risk	NO	YES	N/A	Comments
1. Origin of wealth and/or source of funds is easily identified or well described.		x		Rental income.

2. Customer's profile (age, occupation, employment status, salary, level of education) is consistent with wealth, transactions and account turnover.		x	
3. Customers with valid reasons to open the account/establish the relationship in the requested jurisdiction.		x	
4. Walk-in customers have not been actively prospected by the institution or lacking an obvious connection with the institution.	x		
5. Customers who have not been physically met.	x		
6. Customer introduced by a TCSP and/or uses an intermediary in all interactions including business relationships with no robust rationale.	x		
7. Politically Exposed Person (PEP) or related to a PEP.		x	**High Risk indicator:** Agent for the North Korean Reconnaissance General Bureau
8. Customer working in high-risk industry. This includes arms dealing, manufacturing, nuclear industry including research, construction, art and antiques dealer, auctioning house, shadow banking, currency exchange bureaus, money transmitters, oil, precious metals and stones and high-value goods dealers, wildlife trade, maritime and international shipping, import/export related business, freight transportation or industries linked to goods subject to export control and DUGs, diplomacy, VASPs. *Refer to Table 5 for details of industries with elevated PF risk factors.*		x	**High Risk indicator:** UN sanctioned North Korean diplomat working in the Reconnaissance General Bureau.
9. Customer operating in gambling activities.	x		
10. Customer involved in crypto-mining or trading with crypto currencies.	x		
11. Customer operating from a complex, multi-layered business structure.	x		
12. Complex legal structure with no reasonable economic or wealth management purpose.	x		
13. Client is using companies where multiple, unexpected statutory changes have occurred. This may have been over a short period of time and may include, for example, the designation of new directors, a change in the country of registration to a high or medium risk country or the modification of the company's objective without an economic justification.	x		
14. Dormant customer with a sudden unexplained surge in activities.	x		
15. Customer operates within a company with nominee directors and/or shareholders and/or bearer shares.	x		
16. Missing ID documentation, invalid forms of ID, false and/or incomplete residential address, overall reluctance to provide CDD, KYC and ID documentation.	x		
17. The customer may be raising funds on behalf of designated individual/ entity.		x	**High Risk indicator:** Owner of the

This includes holding a legal title to any asset, conducting transactions for the benefit of, or on behalf of, or at the direction of a designated individual or entity.				property is a known North Korean diplomat. Rental income may be used to support North Korea.
18. The customer displays signs of acting on somebody else's instruction and/or has a disproportionate level of authority provided by the end client.		x		**High Risk indicator:** The French national receiving payments on his behalf has not provided CDD. There is uncertainty as to whether he may be acting for or on behalf of Kim Sou Gwang.

C. Products, Services and Transaction risk	NO	YES	N/A	Comments
1. First transfer on the account made by cash deposit. For DNFBPs, this includes purchases done through multiple cash transactions or where seller insists on cash only payments.			x	
2. Commercial transaction at a price that is undervalued, overvalued or unjustified.			x	
3. Business relationship has no legitimate economic or legal grounds.			x	
4. Customer involved in trade finance or correspondent relationships.			x	
5. Transaction involves the sale or purchase of dual-use, proliferation sensitive or military goods, particularly with higher risk jurisdictions.			x	
6. Transaction involves the shipment of goods incompatible with the technical level of the country to which it is being shipped.			x	
7. Transactions involve possible shell companies. Indicators of shell companies may be use of nominee directors, mass registration address, address of a TCSP, limited capitalization and/or assets.			x	
8. Transaction involves person or entity in foreign country of proliferation concern or the country with weak export control laws.		x		**High Risk indicator:** French national residing in a country neighboring DPRK and may be used for PF diversion.
9. Transaction involves jurisdictions known to have inadequate AML/CTF/CPF measures.		x		**High Risk indicator:** French

			national residing in a country neighboring DPRK and may be used for PF diversion.
10. The customer makes out of character payments (including in cash) and/or transactions (payment in precious metals and stones and/or VAs) to other companies, subsidiaries or entities that belong to the same group. Consideration should be given to payments made to other companies that have the same directors, shareholders and/ or beneficial owners.	x		
11. Use of bulk cash or precious metals (e.g. gold) in transactions aimed for purchase of unrelated items (e.g., industrial items, real estate, etc.).	x		
12. Payment from purchaser is financed through an unusual source (e.g., offshore bank located in a high-risk jurisdiction).	x		
13. Purchaser pays the initial deposit with a third-party cheque.	x		
14. The speed of the transaction (e.g., sale or purchase of a good) is particularly fast.	x		
15. The customer is using complex loans or opaque means of financing which do not appear to involve regulated financial institutions.	x		
16. Client owns assets located in other jurisdiction and do not appear to be declared in tax returns.	x		
17. Client is invoiced by organizations that are in jurisdictions known for strict bank secrecy laws, offshore and/or high-risk jurisdictions.	x		
18. Transactions involve transshipment of dual-use / controlled items to high-risk jurisdictions.			

D. Sanctions and adverse media screening	NO	YES	Comments
1. Customer, or purchaser, or seller, or UBO is a confirmed name match while screening through sanction list (UNSC, domestic list and other lists).		x	**High Risk indicator:** UN sanctioned North Korean national.
2. Customer, or purchaser, or seller, or UBO is linked to negative news, crime and/or ML/TF/PF reports from watchlist screening tool.		x	**High Risk indicator:** We assume for the purpose of this exercise that the name of the French national is a match on adverse media (UN PoE Report).

E. DNFBPs	NO	YES	Comments
1. Customer's economic profile/business activity and purpose aligns with the cost of the good.	x		
2. Customer's source of funds can be identified and documented.	x		

3. Customer is using an intermediary for interactions and conducting transactions with no logical reason. Consideration must also be given to a customer who appears to be acting on behalf of a third party whose identity is concealed. In addition, consideration must be given to the good standing of the intermediary and whether they are adequately supervised and trained. Finally, consideration must also be given to potential different geolocations between the customer and the intermediary and whether there is a rationale.	x		
4. Customer is purchasing the good in the name of a nominee, a relative, or on behalf of minors. Consideration must be given as to whether the customer hesitates or declines to put his name on documentation connecting them to the goods.	x		
5. The customer structures payments to ensure that transactions do not exceed DNFBPs' CDD thresholds as per FATF Recommendation 22. More specifically, DNFBPs' thresholds are: • USD 15,000 in cash for dealers in precious metals & stones • USD 3,000 for casinos	x		
6. Purchaser/ seller is unconcerned about the economic or investment value of the good being purchased/sold.	x		
7. Purchaser/ seller buys/ sells multiple goods in a short period of time and has limited concerns or interests relating to the location and/ or price of the good.	x		
8. Lack of clarity of who the end user is and/or involvement of a third party (e.g., payment from third party or delivery of good to a third party who did not purchase the goods).		x	**High Risk indicator:** The French national residing in China may be acting on behalf of Kim Sou Gwang and North Korea.
9. The customer is not concerned with making losses where loss is avoidable.	x		
10. The customer offers to pay unusually high fees for a product or a service with no rationale.	x		

Recommendations

63. Activity associated with the management of Kim Sou Gwang's property is high risk. It matches a total of 12 risk criteria and requires the DNFBP to reclassify the account as high risk. Under such circumstances, a SAR should be logged with the local FIU as the French national residing in China is suspected to be acting for or on behalf of Kim Sou Gwang who is sanctioned by the United Nations.[30]

[30] Refer to the 2019 UN Panel of Expert Report. Available online: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf, p. 25, para. 54.

64. The DNFBP may subsequently decide to liaise with relevant authorities to identify next steps (i.e., suspend payments to the French national residing in China and exit the customer relationship).

Conclusion

65. This guide is an addendum to the Guidance on Counter Proliferation Financing for FIs, DNFBPs, and VASPs. It aims to provide additional support to the private sector as to how to identify and mitigate PF risk, including the necessary methodology for developing and conducting an institutional PF RA, and identifying mitigating controls and strategies.

66. While the addendum provides a useful starting point for conducting an institutional PF RA, institutions are ultimately responsible for analyzing and applying these guidelines in a way that produces a reasonable judgement of their PF institutional risk.

67. For further information on Targeted Financial Sanctions, the UAE's legal framework and how to report confirmed or partial name matches, FIs, DNFBPs, and VASPs should refer to the Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs issued by the EOCN.