P O Box 427 Pretoria 0001 South Africa
370 Helen Joseph Street Pretoria 0002
+27 12 313 3911 / 0861 12 7272
www.resbank.co.za

South African Reserve Bank
Prudential Authority

Ref.: 15/8/1/2

G12/2022

To: All banks, branches of foreign institutions, controlling companies, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Guidelines related to risk management practices concerning proliferation financing risk.

Executive summary

The purpose of this Guidance Note is to provide guidance to banks, branches of foreign institutions and controlling companies (hereinafter collectively referred to as 'banks'), and to inform eligible institutions and auditors of banks or controlling companies, regarding the implementation of corporate governance, risk management, internal controls, policies, processes and procedures to ensure banks' compliance and adequate risk management of exposure to the financing of proliferation of weapons of mass destruction (WMD), taking into account Recommendation 1 and 7 of the Financial Action Task Force (FATF) Recommendations.

Regulation 36(17) of the Regulations relating to Banks (Regulations) requires, among others, that banks' policies, processes and procedures should be sufficiently robust to ensure that the bank or controlling company, inter alia, continuously receives relevant information relating to risk exposure incurred by any foreign operation and that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time; and the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.

1. Introduction

1.1. Targeted financial sanctions regimes

1.1.1. South Africa's targeted financial sanctions regime originates from resolutions of the United Nations Security Council Resolutions (UNSCR) under Chapter VII of the Charter of the United Nations (UN). South Africa implements two distinct targeted financial sanctions regimes through the Financial Intelligence Centre Act 38 of 2001 (FIC Act) and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (POCDATARA Act), which form part of the anti- money laundering and counter financing of terrorism (AML/CFT) regulatory framework.

1.1.2. Proliferation financing (PF)[1] risk refers strictly to the potential breach, non-implementation, or evasion of the Targeted Financial Sanctions (TFS) obligations referred to in FATF Recommendation 7.

1.1.3. Proliferation of weapons of mass destruction according to FATF[2] refers to the "…manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual-use goods used for non-legitimate purposes)".

1.1.4. The definition of financing of proliferation of WMD as set out in FATF guidance[3] refers to: "…the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for nonlegitimate purposes)"

1.1.5. Sections 26A, 26B and 26C of the FIC Act, include the TFS obligations relating to the Chapter VII of the United Nations Charter, which is also aimed at combating proliferation financing. These provisions deal with the financing element of terrorism or proliferation of WMD, and not the act of terrorism or proliferation itself.

1.1.6. The UNSC resolutions relevant to PF TFS are implemented through section 26A of the FIC Act. UNSC resolutions 1718(2006), 2087(2013), 2094(2013) and 2270(2016) relate to the Democratic People's Republic of Korea (DPRK) and set out the specific restrictions that include TFS aimed at combating PF[4].

1.2. International standards

1.2.1. South Africa, as a member of the FATF, has a duty to conform to the FATF's 40 Recommendations against money laundering and terrorism financing. The FATF Recommendation 7 focuses on the requirement relating to the implementation of the UNSCRs on TFS regime for all FATF member countries.

1.2.2. During 2021 the FATF Recommendation 1 was updated to require countries to additionally identify, assess and understand the PF risks for the country and respective private sector, and to take action to mitigate such risks[5].

1.2.3. The FATF Recommendation 2 requires countries to ensure that policymakers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate and, where appropriate, coordinate domestically with one another concerning the development and implementation of policies and activities to combat ML/TF and the financing of WMD proliferation.

---

[1] Currently, there is no universal definition of proliferation financing, however the June 2021 FATF Guidance on Proliferation Financing Risk Assessment Mitigation (FATF Guidance), stated that the financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes. Thus, the underlying financial services/activities make proliferation possible.

[2] FATF Guidance on proliferation financing risk assessment and mitigation June 2021

[3] FATF Guidance on proliferation financing risk assessment and mitigation June 2021

[4] https://www.un.org/securitycouncil/sanctions/information

[5] Over and above money laundering and counter financing of terrorism risk.

1.2.4. The FATF Recommendation 6 requires countries to implement TFS regimes to comply with UNSCRs relating to the prevention and suppression of terrorism and terrorist financing (including identifying and preventing sanctions evasion). The resolutions require countries to freeze, without delay, the funds or other assets, and to ensure that no funds or other assets are made available to, directly or indirectly, or benefit any person or entity either designated by, or under the authority of, the UNSCR under Chapter VII of the Charter of the UN, including in accordance with UNSCR 1267 (1999) and its successor resolutions or designated by that country pursuant to UNSCR 1373 (2001).

1.2.5. The FATF Recommendation 7 is applicable to all current and future successor resolutions to UNSCR 1718 (2006). This requires countries to implement TFS to comply with the UNSCRs relating to the prevention, suppression and disruption of the financing of proliferation of WMD and its financing. These resolutions require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, directly or indirectly, or benefit any person or entity designated by, or under the authority of, the UNSCR under Chapter VII of the Charter of the UN.

1.2.6. FATF Recommendation 7 aims to restrict designated individuals and/or entities[6] and/or vessels[7] involved in the proliferation of WMD from raising, moving and/or using funds.

1.2.7. FATF Recommendations 1, 2, 7 and 15 are the specific standards that focus on PF.

1.2.8. In particular, FATF Recommendations 2, 6 and 7 require each country to implement TFS regimes to comply with the UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, including proliferation and PF.

1.2.9. The Panel of Experts Report[8] issued by the United Nations Security Council (UNSC) highlights the present and persistent risk to international security in respect of WMD, for example nuclear, biological, and chemical weapons.

1.3 Legislative requirements

1.3.1. In July 1993 South Africa enacted and implemented the provisions of the Non- Proliferation of Weapons of Mass Destruction Act 87 of 1993 (NPWMD Act) which created the national legal framework for the South African Council for the Non- Proliferation of Weapons of Mass Destruction (Non-Proliferation Council)[9] and for the government to prevent the development of WMD, including controlling trade in goods that could be used in the development or production of WMD. It should be noted where these goods may also have commercial applications they would be classified as dual-use goods.

1.3.2. The NPWMD Act made it a criminal offence for any South African citizen to develop or assist in the development of chemical, biological, and nuclear weapons as well as missile delivery systems for such weapons, including ballistic missiles. It established national control over the use, import, or export of dual-use equipment, relevant

[6] https://www.fic.gov.za/Documents/SOUTH%20AFRICA%20IMPLEMENTS%20TARGETED%20FINANCIAL%20SANCTIONS.pdf

[7] Full listing of vessels designated by the UNSC can be found on the UNSCRs 1718 of 2006 and 2270 of 2016, including any succeeding resolutions, Designated Vessels List available at: https://www.un.org/securitycouncil/sanctions/1718/materials/1718-Designated-Vessels-List

[8] United Nations Security Council Report of Panel of Experts 2019, available at https://undocs.org/S/2019/691

[9] Non-Proliferation Council and the legislation is available on the website: http://non-proliferation.thedtic.gov.za

materials, or purpose-built equipment.

1.3.3. The list of controlled nuclear dual-use items reflected the dual-use list of the Nuclear Suppliers Group (NSG), and the controlled missile and delivery systems dual-use items reflected the Category I and Category II lists of the Missile Technology Controlled Regime (MTCR).

1.3.4. The chemical list includes, but is not limited to, the Chemical Weapons Convention scheduled chemicals while the biological list is compiled based on the Non-Proliferation Council's assessment of proliferating biological items.

1.3.5. The NPWMD Act inter alia provides for:

1.3.5.1. the establishment of the Non-Proliferation Council;
1.3.5.2. support by the Department of Trade, Industry and Competition (DTIC);
1.3.5.3. appointment of inspectors;
1.3.5.4. seizure of goods for alleged contravention of the NPWMD Act; registration when involved in controlled activities; certain goods and technologies to be declared as controlled goods; the Minister to promulgate regulations for such controlled goods; information received by the Council to be treated with confidentiality; annual reporting on the activities of the Council; offences and penalties applicable to such; treaties, conventions and regimes to be part of the schedule of the Act.

1.3.6. The Nuclear Energy Act 46 of 1999 (NEA) was revised in 1999 to embody the obligations undertaken by South Africa when it acceded to the Non-Proliferation of Nuclear Weapons Treaty (NPT) and signed a safeguards agreement with the International Atomic Energy Agency (IAEA).

1.3.7. The NEA and associated regulations prohibit the export of nuclear materials, equipment, technology, or facilities to non-nuclear weapons states, unless they have full-scope IAEA safeguards in operation. In terms of the NEA nuclear exports can be or is controlled.

1.3.8. In terms of the Banks Act the following Regulations are applicable:

1.3.8.1. Regulations 36(17)(a)(iv) and 36(17)(b)(ii) of the Regulations, state that in order to promote and maintain sound standards in respect of corporate governance, risk management and internal controls, every bank and every bank controlling company shall have in place board-approved policies and comprehensive risk- management processes and procedures, which policies, processes and procedures (i) shall include comprehensive and robust know-your-client standards that shall prevent the bank from being used for any money laundering or other unlawful activity and (ii) shall be sufficiently robust to ensure that the relevant bank continuously (ii) monitors account activity for potential suspicious transactions.

Regulations 36(17)(b)(ii)[10], 38(4), 39(1) to (3)[11] and 50[12] of the Regulations, are relevant to requirements applicable to all banks, controlling companies, representative offices, eligible institutions, and auditors of banks or controlling companies, to

[10] Regulation 36(17)(b)(ii) requires that entities should implement and apply at all times AML/CFT measures consistent with relevant/applicable FATF Recommendations, which inter alia states that entities should always apply the higher AML/CFT standards issued in the Republic of South Africa or in the host country.

[11] Regulation 39: Banks should manage its risk, of which one of the risks include "detection and prevention of criminal activities.

[12] Regulation 50: A bank shall implement and maintain robust structures, policies, processes to guard against the bank being used for purposes of financing of terrorism and money laundering.

implement corporate governance, risk management, internal controls, policies, processes, and procedures to ensure ongoing compliance and adequate risk management of risk exposure, which exposure may PF risk exposure.

1.3.8.2. In terms of regulation 38(4)(c) of the Regulations, if the PA is of the opinion that the policies, processes, and procedures of banks relating to its risk assessments are inadequate, the PA may require the said bank to strengthen the bank's risk management policies, processes or procedures.

1.3.9. The application of the UNSCRs and FATF Recommendations by South Africa is reflected in sections 26A, 26B, 26C and 28A of the FIC Act, as well as sections 4 and 25 of the POCDATARA Act.

1.3.10. Section 26B read together with section 49A of the FIC Act, prohibits the financing of persons/entities who are subject to TFS in terms of section 26A of the FIC Act.

1.3.11. One of the principal objectives of the FIC Act, requires accountable institutions (AIs) to immediately freeze property and transactions pursuant to resolutions adopted by the UNSC referred to in a notice contemplated in section 26A of the FIC Act TFS provides for financial sanctions only and includes a list of all persons and/or entities and/or vessels who are subject to TFS under the FIC Act.

1.3.12. The non-implementation, a breach or evasion of PF-TFS may result in reputational damage to the country, relevant sector(s) or private sector firms, and punitive measures such as the implementation of sanctions by the UN and/or national authorities.

2. PF risks

2.1. At a country level, South African PF of WMD risk factors stem from several environmental vulnerabilities that can be exploited to facilitate PF, which, inter alia, may consist of the following:

2.1.1. poor enforcement of security protocols and contraventions by officials in the Border Security environment in the issuing of travel and identity documentation is the first major PF vulnerability[13];

2.1.2. in the context of a large informal economy that is mostly cash-based, a large number of remittances from émigré communities to their host countries, including high-risk countries, present a further vulnerability that can be abused for PF;

2.1.3. against the background of voluntary registration, non-profit organisations (NPOs) that operate in high-risk jurisdictions and insufficient attention being applied to security concerns linked to PF by regulatory authorities; and

2.1.4. crowdfunding by clients via the use of new payment technologies which platforms lack regulations by regulatory authorities.

2.2. The non-implementation, a breach or evasion of PF-TFS may result in reputational damages to the country, relevant sector(s) or private sector firms, and punitive measures such as the implementation of sanctions by the UN and/or national authorities.

[13] Hong Kong Monetary Authority "Guideline on Anti-Money Laundering and Counter-Financing of Terrorism" September 2020 Available at: https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline_on_AMLCFT_for_SVF_eng_Sep2020.pdf and UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014).

2.3. Within SA, it is possible for entities to inadvertently process funds that are unknowingly linked to PF and/or the movement of goods destined for proliferation of WMD. It is not enough to merely conduct sanctions screening, but rather delve into the potential for heightened PF of WMD risk factors within the bank's operations.

2.4. In consideration of the legislative requirements outlined in paragraph 1.3. above, banks must be cognisant of the requirements set out in Regulations 36(17)(a)(iv) and 36(17)(b)(ii), 38(4)(c), 39(1) to (3) and 50 of the Regulations**,** to enable them to adequately assess their risk and ensure the required policies, processes and controls are in place to mitigate the risk of PF.

2.5. In order to ensure an effective risk approach, a PF risk assessment that is undertaken will assist the bank. It is important that banks fully understand and document their inherent and residual PF of WMD risks to which the business's operations could be exposed to.

2.6. A PF risk assessment should include the following:

2.6.1 identification of all PF threats and vulnerabilities by compiling a list of major known or suspected threats, key sectors, products or services, activities that designated individuals/entities engaged in or that have been exploited, based upon known typologies; and

2.6.2 assessment and risk rating of the identified PF threats and vulnerabilities in light of the nature, scale, complexity and geographical footprint of the bank, its target market/s and client profiles, the volume and size of its transactions and the products and services offered.

2.7. Regular PF of WMD risk assessments are necessary to enhance and update banks' PF risk understanding and be in a position to evidence same.

2.8. Banks must articulate their understanding of their PF of WMD risks in their implemented corporate governance, risk management, internal controls, policies, processes and procedures to ensure ongoing compliance and adequate risk management of their respective exposures to risk.

3. PF client risk assessment

3.1. PF client risk should be identified and assessed in accordance with the processes, procedures and methodology outlined in banks' risk management and compliance programmes.

3.2. In assessing PF client risk, banks should[14][14]:

3.2.1. scrutinise all clients at on-boarding to ensure that the client is not a sanctioned person/entity;

3.2.2. assess whether the client is connected or situated in a country that is subject to relevant UN sanctions;

3.2.3. assess the type of business the client engages in, particularly businesses dealing in dual-use goods or goods subject to export control or complex transactions;

[14] https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment- Mitigation.pdf

3.2.4. consider that a client who lists a dual-use good as being traded may have a legitimate purpose for the dual-use good and would need to apply to the appropriate authority (such as the Non-proliferation Council) for a permit to obtain authorisation to trade therein and that where such permit is produced may be a contributing factor for consideration in the overall risk assessment of the client;

3.2.5. consider that proliferators may not openly indicate that they wish to trade in controlled goods and may also seek to trade in goods that have specifications that are slightly below the specifications of controlled goods and may modify/upgrade/process goods further down the line to the controlled specifications as per their requirements for use in proliferation activities;

3.2.6. assess whether the client's duration of the business accords with the knowledge and transactional activity of the client;

3.2.7. consider how the geographic proximity to jurisdictions that are vulnerable to PF of WMD risk may impact it;

3.2.8. consider if the client is diplomatic personnel or linked to any embassy or diplomatic personnel from high-risk countries with high PF and/or WMD proliferation concerns;

3.2.9. consider if higher PF and/or WMD proliferation risks may be present where there are active ports and potential PF transit/transhipment routes (South Africa has large and active ports in Africa);

3.2.10. consider the cross-border financial and trade flow with high-risk jurisdictions (e.g., linked to mineral products/iron, steel, machinery, chemicals, vehicles, aircraft and vessels for North Korea or relate to copper and precious metals for Iran but strong fluctuations in flows;

3.2.11. assess the level of disclosure or proposed trading activities by clients during on-boarding or the vagueness of such disclosure when requested to do so;

3.2.12. assess whether clients have the requisite technical knowledge/skill to align to the stated business activity that they wish to conduct;

3.2.13. assess whether the utilisation of numerous third parties and/or complex trade-based activities are aligned to the business profile held in respect of the client at onboarding or during the client relationship;

3.3. ensure that where trade finance transactions are concerned in respect of clients, that they thoroughly understand the activities of their clients with regards to the trade finance transactions being engaged in, including the beneficial owners, the parties to the transaction and the flow of funds in terms of geographical areas, with increased scrutiny being applied where heightened risk is identified.

3.3.1. assess whether the originator and/or beneficiary of a transaction is a person or entity resident or domiciled in a country of PF or diversion concern; and/or

3.3.2. consider additional factors such as the purpose of the relationship, corporate structure and volume of anticipated transactions which may be indicators of increased potential for PF risk.

3.4. When assessing the shipment of goods (import, transit, transhipment and/or export transactions), banks may consider the following:

3.4.1. goods are shipped with inconsistent and unconventional geographic patterns;

3.4.2. goods are shipped via countries with weak implementation of UNSCR obligations;

3.4.3. the export controls in the countries of trade and the implementation thereof;

3.4.4. the shipping cost of goods is high in comparison to the declared value of the goods;

3.4.5. a freight forwarding firm is listed as the final destination of the product;

3.4.6. the importer's location and the destination of the shipment do not align; and/or

3.4.7. the application of an enhanced due diligence approach to obtain full information of all the trade documents and financial flows would assist in understanding the potential PF risks at all levels of the transactions regarding trade-based finance transactions.

3.5. Banks should ensure that all monitoring, mitigation, and management of their PF risk at a client level are diligently and accurately recorded and that this is able to be evidenced.

4. Typologies

4.1. 'Typologies' refer to the various techniques used to finance the proliferation of WMD.[15][15], which can assist banks, controlling companies, branches of foreign institutions, and auditors of banks or controlling companies in identifying PF risks.

4.2. Examples of different typologies linked to PF risks identification are set out in Annexure A of this Guidance Note.

5. Acknowledgment of receipt

5.1. Kindly ensure that a copy of this proposed guidance is made available to your institution's independent auditors. The attached acknowledgment of receipt duly completed and signed by both the chief executive officer of the institution and the said auditors should be returned to the PA at the earliest convenience of the aforementioned signatories.

Fundi Tshazibana

Fundi Tshazibana
Chief Executive Officer

Date: 28/10/22

Encl. 1

[15] Battelle Memorial Institute RA Weise, G Hund and G Carr 2018 Export controls and counter-proliferation finance: Two sides of the same underlying illegal weapons of mass destruction (WMD) activities available at: https://www.tandfonline.com/doi/full/10.1080/10736700.2018.1473107

The previous Guidance Note issued was Guidance Note 11/2022 dated 23 September 2022.

Annexure A

Typologies

The following are a few examples of typologies linked to PF risk abuses to which banks could be exposed.

It should be noted that the understanding of the underlying procurement process of goods is critical. It is more likely that individual goods or components will be shipped rather than off-the-shelf weapons.[16]

Typologies		
No.	**Type of technique**	**Description**
1.	Front companies (procurement)	The procurement network used by Pakistan mostly operates through front companies. Different front companies may use the same address, the same phone numbers and the same managers, and may issue identical requests for quotations to multiple suppliers over long periods of time (e.g., six months to two years).[17] Front companies have also been used by Syria as a procurement method. The Syrian Scientific Studies and Research Centre (SSRC) was believed to be a significant entity developing Syria's chemical weapons and ballistic missile programme, but piloted procurement programmes (before 2011) by ordering goods from foreign suppliers via front companies.[18]
2.	Individual goods and component parts (the 'nuts and bolts')	'Nuts and bolts' were exported by a Dutch shipping company to Iran through a network of companies in Malaysia. The beneficial owner of the companies acted as a broker between two individuals and the Iranian buyers. The broker had a contract to procure and supply Iranian aviation firms with parts and components for planes and helicopters.[19]
3.	Cybercrime (Theft and extortion via the use of code used in the malicious software deployed)	On 4 February 2016, hackers targeted the Bangladesh Central Bank with the aim of effecting fraudulent transfers totalling as much as US$951 million from the Bangladesh Central Bank's account at the Federal Reserve Bank of New York. Most of the attempted transfers were blocked, but US$81 million was routed to accounts in the Philippines and diverted to casinos, and most of these funds are still missing.20[20]

[16] Centre for a New American Security Brewer, J January 2018, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation, Centre for a New American Security (CNAS) available at: https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation.

[17] J Brewer, October 2017, *Project Alpha: Final Report of the Study of Typologies of Financing of WMD Proliferation*, Kings College London, available at https://www.kcl.ac.uk/alpha/assets/pdfs/FoP-13-October-2017-Final.pdf, and comments made to the author by officials of an EU member state during the course of this study.

[18] Centre for a New American Security and Brewer, J January 2018, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation,Centre for a New American Security (CNAS) available at: https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation

[19] Centre for a New American Security and J Brewer January 2018, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation, Centre for a New American Security (CNAS) available at: https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction- proliferation

[20] Centre for a New American Security and J Brewer - Kings College London October 2017, Project Alpha: Final Report of the Study of Typologies of Financing of Weapons of Mass Destruction Proliferation available at: https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation.

Typologies		
No.	**Type of technique**	**Description**
4.	Entity without a website or stated business purpose	In 2017, the US Department of Justice brought a civil asset forfeiture complaint for the US$1.9 million associated with Mingzheng, a Hong Kong-based company that sent and received wires in US dollars on behalf of a foreign trade bank that was involved in the DPRK's WMD programme.[21]
5.	Diplomatic cover	A preferred method used by the DPRK is the use of diplomatic cover in proliferation-related procurement and fundraising. The UN's Panel of Experts on the DPRK 2019 confirmed a persistent trend by DPRK diplomats stationed overseas acting as procurement agents for their country's WMD programme and using their bank accounts in developing countries to pay for goods.[22]
6.	Sanctions evasion (Falsifying documents)	Gradually, more shipping companies and vessels are used prominently in sanctions evasion. For example, the DPRK and Iran falsify documents, reflag vessels, and switch off automatic identification systems to avoid being discovered in the process of illicit transfers of goods.[23]
7.	Misrepresenting: price, quality and/or quantity of goods (under-, over- and/or multiple invoicing, including short-, over- and phantom-shipping)	The techniques of misrepresenting the price, quality and/or quantity of goods and/or the shipping thereof rely on collusion between the seller, buyer and/or broker. Another example is the procurement of goods under the threshold limit.[24] Such arrangements aim to obtain a benefit in excess of what would be expected from an arm's length transaction. Such a relationship may arise as both parties could be controlled by the same person(s).[25] It is not feasible to try and determine whether cases of over- invoicing or under-invoicing exist based on the trade documents alone.[26] However, FIs could use unit pricing to determine whether it appears manifestly unusual, which could prompt an enquiry to be made. As such, an FI's risk-based approach[27] should provide the steps to be taken in respect of individual clients or transactions based on that FI's analysis of the risk(s) in relation to the parties

[21] United States (US) Department of Justice, 15 June 2017, *United States Files Complaint to Forfeit More Than $1.9 Million from China-Based Company Accused of Acting as a Front for Sanctioned North Korean Bank*, available at: https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeitmore-19-million-china-based-company-accused- acting

[22] United Nations Security Council (UNSC), March 2019, UNSC – S/2019/171, available at: https://ww.undocs.org/S/2019/171, 52 to 53.

[23] Association of Certified Anti-Money Laundering Specialist ACAMS "Proliferation Financing: What Financial Institutions Should Know and What They Can Do?" September 2019 available at: https://www.acamstoday.org/proliferation- financing-what-financial-institutions-should-know-and-what-they-can-do/ and ACAMS March 2019 "2019 UN North Korea Panel of Experts report: Takeaways for Financial Institutions" – Togzhan Kassenova https://www.acamstoday.org/2019-u-n-north-korea-panel-of-expers-report-takeaways-for-financial-insitutions-2

[24] Association of Certified Anti-Money Laundering Specialist ACAMS "Proliferation Financing: What Financial Institutions Should Know and What They Can Do?" September 2019 available at: https://www.acamstoday.org/proliferation- financing-what-financial-institutions-should-know-and-what-they-can-do/.

[25] The Wolfsberg Group: 'The Wolfsberg Group, International Chamber of Commerce (ICC) and Bankers Association for Finance and Trade (BAFT) Trade Finance Principles', Wolfberg Group 2017, available at: http://www.wolfsberg- principles. com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.

[26] The Wolfsberg Group: 'The Wolfsberg Group, International Chamber of Commerce (ICC) and Bankers Association for Finance and Trade (BAFT) Trade Finance Principles', Wolfberg Group 2017, available at: http://www.wolfsberg- principles. com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf

[27] The Wolfsberg Group has issued general guidance on a Risk-Based Approach (RBA) 12 in relation to trade finance, available at http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_RBA_Guidance (2006).pdf.

Typologies		
No.	**Type of technique**	**Description**
		involved, the type of transaction(s), the monetary value of the transaction(s), and any other factors that may either increase or reduce the risk of financial crime in any given transaction.[28]
8.	Government oversight and licensing	Another method used by proliferates is to pretend that they are ordering goods for a domestic company (i.e., supplier companies do not have to apply for licences); in this way they avoid government oversight and/or licensing requirements.[29]

[28] The Wolfsberg Group: 'The Wolfsberg Group, International Chamber of Commerce (ICC) and Bankers Association for Finance and Trade (BAFT) Trade Finance Principles', Wolfberg Group 2017, available at: http://www.wolfsberg- principles. com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.

[29] Association of Certified Anti-Money Laundering Specialist ACAMS "Proliferation Financing: What Financial Institutions Should Know and What They Can Do?" September 2019 https://www.acamstoday.org/proliferation-financing-what- financial-institutions-should-know-and-what-they-can-do/.