مصرف البحرين المركزي
Central Bank of Bahrain

RISK ASSESSMENT

GUIDANCE FOR FINANCIAL INSTITUTIONS

OCTOBER 2021

Contents

I. PURPOSE, SCOPE AND APPLICABILITY 3
II. INTRODUCTION 4
III. SCOPE OF RISK ASSESSMENT 7
IV. IDENTIFYING RISK 8
V. ASSESSING RISK 20
VI. EVALUATING RISK 22
VII. MITIGATING RISK 23
VIII. EVALUATING EFFECTIVENESS OF THE RISK ASSESSMENT 25

I. PURPOSE, SCOPE AND APPLICABILITY

- This guidance paper issued by the Central Bank of Bahrain ("CBB") should be read in conjunction with CBB regulations (specifically, the Financial Crime ("FC") Module requirements), international standards and best practices. The guidance included in this paper applies to all licensees regulated and supervised by the CBB.

- The FATF Recommendations were last updated in October 2020 to include the requirement of identifying and assessing the risks related to proliferation financing in addition to money laundering and terrorist financing. Therefore, this paper aims to provide guidance to assist financial institutions in implementing the requirements to identify, assess, understand, and mitigate their money laundering, terrorist financing and proliferation financing risks.

- This guidance paper was developed by consolidating relevant information applicable to financial institutions included in guidance papers issued by the Financial Action Task Force ("FATF"), including:

  - 'Guidance on Proliferation Financing Risk Assessment and Mitigation' issued in June 2021
  - 'Terrorist Financing Risk Assessment Guidance' issued in July 2019;
  - 'Guidance for a Risk-Based Approach – The Banking Sector' issued in October 2014; and
  - 'National Money Laundering and Terrorist Financing Risk Assessment' issued in February 2013.

- In summary, this paper outlines the methods of identifying types of money laundering, terrorist financing and proliferation financing risks and the means to assess, evaluate, and mitigate such risks using a risk-based approach. It discusses the application of a risk assessment and the necessity of reviewing and evaluating an FI's risk assessment effectiveness.

II. INTRODUCTION

Money Laundering ("ML") is the processing of proceeds of crime in order to disguise their illegal origin. This involves placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds, and integration of the funds into society in the form of holdings that appear legitimate. **Terrorist financing ("TF")** is the financing of terrorist acts, terrorists and terrorist organisations. It involves the risk that funds or other assets intended for a terrorist or terrorist organisation are being raised, moved, stored or used in or through a jurisdiction, in the form of legitimate or illegitimate funds or other assets. Though ML focuses primarily on concealing the source of funds, TF focuses more on masking the activity of funding in addition to the nature of the funded activity. **Proliferation Financing ("PF")** is the act of providing funds or financial services which are used in proliferation[1]. PF facilitates the movement and development of proliferation-sensitive items and can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction ("WMD") are developed and deployed.

In the context of this guidance paper, **ML and TF risk** can be defined as the effect of ML and TF-related uncertainty on a financial institution's objectives. Conversely, **PF risk** refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions ("TFS") obligations referred to in FATF's Recommendation 7 ("R7"). **These R.7 obligations apply to two country-specific regimes for the Democratic People's Republic of Korea (DPRK) and Iran**, which require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of (a) any person or entity designated by the United Nations ("UN"), (b) persons and entities acting on their behalf or at their direction, and (c) those owned or controlled by them.

The source of proliferation financing risks would depend upon a number of factors as follows:

- **Risk of a potential breach or non-implementation of targeted financial sanctions:** This risk may materialise when designated entities and individuals access financial services, and/or funds or other assets, as a result, for example, of delay in communication of designations at the national level, lack of clear obligations on private sector entities, failure on the part of private sector entities to adopt adequate policies and procedures to address their proliferation financing risks (e.g. weak customer on-boarding procedures and ongoing monitoring processes, lack of staff training, ineffective risk management procedures, lack of a proper sanctions screening system or irregular or inflexible screening procedures, and a general lack of compliance culture); and

[1] Proliferation is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-used goods used for non-legitimate purposes), in contravention of national laws or where applicable, international obligations.

- **Risk of evasion of targeted financial sanctions:** This risk may materialise due to concerted efforts of designated persons and entities to circumvent targeted financial sanctions (e.g., by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries).

Financial institutions should conduct ML, TF, and PF risk assessments. A **risk assessment** is a process based on a methodology that attempts to identify, analyse and understand ML, TF, and PF risks and serves as a first step in addressing them. Financial institutions should have processes in place to identify, assess, monitor, manage and mitigate money laundering, terrorist financing, and proliferation financing risks. FIs should take appropriate steps to identify and assess their money laundering, terrorist financing, and proliferation financing risks prior to commencing a new business, introducing new products or business practices or establishing customer relationships, and should continue assessing such risks on an ongoing basis and keep the assessments up-to-date.

A risk assessment is ideally a function of threats, vulnerabilities and consequences. A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. The concept of **vulnerabilities** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. **Consequence** refers to impacts and harms and can be further categorised into, for instance, physical, social, environmental, economic and structural.

A. Money Laundering/Terrorist Financing

- **ML/TF Threat:** ML/TF threat includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. Threat is one of the factors related to risk, and typically serves as an essential starting point in developing an understanding of ML/TF risk.

- **ML/TF Vulnerabilities:** these are the factors that represent weaknesses in AML/CFT systems or controls or certain features of an FI. They may also include the features of a particular sector, geography, a financial product or type of service that make them attractive for ML or TF purposes.

- **ML/TF Consequences:** ML/TF consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature, affecting populations, specific communities, the business environment, or national or international interests, the

reputation and attractiveness of a country's financial sector, as well as financial institutions' reputation, regulatory enforcements, negative media and financial repercussions.

B. Proliferation Financing

- **PF Threat:** PF threat refers to designated persons and entities that have previously caused or with the potential to evade, breach or exploit a failure to implement Proliferation Financing-Targeted Financial Sanctions ("PF-TFS") in the past, present or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities. It can be an actual or a potential threat.

- **PF Vulnerability:** PF vulnerability refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF-TFS. For financial institutions, vulnerabilities may include features of a particular jurisdiction, particular sector, a financial product or type of service that make them attractive for a person or entity engaged in the breach, non-implementation or evasion of PF-TFS, and weaknesses in the financial institution's counter-proliferating financing systems and controls.

- **PF Consequence:** PF consequence refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for proliferation financing. A breach, non-implementation or evasion of PF-TFS may also cause reputational damages to the FI and punitive measures such as sanction designations by the UN and/or relevant authorities. Ultimately, the consequence of proliferation financing is more severe than that of ML or other financial crimes, and is more similar to the potential loss of life associated with the consequences of TF.

III. SCOPE OF RISK ASSESSMENT

A. Money Laundering/Terrorist Financing

- When deciding on the scope of an ML/TF risk assessment, a key consideration is to determine whether ML and TF risks should be assessed separately or together. Factors associated with TF that might need to be considered may differ from those associated with ML. For example, funds used to finance terrorist activities may be derived from criminal activity or legal sources. In addition, a key focus in combating TF is on preventing future terrorist acts from occurring, whereas with combating ML, the criminal activity (the predicate offence) has already taken place. Another difference is that transactions associated with TF may be conducted in very small amounts, which could be the same transactions frequently considered to involve minimal ML risk when not viewed in the TF context.

B. Proliferation Financing

- Given the limited literature on typologies of the breach, non-implementation or evasion of PF-TFS, conducting a **contextual analysis**[2] as part of scoping may benefit FIs. FIs may focus their analysis on reviewing various recent methods, trends, and typologies of the breach, non-implementation or evasion of PF-TFS identified in the UNSC Panels of Experts ("PoE") on DPRK and Iran's reports, any existing available PF risk assessments prepared by various jurisdictions, other typologies common to TFS breaching, circumvention or evasion, and apply the information therein to the FI's business context. Financial institutions should also identify information and data gaps that they should address while going through the risk assessment process. A PF risk assessment may also include mapping the UNSCR PF-TFS[3] obligations applicable to financial institutions and their products or services.

[2] Contextual Analysis refers to analysing the environment in which an FI operates.

[3] The 2018 FATF Guidance on Counter Proliferation Financing provides a list of requirements of UNSCR TFS of proliferation financing.

IV. IDENTIFYING RISK

- In general terms, the process of identification in the context of an ML/TF/PF risk assessment starts by developing an initial list of potential risks or risk factors[4] financial institutions face when combating ML, TF, and PF. These will be drawn from the factors represented below. Ideally, the identification process should attempt to be comprehensive. However, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.

- Prior to conducting a risk assessment, an FI should understand the concepts of inherent and residual risks. An **inherent risk** refers to the natural level of risk prior to introducing any measures to mitigate or reduce the likelihood of an actor exploiting that risk – those measures are often referred to as controls or control measures. Understanding inherent risk is beneficial as it can facilitate the corresponding understanding and assessment of whether the control measures are effective, and in the case where no control measures are to be introduced, the impact of such risk to the FI. Conversely, a **residual risk** refers to the level of risk that remains after the risk mitigation process. An understanding of residual risk allows FIs to determine if they are effectively managing ML/TF/PF risks within their business operations. A high degree of residual risk may suggest that control measures are inadequate and that an FI should take remedial action to address that risk.

A. Identifying ML/TF Risks

- Crucially the factors associated with TF risk are also distinct from those associated with ML risk. While laundered funds come from the proceeds of illegal activities, funds used to finance terrorism may come from both legitimate and illegitimate sources. Similarly, for ML, it is often the case that the generation of funds may be an end in itself, with the purpose of laundering being to transmit the funds to a legitimate enterprise. In the case of TF, the end is to support acts of terrorism, terrorist individuals and organisations, and for that reason, the funds or other assets should, for the most part, ultimately be transferred to persons connected with terrorism.

- Although there may be some overlap in the potential vulnerabilities that criminals and terrorists misuse, the motive, and therefore the threat and risk indicators, differ. While transferring a low volume of funds may be a lower risk for ML, this type of activity may pose a higher risk indicator for TF when considered along with other factors (e.g. reporting thresholds or limited amount of funds necessary to carry out terrorist acts). For example,

[4] The term '*risk factors'* is used to refer to specific threats or vulnerabilities that are the causes, sources or drivers of ML, TF or PF risks.

terrorist financiers have been known to use low-limit prepaid cards for TF purposes despite being considered lower risk for ML.

- When identifying ML/TF risks for a risk assessment, FIs must should consider, individually or together with other risk categories, the following risks:

a) Country/Geographic Risk

- Country/geographic area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of higher risk include:

  - Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;
  - Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
  - Countries identified by credible sources as having significant levels of corruption or organised crime or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;
  - Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation; and
  - Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

b) Customer/Investor Risk

- Examples of high-risk customer categories include:

  - The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);
  - Non-resident customers;
  - Legal persons or arrangements that are personal asset-holding vehicles;
  - Companies that have nominee shareholders or shares in bearer form;
  - Cash-intensive businesses;
  - The ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

- The customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT regime and is not engaging in remediation to improve its compliance;
- Customer is a PEP or customer's family members, or close associates are PEPs (including where a beneficial owner of a customer is a PEP);
- Customer resides in or whose primary source of income originates from high-risk jurisdictions;
- Customer resides in countries considered to be uncooperative in providing beneficial ownership information;
- The customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or financial crimes;
- Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or competent national authorities;
- Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business;
- The number of STRs and their potential concentration on particular client groups;
- Customers who have sanction exposure; and
- The customer has a non-transparent ownership structure.

c) Product/Service/Transactions Risk

- An overall risk assessment should determine the potential risks presented by product, service, transaction, or the financial institution's delivery channel. An FI should assess, using an RBA, the extent to which the offering of its product, service, transaction or delivery channel presents potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

- Determining the risks of product, service, transaction, or the delivery channel offered to customers may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:

  - Private banking;
  - Anonymous transactions (which may include cash);
  - Non-face-to-face business relationships or transactions;
  - Payment received from unknown or unassociated third parties;
  - Products or services that may inherently favour anonymity or obscure information about underlying customer transactions;
  - The geographical reach of the product or service offered, such as those emanating from higher-risk jurisdictions;

- Products with unusual complexity or structure and with no obvious economic purpose;
- Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction; and
- Use of new technologies or payment methods not used in the normal course of business by the FI.

d) Distribution channel Risk

- A customer may request transactions that pose an inherently higher risk to the financial institution. Factors that may be considered as indicators of higher risk include:

  - A request is made to transfer funds to a higher risk jurisdiction/country/region without a reasonable business purpose provided; and
  - A transaction is requested to be executed, where the FI is made aware that the transaction will be cleared/settled through an unregulated entity.

- An overall risk assessment should include the risks associated with different types of delivery channels to facilitate the delivery of the financial institution's products and services. For example, an FI that distributes products or services directly through online delivery channels should identify and assess the ML/TF risks that may arise in relation to distributing its products using this business model.

- In addition to the analysis of risks performed in advance of engaging in a new business model, the risk assessment process should be performed when the FI develops new products and new business practices.

- A financial institution should also analyse the specific risk factors that arise from the use of **intermediaries** and their services. Intermediaries' involvement may vary with respect to the activity they undertake and their relationship with the FIs.

- A financial institution should understand who the intermediary is and perform a risk assessment on the intermediary prior to establishing a business relationship. FIs and intermediaries should clearly establish their respective responsibilities for compliance with the applicable regulation.

- An intermediary risk analysis should include the following factors, to the extent that these are relevant to the financial institution's business model:

- Intermediaries suspected of criminal activities, particularly financial crimes or association with criminal associates;
- Intermediaries located in a higher risk country or a country with a weak AML/CFT regime;
- Intermediaries serving high-risk customers without appropriate risk-mitigating measures;
- Intermediaries with a history of non-compliance with laws or regulations or that have been the subject of relevant negative attention from credible media or law enforcement;
- Intermediaries that have failed to attend or complete AML/CFT training programmes requested by the FI; and
- Intermediaries that have weak AML/CFT controls or operate substandard compliance programmes (i.e., programs that do not effectively manage compliance with internal policies and/or external regulation or the quality of whose compliance programmes cannot be confirmed).

B. Identifying Proliferation Financing Risks

- Identifying PF risks entails identifying the FI's PF threats and vulnerabilities. A good foundation of the identification process for **PF threats** is to begin by compiling a list of:

  - major known or suspected threats;
  - key sectors, products, or services that have been exploited;
  - types and activities that designated individuals/entities engaged in; and
  - the primary reasons why designated persons and entities are not identified or deprived of their assets.

- While the methodology of identifying PF threats could be similar to that of ML/TF, FIs should note that the nature of PF threats is significantly different from ML/TF threats. Unlike ML and TF threats, PF threats can be posed by persons and entities designated pursuant to relevant UNSCRs (i.e. DPRK and Iran) and the international networks they have created to disguise their activities. As a result, designated persons and entities' financing needs and methods may not necessarily be the same as those of money launderers and terrorists.

- In the context of a potential breach, non-implementation or evasion of PF-TFS, FIs should note that the financing can be sourced from both legitimate and illegitimate activities for raising funds or for obtaining foreign exchange and may not necessarily involve laundering of proceeds. Frequently, designated persons and entities use front and shell companies to conduct such businesses. Doing so is a deliberate strategy to obscure the fact that economic resources, assets, and funds are ultimately made available to designated persons or entities.

- Financial institutions are encouraged to take a holistic approach when gathering information related to proliferation financing threats. Potential information sources may include actual or known typologies, summaries of case types, schemes, or circumstances involved in the breach, non-implementation or evasion of PF-TFS.

- Other relevant information sources for PF risk assessments include firm and group-wide databases containing customer due diligence ("CDD") information collected during the onboarding and ongoing due diligence (particularly the beneficial ownership of legal persons and arrangements), and transaction records involving the sale of dual-use goods or goods subject to export control. Internal control rules designed to identify designated persons and entities and those acting on their behalf or at their direction may also be relevant for compliance with PF-TFS.

- After formulating a list of PF threats, the next step is to compile a list of major **PF vulnerabilities**. FIs are encouraged to consider adapting their methodology used for identifying ML/TF vulnerabilities for PF purposes. Similar to ML/TF, these vulnerabilities could be based on a number of factors, such as structural, sectoral, product or service, customers and transactions.

- PF risk assessment considerations may also include the nature, scale, diversity, and geographical footprint of the FI's business, target market(s) and customer profiles, and the volume and size of transactions handled by a financial institution.

- FIs may consider contextual features of a particular sector that potentially make it attractive for designated persons and entities to exploit for the purpose of PF sanction evasion. A low level of PF risk awareness, understanding of TFS requirements, and an overall weak culture of compliance within a sector all constitute vulnerabilities for misuse. Considerations may also include the relative complexity and reach of funds movement of each sector and sub-sector.

- FIs may consider the vulnerabilities associated with their products, services, customers and transactions. The vulnerabilities refer to weaknesses and features, which could be exploited for sanctions evasion purposes. Product- or service-specific vulnerabilities may include whether a product or service provided by the financial institution is complex in nature, has a cross-border reach (e.g. via the distribution channels), is easily accessible to customers, attracts a diverse customer base, or is offered by multiple subsidiaries or branches.

- Identifying customer and transaction vulnerabilities is crucial for risk assessments conducted by a financial institution. As a starting point, they may consider to review the number of customers already identified as high risk, especially those often carrying out cross-border transactions involving legal persons and arrangements or multiple shell or front companies.

Information on the type and identity of the customer, as well as the nature, origin and purpose of the customer relationship, is also relevant. Other considerations include: the number, amount (especially in cash), and frequency of transactions:

- originating from, transiting through, or designating for an overseas jurisdiction that has a weak implementation of relevant UNSCR obligations and FATF Standards, weak governance, law enforcement and regulatory regimes;
- involving individuals acting on behalf of a legal person or arrangement (e.g. authorised signatory, director); and
- transactions that are unrelated to a financial institution's stated business profile.

- A financial institution would particularly benefit from PF vulnerabilities-related information obtained from customer onboarding and ongoing CDD processes, and transaction monitoring and screening, as well as internal audit and regulatory findings. Other information obtained through public-private information sharing initiatives on the weaknesses observed by both parties may also provide insights into vulnerabilities.

C. Indicators of Proliferation Financing

- A risk indicator demonstrates or suggests the likelihood of the occurrence of unusual or suspicious activity. The existence of a single standalone indicator in relation to a customer or transaction may not alone warrant suspicion of proliferation financing, nor will a single indicator necessarily provide a clear indication of such activity. However, it could prompt further monitoring and examination, as appropriate. Similarly, the occurrence of several indicators (especially from multiple categories) could also warrant closer examination. Generally, whether one or more of the indicators suggests proliferation finance depends on the business lines, products or services that an institution offers, how it interacts with its customers, and the institution's human and technological resources.

a) Customer Profile Risk Indicators:

- During onboarding, a customer provides vague or incomplete information about their proposed trading activities. The customer is reluctant to provide additional information about their activities when queried;

- During subsequent stages of due diligence, a customer, particularly a trading entity, its owners or senior managers, appear in sanctioned lists or negative news (e.g. past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes);

- The customer is a person connected with a country of proliferation or diversion concern (e.g. through business or trade relations – this information may be obtained from the national risk assessments or directives and circulars from relevant authorities);

- The customer is a person dealing with dual-use goods or goods subject to export control, goods or complex equipment for which he/she lacks technical background or which is incongruent with their stated line of activity;

- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding;

- A customer or counterparty declared to be a commercial business conducts transactions that suggest that they are acting as a money-remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the activity associated with originators appear to be entities who may be connected to a state-sponsored proliferation programme (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls; and

- A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control.

b) Account and Transaction Activity Risk Indicators:

- The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern (i.e. DPRK and Iran);

- Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes;

- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies (e.g. companies do not have a high level of capitalisation or display other shell company indicators). FIs may identify more indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity;

- Demonstrating links between representatives of companies exchanging goods (i.e. same owners or management, same physical address, IP address or telephone number, or their activities may be co-ordinated);

- Account holder conducts financial transactions in a circuitous manner;

- Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services);

- Manufacturing or trading firm customer wants to use cash in transactions for industrial items or trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals;

- Transactions are made on the basis of "ledger" arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance these accounts; and

- A customer uses a personal account to purchase industrial items under export control or otherwise not associated with corporate activities or congruent lines of business.

c) International Trade Risk Indicators:

– **Maritime Sector**[5]:

- A trading entity is registered at an address that is likely to be a mass registration address (e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit);

- A freight forwarding firm is listed as the product's final destination;

- The destination of a shipment is different from the importer's location;

[5] DPRK PF-TFS, i.e. UNSCR 2270 (2016) OP 23, has designated the DPRK firm Ocean Maritime Management and vessels as economic resources controlled or operated by OMM and therefore subject to the asset freeze imposed in OP 8(d) of UNSCR 1718 (2006). UNSCR 2270 (2016) OP 12 also affirms that "economic resources" as referred to in OP 8(d) of UNSCR 2270 (2016), includes assets of every kind, which may potentially be used to obtain funds, goods, or services, such as vessels (including maritime vessels).

- Inconsistencies are identified across contracts, invoices, or other trade documents (e.g. contradictions between the name of the exporting entity and the name of the recipient of the payment, differing prices on invoices and underlying contracts, or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions);

- Shipment of goods have a low declared value vis-à-vis the shipping cost;

- Shipment of goods incompatible with the technical level of the country to which it is being shipped, e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry;

- Shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet;

- Shipment of goods is inconsistent with normal geographic trade patterns (e.g. the destination country does not normally export or import the goods listed in trade transaction documents);

- Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement of export control laws; and

- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons (e.g. by a shell or front company not involved in the trade transaction).

  – **Trade Finance[6]:**

- Prior to account approval, the customer requests a letter of credit for trade transaction for shipment of dual-use goods or goods subject to export control;

- Lack of full information or inconsistencies are identified in trade documents and financial flows, such as names, companies, addresses, final destination, etc.; and

[6] DPRK PF-TFS, i.e. UNSCR 2087 (2013) OP 5(a), UNSCR 2094 (2013) OP 8, UNSCR 2270 (2016) OP 10, UNSCR 2321 (2016) OP3, UNSCR 2371 (2017) OP 18, UNSCR 2375 (2017) OP 3, specifies that the listed individuals and entities are subject to the asset freeze imposed in OP 8(d) of UNSCR 1718 (2006). These designated entities include trading companies.

- Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

D. Examples of Services/Products that are Highly Vulnerable to PF Risk

- In order to identify PF vulnerabilities, FIs should pay closer attention to services and products that are more likely to be vulnerable to the potential breach, non-implementation, or evasion of PF-TFS. Examples of such products and/or services include, but are not limited to, the following[7]:

a) Correspondent Banking Services:

- FATF papers indicate that cases have been identified where financial institutions can face challenges screening transactions that go through foreign respondents as designated persons and entities tend to create layered corporate entities and shell companies to gain access to the international financial system. Financial institutions should understand the risk profile of their foreign respondents and determine appropriate measures to mitigate the risks.

b) Trade Finance:

- Trade finance is another example of a service exploited by designated persons and entities. This is due to the fact that PF sanctions evasion often involves cross-border trade of goods or commodities. Designated persons and entities rely on trade finance instruments fraudulently, using forged documents, misrepresenting the parties to a transaction, or arranging for a different end-destination or end-user from the one listed in the paperwork.

c) Virtual Assets

- FATF papers indicate that as the access to the formal financial system has become increasingly closed to designated persons and entities due to the introduction of various financial sanctions, they have used virtual assets ("VAs") as another means to evade sanctions. This novel method and technology to access financial services are particularly attractive to individuals, entities, and counterparties designated under DPRK-related PF-TFS, who have met increasing obstacles in accessing banking services due to the sanctions measures included in successive UNSCRs.

[7] Examples are derived from the FATF's guidance paper on Proliferation Financing Risk Assessment and Mitigation issued in June 2021

- Some of the activities identified include, amongst others, the theft of VAs (through attacks on both exchanges and users) and the mining of cryptocurrencies through crypto-jacking (i.e. the introduction of malware to computers to turn those systems into cryptocurrency miners for the benefit of DPRK hackers), as well as through the use of its own computer networks to generate funds). A digital version of layering was used to disguise these activities, which created thousands of transactions in real-time through one-time use VA wallets.

V. ASSESSING RISK

- Analysis of relevant information and data lies at the heart of the risk assessment process. Therefore, financial institutions should analyse the identified risks to understand their nature, sources, likelihood, and consequences to assign some relative value or importance to each of the risks and identify the overall risk level.

- When weighing and categorising risk factors, financial institutions should differentiate the level of risk presented by diverse types of the identified risks, which will, in turn, assist with prioritising mitigation. This stage involves a consideration of the potential likelihood and consequences of the materialisation of specific ML/TF/PF risks.

- In terms of **ML/TF risks**, financial institutions should assess the potential likelihood and consequences of specific ML/TF risks occurring by considering the prevalence of known cases, typologies, capabilities and intent of money launderers/terrorist organisations/individuals and supporters, and strength of AML/CFT controls.

- Likelihood and consequence may be assessed or scored using descriptive words or number scales. The important issue is to use these concepts to differentiate the level of risk presented by diverse types of ML/TF, and thus, assist with prioritising mitigation.

- When analysing the likelihood and consequences of **PF risks**, considerations could include the prevalence of known cases, typologies, strengths of counter-proliferation financing ("CPF") controls, and capabilities and intent of designated persons and entities. The starting point is to assume that the consequences of the potential breach, non-implementation or evasion of PF-TFS (including the potential development of WMD) would be severe. It is also important to note that not all PF methods have equal consequences and that consequences may differ depending on the source, channel, or intended recipients of the funds or assets.

- Below is an example of a simple risk rating matrix as applied to a specific risk. FIs' risk rating matrix will likely vary depending on their nature, size, type and complexity.

Example 1: General Risk Rating Matrix

Likelihood	***Impact***	***Rating***
Very Likely	Significant Impact	**Significant**
Likely	Major Impact	**High**
Moderately Likely	Moderate Impact	**Medium**
Unlikely	Minor Impact	**Low**

- A particular challenge, however, is that ML/TF/PF risks are inherently difficult to describe or measure in quantifiable or numerical terms. It is therefore important to remember that risk is a combination of threats, vulnerabilities, along with consequences. If the level of individual risks can be examined according to their consequences or impact and the likelihood of their materialising, then a rough estimate of risk level may be obtained.

- As a result of risk analysis, the level of risks is often classified in one of these categories: low, medium, or high, with possible combinations between different categories (e.g. medium-high, medium-low). The same risk may be regarded as high in one FI, while in another FI, it may be viewed as low, depending on the overall context and circumstances. This classification aims to assist in the understanding and prioritisation of ML/TF/PF risks.

VI. EVALUATING RISK

- The last stage of risk assessment is evaluation. It involves taking the results found during the analysis process to determine priorities for addressing the risks, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to the development of a strategy for their mitigation or, in some instances, risk avoidance, for example, by not pursuing a particular product, service, business etc.

- Depending on the source, there are a number of methods for addressing (or "controlling") risk. The most relevant of these methods are prevention (e.g., prohibiting certain products, services, or activities) and risk mitigation (or reduction). Therefore, evaluating levels of ML/TF/PF risk normally leads to the development of a strategy for addressing the risks.

- Financial institutions should consider adapting/calibrating/enhancing their policies, controls, and procedures to manage and mitigate the identified risks effectively. For **PF-related risks**, financial institutions may also review and refer to suspected activity of the breach, non-implementation or evasion of PF-TFS to inform their findings of any risk assessment.

- Financial institutions should allocate appropriate and proportionate resources and provide training to relevant staff members on the implementation of AML/CFT/CPF measures based on the risk assessment findings.

- The risk evaluation process typically results in courses of action commensurate with the level of risk identified.

VII. MITIGATING RISK

A. Risk Mitigation Measures by Financial Institutions

- Financial institutions should implement necessary measures and allocate appropriate resources to mitigate the risks which they have identified. The risk-based approach allows FIs to develop a more flexible set of measures in order to target their resources more effectively, including the application of preventive measures.

- FIs should take steps to identify circumstances in which customers and transactions may present money laundering, terrorist financing and proliferation financing risks, and ensure that their sanctions policies, controls and procedures address these risks, in accordance with CBB's regulations and applicable international standards. FIs should develop a clear understanding of the contextual information and the sources of ML/TF/PF risks that they are exposed to, and take appropriate measures to mitigate them. The nature of risk mitigation measures will depend on the source and degree of risks and could include:

  - Improved on-boarding processes for customers (including beneficial owners);
  - Enhanced customer due diligence procedures;
  - Effective maintenance of customer master data;
  - Regular controls to ensure effectiveness of procedures for sanctions screening; and
  - Leveraging the existing compliance programmes (including internal controls) to identify potential sanctions evasion.

- A sanctions breach and failure to implement sanctions may typically result from inadequate internal controls (e.g. inadequate CDD and record keeping, delays in screening customers, inadequate transaction monitoring and screening systems and procedures, use of out-of-date sanctions lists and lack of accuracy in matching names). Mitigating these risks essentially requires building sound processes and internal controls, and ensuring these are followed.

- Training of staff, in particular for those responsible for on-boarding customers and maintaining customer relationships, monitoring and screening transactions and handling risk assessments is fundamental in a strong compliance regime. As appropriate, staff should be aware of proliferation financing risks, typologies in relation to the breach, non-implementation or evasion of targeted financial sanctions, and the required risk mitigation measures. These training programmes can be rolled into the existing sanctions training or wider AML/CFT training modules.

- Mitigating sanctions evasion risks aims at reducing the risks as much as reasonable by following an approach proportionate to risks. Sanctions evasion schemes aim to hide the designated persons and entities. As the very objective of these schemes is to circumvent sanctions, financial institutions could be in situations where despite a good understanding of risks, a robust compliance function and sound due diligence, they might not be able to detect all potential evasion of targeted financial sanctions. However, this gives rise to financial, legal and reputational risks for these institutions. The risks increase when a financial institution does not understand the risks of potential sanctions evasion schemes and how to implement tailored, risk-based measures to mitigate those risks.

- Financial institutions exposed to higher risks may proactively incorporate a wide range of information for their compliance policies and procedures, which may include guidance provided by relevant authorities, risk indicators, typologies and reports of Panel of Experts of the relevant UNSCRs, into their risk management practices and procedures. These practices and procedures should be tailored to the risk profile of these institutions and periodically reviewed to ensure they remain relevant and up-to-date with current trends.

- Investment in technology and advanced software, capable of machine learning and artificial intelligence to conduct analysis may help strengthen the compliance practices of large and complex financial institutions that could be exposed to higher levels of risks. This would enable them to identify linkages and relationships, and build reliable scenarios and recognise patterns (e.g. transaction times, value, purpose, counterparties, geolocation), which would be difficult to establish otherwise. As designated entities and individuals are increasingly using advanced deception techniques, including wire/payments stripping techniques[8] to hide their true identities and conceal the beneficial owners, financial institutions should be vigilant to such risks and deploy appropriate tools to address such risks.

[8] Stripping is the deliberate act of changing or removing information from a payment or instruction, to obscure the identity of the payment originator/beneficiary or to connect them to designated individuals or entities.

VIII. EVALUATING EFFECTIVENESS OF THE RISK ASSESSMENT

- Financial institutions should update their risk assessments regularly, using appropriate tools, methodology and approach, taking into account risks that are inherent in their activities as well as any new risks that may arise, changes to the FI's risk appetite, existing business operations or requirements from relevant authorities. These updated assessments are likely to become more refined over time.

- FIs should therefore stay up-to-date on methods, trends, and typologies of ML/TF/PF and relevant local and international standards and advancements in relation to AML/CFT/CPF. FIs should also aim to identify any future needs pertinent to its business operations' nature, size, and complexity.