TABLE OF CONTENTS

1. Introduction, Purpose and Scope

i. Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. An effective Anti-Money Laundering and Countering the Financing of Terrorism("AML/CFT") regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF.

ii. Securities and Exchange Commission of Pakistan ("SECP"), in order to maintain the integrity of its regulated financial sector inter-alia; the brokers, insurers, NBFCs and Modaraba' in respect of preventing and combating ML and TF, notified the Securities and Exchange Commission of Pakistan' Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 ("the SECP AML/CFT Regulations" or "the Regulations"). The SECP AML/CFT Regulations require relevant Regulated Persons (RPs) to establish systems to detect ML and TF, and therefore assist in the prevention of abuse of their financial products and services.

iii. This policy is based on the guidelines which are applicable to all Regulated Persons ("RPs") including brokers as defined under the SECP AML/CFT Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. It supplements the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities.

iv. This policy is prepared under the guidelines are based on Pakistan' AML/CFT legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

2. Obligation of TSL as RP in Establishing an Effective AML/CFT Governance and Compliance Regime

i. TSL as RP shall understand its obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

ii. TSL's Board of Directors and senior management must be engaged in the decision making on AML/CFT policies, procedures and control and take ownership of the risk based approach. They must be aware of the level of ML/TF risk the TSL is exposed to and take a view on whether it is equipped to mitigate that risk effectively.

iii. TSL as RP must give due priority to establishing and maintaining an effective AML/CFT compliance culture and must adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with

the Regulations.

iv. TSL as RP must establish written internal procedures so that, in the event of a suspicious activity being discovered, employees are aware of the reporting chain and the procedures to be followed. Such procedures should be periodically updated to reflect any legislative changes.

v. To oversee the compliance function, the Regulations require TSL as RP to appoint a Compliance Officer ("CO") at the management level, who shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

vi. TSL shall ensure that any suspicious transaction report must be made by employees to the Compliance Officer, who is well versed in the different types of transactions which TSL handles and which may give rise to opportunities for ML/TF.

vii. TSL is responsible for ensuring that employees shall be aware of their reporting obligations and the procedure to follow when making a suspicious transaction report.

3. Program and Systems to prevent ML and TF

i. TSL shall establish and maintain programs and systems to prevent, detect and report ML/TF. The systems should be appropriate to the size of TSL and the ML/TF risks to which it is exposed and should include:

a) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
b) Policies and procedures to undertake a Risk Based Approach ("RBA");
c) Internal policies, procedures and controls to combat ML/TF, including appropriate risk management arrangements;
d) Customer due diligence measures;
e) Record keeping procedures;
f) Group-wide AML/CFT programs;
g) An audit function to test the AML/CFT system;
h) Screening procedures to ensure high standards when hiring employees; and
i) An appropriate employee-training program.

ii. It is the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF and TSL is in compliance with the applicable legislative and regulatory obligations.

4. The Three Lines of Defense

i. TSL shall establish the following three lines of defense to combat ML/TF;

- First the business units (e.g. front office, customer-facing activity): They should know and carry out the AML/CFT due diligence related policies and procedures and be allotted sufficient resources to do this effectively.
- Second the Compliance Officer, the compliance function and human resources or technology.
- Third the internal audit functions.

ii. As part of first line of defense, policies and procedures shall be clearly specified in writing, and communicated to all employees. TSL shall contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the reporting entity in compliance with the Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

iii. As part of second line of defense, the Compliance Officer must have the authority and ability to oversee the effectiveness of TSL's AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT policies and procedures.

iv. Compliance Officer must be a person who is fit and proper to assume the role and who:

1) Has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
2) reports directly and periodically to the Board of Directors ("Board") or equivalent on AML/CFT systems and controls;
3) has sufficient resources, including time and support staff;
4) has access to all information necessary to perform the AML/CFT compliance function;
5) ensures regular audits of the AML/CFT program;
6) maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"),and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
7) responds promptly to requests for information by the SECP/Law enforcement agency.

v. Internal audit, the third line of defense, shall periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT measures.

Monitoring AML/CFT Systems and Controls

5. Monitoring AML/CFT Systems and Controls

i. TSL shall have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. TSL shall update its systems as appropriate to suit the change in risks.

ii. Additionally, TSL shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, TSL shall need to consider monitoring certain aspects which include:

1) The ability to identify changes in a customer profile or transaction activity/behavior, which come to light in the normal course of business;
2) The potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback,

etc.;

3) The adequacy of employee training and awareness;
4) The adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
5) The compliance arrangements (such as internal audit);
6) The performance of third parties who were relied on for CDD purposes;
7) Changes in relevant laws or regulatory requirements; and
8) Changes in the risk profile of countries to which TSL or its customers are exposed.

6. Documentation and Reporting

i. TSL shall document its RBA. Documentation of relevant policies, procedures, review results and responses shall enable TSL to demonstrate to the Commission:

1) Risk assessment systems including how TSL assesses ML/TF risks;
2) Details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
3) How it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
4) The arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

ii. TSL shall note that the ML/TF risk assessment is not a one-time exercise and therefore, it shall ensure that ML/TF risk management processes are kept under regular review, done at least annually. Further, TSL's management should review the program's adequacy when the reporting entity adds new products or services, opens or closes accounts with high-risk customers, or expands through mergers or acquisitions.

iii. TSL shall be able to demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, during the SECP's on-site inspection. TSL shall maintain Control Assessment Template (Annex 2) within the period as required by the Commission from time to time.

7. New Products and Technologies

i. TSL shall have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

1) Electronic verification of documentation;
2) Data and transaction screening systems. or
3) The use of virtual or digital currencies.

ii. TSL shall undertake a risk assessment prior to the launch or use of such products, practices and technologies, and take appropriate measures to manage and mitigate the risks.

iii. TSL shall have policies and procedures to prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favor anonymity. For example, securities trading and investment business on the Internet add a new dimension to TSL' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud. It is not appropriate that TSL shall offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied.

iv. To maintain adequate systems, TSL shall ensure that its systems and procedures are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by TSL. Risks identified shall be fed into TSL's business risk assessment.

8. Cross-border Correspondent Relationship

i. Cross-border correspondent relationships are the provision of services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require EDD.

ii In order for TSL to manage its risks effectively, it shall consider entering into a written agreement with the respondent institution before entering into the correspondent relationship.

iii. In addition to setting out the responsibilities of each institution, the agreement could include details on how the TSL will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls.

iv. Correspondent Institutions are encouraged to maintain an ongoing and open dialogue with the respondent institutions to discuss the emerging risks, strengthening AML/CFT controls, and help the respondent institutions in understanding the correspondent institutions' AML/CFT policies and expectations of the correspondent relationship.

9. Customer Due Diligence

i. TSL shall take steps to know who its customers are. TSL shall not keep anonymous accounts or accounts under fictitious names. TSL shall take steps to ensure that its customers are who they purport themselves to be. TSL shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

ii.TSL shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the TSL's knowledge of the customer, its business and risk profile (Annex 3), including, where necessary, the source of funds. TSL shall conduct CDD when establishing a business relationship if:

(1)There is a suspicion of ML/TF, Annex 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help TSL recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.; or

(2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information

iii. In case of suspicion of ML/TF, TSL shall:

(1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and
(2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

iv. TSL shall monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

v. TSL shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, TSL shall identify and verify the customer's beneficial owner(s) to ensure that TSL understands who the ultimate beneficial owner is.

vi. TSL shall ensure that it understand the purpose and intended nature of the proposed business relationship or transaction. TSL shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

vii.The Regulations require TSL to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person").TSL shall also verify whether that authorized person is properly authorized to act on behalf of the customer. TSL shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, TSL shall ascertain the reason for such authorization and obtain a copy of the authorization document.

viii. TSL may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, it could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

ix. When performing CDD measures in relation to customers that are legal persons or legal arrangements, TSL shall identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

x. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business

relationship; and second, to take appropriate steps to mitigate the risks. In this context, TSL shall identify the customer and verify its identity. The type of information that would normally be needed to perform this function should be as specified in Annexure 1 of the Regulation.

xi. If TSL has any reason to believe that an applicant has been refused facilities by another RP due to concerns over illicit activities of the customer, it shall consider classifying that applicant as higher-risk and apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

a) Timing of Verification

i. The best time to undertake verification is prior to entering into a business relationship or conducting a transaction. However, as provided in the Regulations TSL may complete verification after the establishment of the business relationship.

ii. Examples of the types of circumstances (in addition to those referred for beneficiaries of life insurance or Takaful policies) where it would be permissible for verification to be completed after the establishment of a business relationship, because it would be essential not to interrupt the normal conduct of business, include:

(1) Non face-to-face business.

(2) Securities transactions: in the securities industry intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

(3) In cases of telephone or electronic business where payment is or is expected to be made from a bank or other account, the person verifying identity should:

(a) satisfy himself/herself that such account is held in the name of the customer at or before the time of payment; and

(b) not remit the proceeds of any transaction to the customer or his/her order until verification of identity has been completed.

iii. The above are only examples and TSL shall adopt risk management procedures with respect to the conditions under which an applicant may utilize the business relationship prior to verification. Such conditions may include restricting the funds received from being passed to third parties, imposing a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. For the avoidance of doubt, TSL shall not postpone the verification where the ML/TF risks are high and enhanced due diligence measures are required to be performed. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an applicant does not pursue an application, TSL's staff could consider that this in itself is suspicious, and TSL shall evaluate whether a STR to FMU is required.

iv. Where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/TF, TSL shall not voluntarily agree to open accounts with such customers. In such situations, TSL shall file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

b) Existing Customers

i. TSL is required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on extant relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

ii. The CDD requirements entail that, if TSL has any suspicion of ML/TF or becomes aware at anytime that it lacks sufficient information about an existing customer, it shall take steps to ensure that all relevant information is obtained as quickly as possible.

iii. TSL is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

iv. Where TSL is unable to complete and comply with CDD requirements as specified in the Regulations, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, then TSL shall terminate the relationship. Additionally, TSL shall consider making a STR to the FMU.

c) Tipping-off & Reporting

i. The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when the TSL is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

ii. Therefore, if TSL forms a suspicion of ML/TF while conducting CDD or ongoing CDD, it should take into account the risk of tipping-off when performing the CDD process. If TSL reasonably believes that performing the CDD or some other on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. TSL shall ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

d) No Simplified Due Diligence for Higher-Risk Scenarios

TSL shall not adopt simplified due diligence measures where the ML/TF risks are high. TSL shall identify risks and have regard to the risk analysis in determining the level of due diligence.

10. <u>On-going Monitoring of Business Relationships</u>

i. Once the identification procedures have been completed and the business relationship is established, TSL is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. TSL shall conduct ongoing monitoring of their business relationship with their

customers. Ongoing monitoring helps TSL to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. TSL shall conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer:

iii. TSL shall develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the "identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records.

iv. TSL shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by TSL based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever occurs first. Examples of triggering events include:

(1) Material changes to the customer risk profile or changes to the way that the account usually operates;
(2) Where it comes to the attention of TSL that it lacks sufficient or significant information on that particular customer;
(3) Where a significant transaction takes place;
(4) Where there is a significant change in customer documentation standards;
(5) Significant changes in the business relationship.

v. Examples of the above circumstances include:

(1) New products or services being introduced,
(2) A significant increase in a customer's salary being deposited,
(3) The stated turnover or activity of a corporate customer increases,
(4) A person has just been designated as a PEP,
(5) The nature, volume or size of transactions changes.

vi. TSL shall be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

(1) transaction type
(2) frequency
(3) amount
(4) geographic origin/destination
(5) account signatories.

vii. However, if TSL has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it shall take steps to ensure that all relevant information is obtained as quickly as possible

viii. It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism.

ix. Whilst TSL may wish to invest in expert computer systems specifically designed to assist to assist the detection of fraud and ML/TF, it is recognized that this may not be a practical option for the reasons of cost, the nature of its business, or difficulties of systems integration. In such circumstances TSL shall ensure to have alternative systems in place for conducting on-going monitoring.

11. Simplified Due Diligence Measures ("SDD")

i. TSL may conduct SDD in case of lower risks identified by TSL. However, TSL shall ensure that the low risks it identifies are commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD, TSL shall pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity. The simplified measures shall be commensurate with the low risk factors.

ii. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

iii. Where the risks are low and where there is no suspicion of ML/TF, the law allows TSL to rely on third parties for verifying the identity of the applicants and beneficial owners.

iv. Where TSL decides to take SDD measures on an applicant/customer, it shall document the full rationale behind such decision and make available that documentation to the Commission on request.

12. <u>Enhanced CDD Measures ("EDD")</u>

i. TSL shall examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose.

ii. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, TSL shall conduct enhanced CDD measures, consistent with the risks identified. In particular, TSL shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

iii. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).

(2) Updating more regularly the identification data of applicant/customer and beneficial owner.

(3) Obtaining additional information on the intended nature of the business relationship.

(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

(5) Obtaining additional information on the reasons for intended or performed transactions.

(6) Obtaining the approval of senior management to commence or continue the business relationship.

(7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

iv. In case of accounts where the accountholder has instructed TSL not to issue any correspondence to the accountholder's address; such accounts do carry additional risk to TSL and they should exercise due caution as a result. It is recommended on a best practice basis that evidence of identity of the accountholder shall be obtained by TSL. "Hold Mail" accounts shall be regularly monitored and reviewed and TSL shall take necessary steps to obtain the identity of the account holder where such evidence is not already in TSL

file.

a) High-Risk Countries

i. Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to TSL. Conducting a business relationship with an applicant/customer from such a country exposes the TSL to reputational and legal risk.

ii. TSL shall exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

iii. Caution shall also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

iv. TSL shall consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, TSL is encouraged to consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

v. Useful websites include: FATF website at www.fatf-gafi.organd Transparency international, www.transparency.org for information on countries vulnerable to corruption.

13. Politically Exposed Persons (PEPs)

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose TSL to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons, commonly referred to as 'politically exposed persons' (PEPs) and defined in the Regulations, inter-alia, heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

ii. Family members of PEP are individuals who are related to PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

iii. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

iv. Provision of financial services to corrupt PEPs exposes TSL to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of the whole financial system can be undermined.

v. TSL is encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. TSL shall in relation to PEPs, in addition to performing normal due diligence measures:

(1) have appropriate risk management systems to determine whether the customer is a politically exposed person;
(2) obtain senior management approval for establishing business relationships with such customers;

(3) take reasonable measures to establish the source of wealth and source of funds; and
(4) conduct enhanced ongoing monitoring of the business relationship.

vi. TSLs shall obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

vii. TSL shall take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of PEP,TSL shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country;
(2) Has prominent public functions in sectors known to be exposed to corruption;
(3) Has business interests that can cause conflict of interests (with the position held).

viii. The other red flags that the TSL shall consider include (in addition to the above and the red flags that they consider for other applicants):

(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
(3) A PEP uses multiple bank accounts for no apparent commercial or other reason;
(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

ix. TSL shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

(1) the level of (informal) influence that the individual could still exercise; and

(2) whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

14. Record-Keeping Procedures

i. TSL shall ensure that all information obtained in the context of CDD is recorded.This includes both;

a. recording the documents TSL is provided with when verifying the identity of the customer or the beneficial owner, and
b. transcription into TSL's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

ii. TSL shall maintain, for at least 5 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

iii. Where there has been a report of a suspicious activity or TSL is aware of a continuing investigation or litigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer shall be retained until confirmation is received that the matter has been concluded.

iv. TSL shall also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

v. Beneficial ownership information must be maintained for at least 5 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the TSL.

vi. Records relating to verification of identity will generally comprise:

1) a description of the nature of all the evidence received relating to the identity of the verification subject; and
2) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

vii. Records relating to transactions will generally comprise:

1) details of personal identity, including the names and addresses, of:

a) the customer;
b) the beneficial owner of the account or product; and
c) any counter-party.

2). details of securities and investments transacted including:

a. the nature of such securities/investments;
b. valuation(s) and price(s);
c. contract/memoranda of purchase and sale;
d. source(s) and volume of funds and securities;
e. destination(s) of funds and securities;
f. memoranda of instruction(s) and authority(ies);
g. book entries;
h. custody of title documentation;
i. the nature of the transaction;
j. the date of the transaction;
k. the form (e.g. cash, cheque) in which funds are offered and paid out.

15. Internal Controls (Audit Function, outsourcing, employee Screening and Training)

i. TSL shall have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks identified. TSL shall establish and maintain internal controls in relation to:

(1) an audit function to test the AML/CFT systems, policies and procedures;
(2) outsourcing arrangements;
(3) employee screening procedures to ensure high standards when hiring employees; and
(4) an appropriate employee training program.

ii. The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of TSL.

a) Audit Function

i. TSL shall, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit shall be commensurate with TSL's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits shall be conducted to assess the AML/CFT systems which include:

(1) test the overall integrity and effectiveness of the AML/CFT systems and controls;

(2) assess the adequacy of internal policies and procedures in addressing identified risks, including;
(a) CDD measures;
(b) Record keeping and retention;
(c) Third party reliance; and
(d) Transaction monitoring;

(3) assess compliance with the relevant laws and regulations;
(4) test transactions in all areas of TSL, with emphasis on high-risk areas, products and services;
(5) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(6) assess the adequacy, accuracy and completeness of training programs;
(7) assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
(8) assess the adequacy of TSL's process of identifying suspicious activity including screening sanctions lists.

b) Outsourcing

i. TSL shall maintain policies and procedures in relation to outsourcing where it intends to outsource some of its functions.TSL shall conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.

ii. Where TSL decides to enter into an outsourcing arrangement, TSL shall ensure that the outsourcing agreement clearly sets out the obligations of both parties. TSL entering into an outsourcing arrangement shall develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed.

iii. The OSP should report regularly to TSL within the timeframes as agreed upon with TSL. The TSL shall have access to all the information or documents relevant to the outsourced activity maintained by the OSP. TSL must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

iv. TSL shall ensure that the outsourcing agreement requires OSPs to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

c) Employee Screening

i. TSL shall maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening shall be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions.

ii. Employee screening shall be conducted at the time of recruitment, periodically thereafter, i.e.at least annually and where a suspicion has arisen as to the conduct of the employee.

iii. TSL shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, TSL may:

(1) Verify the references provided by the prospective employee at the time of recruitment
(2) Verify the employee's employment history, professional membership and qualifications
(3) Verify details of any regulatory actions or actions taken by a professional body
(4) Verify details of any criminal convictions; and
(5) Verify whether the employee has any connections with the sanctioned countries or parties.

d) Employee Training

i. TSL shall ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

ii. Training to staff shall be provided at least annually or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to TSL's business operations or customer base.

iii. TSL shall provide their staff training in the recognition and treatment of suspicious activities. Training shall also be provided on the results of TSL's risk assessments. Training shall be structured to ensure compliance with all of the requirements of the applicable legislation.

iv. Staff should be aware on the AML/CFT legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.

v. All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.

vi. TSL shall consider obtaining an undertaking from its staff members (both new and existing)

confirming that they have attended the training on AML/CFT matters, read the TSL's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

vii. Staff members who deal with the public such as sales persons are the first point of contact with contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training shall be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

viii. Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

ix. All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account. Whilst TSL may have previously obtained satisfactory identification evidence for the customer, the TSL shall take steps to learn as much as possible about the customer's new activities.

x. Although Directors and Senior Managers may not be involved in the handling of ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

xi. The CO should receive in-depth training on all aspects of the primary legislation, the regulations, regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

16. Reporting of Suspicious Transactions / Currency Transaction Report

i. A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and TSL shall put "on enquiry". TSL shall also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

ii. Where the enquiries conducted by TSL do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT to the relevant authorities.

iii. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result shall be properly documented, and made

available to the relevant authorities upon request. Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

(1) any unusual financial activity of the customer in the context of the customer's own usual activities;
(2) any unusual transaction in the course of some usual financial activity;
(3) any unusually-linked transactions;
(4) any unusual method of settlement;
(5)any unusual or disadvantageous early redemption of an investment product;
(6) any unwillingness to provide the information requested.

iv. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, TSL will need to approach such situations with caution and make further relevant enquiries. Given the type of business TSL conducts and the nature of its customer portfolio, TSL may set wish to set its own parameters for the identification and further investigation of cash transactions.

v. Where TSL has been unable to ascertain any cash transaction as reasonable, TSL will consider it suspicious. TSL is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

vi. If TSL decides that a disclosure shall be made, the law requires TSL to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

vii.The process for identifying, investigating and reporting suspicious transactions to the FMU shall be clearly specified in the policies and procedures and communicated to all personnel through regular training.

viii.TSL is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year. The Compliance Officer shall ensure prompt reporting in this regard.

ix. Vigilance systems shall require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:

(1) the date of the report;
(2) the person who made the report;
(3) the person(s) to whom the report was forwarded; and
(4) reference by which supporting evidence is identifiable.

x. It is normal practice for TSL to turn away business that it suspect might be criminal in intent or origin. Where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration shall be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction shall be reported to the FMU.

xi. Once suspicion has been raised in relation to an account or relationship, in addition

to reporting the suspicious activity TSL shall ensure that appropriate action is taken to adequately mitigate the risk of TSL being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

Implementation of UN Security Council Resolutions

17. <u>Sanctions Compliance – Implementation of UN Security Council Resolutions</u>

i. Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

(1) targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;
(2) economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;
(3) currency or exchange control;
(4) arms embargoes, which would normally encompass all types of military and paramilitary equipment;
(5) prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
(6) import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.; and
(7) visa and travel bans.

ii. The Regulations require TSL not to form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

iii. The UNSC, acting under chapter VII of the United Nations Charter, adopts the Resolutions on counter terrorism measures and proliferation of WMD, in particular;

a. the UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al-Qaida, Taliban, and the Islamic State in Iraq (Daésh) organizations. The regularly updated

consolidated list is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

b. the UNSC Resolution 1373 (2001), 1998 (2011) on terrorism and financing of terrorism requiring member states to proscribe individual and entities, who commit or attempt to commit terrorist act, freeze without delay the funds and other financial assets or economic resources, and prohibit making any funds or financial or other related services available to such proscribed persons and entities.

c. the UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions [1] on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution require, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718(2006) and its successor resolutions (on the DPRK) and listed under UNSCR 2231 (2015) (on Iran) is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/sc/2231/list.shtml

iv. Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. The said SROs are communicated to RPs, from time to time, and have a binding legal effect under the Act No. XIV of 1948. RPS should ensure compliance with the sanctions communicated through SROs. A list of such SROs issued by the Federal Government till date is also available at the following links:

UNSCR 1267

http://www.mofa.gov.pk/contentsro1.php
http://www.mofa.gov.pk/contentsro2.php

UNSCR 1718

http://www.secdiv.gov.pk/page/sro-unscr-sanctions

v. The Federal Government, Ministry of Interior issues Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001). The regularly updated consolidated list is available at the National Counter Terrorism Authority's website, at following link;

http://nacta.gov.pk/proscribed-organizations/

[1] The UNSC sanctions with respect to proliferation of WMD primarily encapsulates currently the Islamic Republic of Iran and the Democratic People's Republic of Korea's sanctions regime. The UNSC resolution on Iran is 2231 (2015). The UNSC resolution on Democratic People's Republic of Korea are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017).

vi. The individuals and entities designated under the aforementioned resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

vii. TSL shall, taking note of the circumstances where customers and transections are more vulnerable to be involved in TF and PF activities[2], identify high-risk customers and transections, and apply enhanced scrutiny. TSL shall conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relations involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

viii. TSL is also required to screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list.
TSL shall undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions. ix. Where there is a true match or suspicion, TSL shall take steps that are required to comply with the sanctions obligations including immediately-

(a) freeze without delay[3] the customer's fund or block the transaction, if it is an existing customer;
(b) reject the customer, if the transaction has not commenced;
(c) lodge a STR with the FMU; and
(d) notify the SECP and the MOFA.

x. TSL is required to submit a STR when there is an attempted transaction by any of the listed persons.

xi. TSL must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the TSL may consider raising an STR to FMU.

xii. Notwithstanding the funds, properties or accounts are frozen, TSL may continue receiving dividends, interests, or other benefits, but such benefits shall still remain frozen, so long as the individuals or entities continue to be listed.

xiii. TSL shall make their sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. TSL shall provide

adequate sanctions related training to their staff. When conducting risk assessments, TSL shall, take into account any sanctions that may apply (to customers or countries).

xiv. The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name.

xv. TSL shall document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

xvi. TSL is expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.

xvii. TSL may also educate their customers that in case of wrongful or inadvertent freezing, they may apply in writing for de-listing to Federal Government through relevant Ministry or to the UN's Ombudsman, as the case may be.

---

[2] The circumstances that the TSL shall take note of where customers and transactions are more vulnerable to be involved in PF activities relating to both DPRK and Iran sanction regime are listed on Annexure 4 as PF Warning Signs/Red Alerts.

[3] According to FATF , without delay is defined to be ideally within a matter of hours of designation by the UNSC

Risk Assessment and Applying a Risk Based Approach

(Please refer to Annex 1 for Risk Assessment Tables)

18. <u>Risk Assessment and Applying a Risk Based Approach</u>

i. The SECP AML/CFT Regulations shift emphasis from one-size-fits-all approach to Risk Based Approach ('RBA'), requiring TSL to carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF.

ii. The RBA enables TSL to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. TSL shall develop an appropriate RBA for its particular organization, structure and business activities and apply the RBA on a group-wide basis, where appropriate. As a part of the RBA, TSL shall:

1) Identify ML/TF risks relevant to them;
2) Assess ML/TF risks in relation to-
    a. Customers (including beneficial owners);
    b. Country or geographic area in which its customers reside or operate and where the RP operates;
    c. Products, services and transactions that the RP offers; and
    d. Delivery channels.
3) Design and implement policies, controls and procedures approved by its Board of Directors;
4) Monitor and evaluate the implementation of mitigating controls;
5) Keep their risk assessments current through ongoing reviews;
6) Document the RBA including implementation and monitoring procedures and updates to the RBA; and
7) Have appropriate mechanisms to provide risk assessment information to the Commission.

iii. Under the RBA, where there are higher risks, TSL is required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk situations or situations which are outside the TSL risk tolerance, the TSL may decide not to take on the accept the customer, or to exit from the relationship.

iv. In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures entities have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guidelines, therefore, applies to CFT as it does to AML, even where it is not explicitly mentioned.

v. The process of ML/TF risk assessment has four stages:

1) Identifying the area of the business operations susceptible to ML/TF;
2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;

3) Managing the risks; and
4) Regular monitoring and review of those risks.

a) <u>Identification, Assessment and Understanding Risks</u>

i. The first step in assessing ML/TF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the TSL. Depending on the specificity of the operations of TSL, other categories could be considered to identify all segments for which ML/TF risk may emerge. The significance of different risk categories may vary from institution to institution, i.e. TSL may decide that some risk categories are more important to it than others.

ii. In the second stage, the ML/TF risks that can be encountered by the TSL need to be assessed, analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the TSL from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for each TSL so that the conclusion on the total risk level must
be based on the relevant information available.

iii. For the analysis, TSL should identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, moderate if it can occur two to three per year and low if it is unlikely, but not possible. In assessing the impact, TSL can, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from low if there is only short-term or there are low-cost consequences, to high when there is cost inducing long-term consequences, affecting the proper functioning of the institution.

iv. The following is an example of a likelihood scale with 3 risk ratings as an example. TSL can customize their own as applicable to their operation with more details, if preferable.

Likelihood Scale			
Consequence Scale	Low	Moderate	High
Almost Certain	Moderate	Moderate	High
Possible	Moderate	Moderate	High
Unlikely	Low	Moderate	Moderate

v. TSL shall allow for the different situations that currently arise in its business or are likely to arise in the near future. For instance, risk assessment should consider the impact of new products, services or customer types, as well as new technology. In

addition, ML/TF risks will often operate together and represent higher risks in combination. Potential ways to assess risk include but are not limited to:

1) How likely an event is;
2) Consequence of that event;
3) Vulnerability, threat and impact;
4) The effect of uncertainty on an event;

vi. The assessment of risk should be informed, logical and clearly recorded. For instance, if a TSL has identified gatekeepers as presenting higher inherent risk in relation to the delivery of a product, the risk assessment should indicate how TSL has arrived at this rating (domestic guidance, case studies, direct experience).

Risk Assessment (lower complexity)

In line with this guidance, TSL may want to assess risk by only considering the likelihood of ML/TF activity. This assessment should involve considering each risk factor that have been identified, combined with business experience and information published by the Commission and international organizations such as the FATF. The likelihood rating could correspond to:

1) Unlikely - There is a small chance of ML/FT occurring in this area of the business;
2) Possible - There is a moderate chance of ML/FT occurring in this area of the business;
3) Almost Certain - There is a high chance of ML/FT occurring in this area of the business

For example, a TSL may have identified that one of its products is vulnerable to ML/TF due to the potential for cross-border movement of funds. The risk assessment highlights the product is easily accessible, that many customers are using it, and it is used in higher-risk jurisdictions. Combined with domestic and international guidance, the TSL assesses that the inherent risk rating of this product as high. The program should then address this likely risk with appropriate control measures. TSL will need to do this with each of the identified risks.

Risk Assessment (moderate complexity)

Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk.

Using likelihood ratings and consequence ratings can provide you with a more comprehensive understanding of the risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist you in applying the appropriate risk management measures as detailed in the program.

For example, TSL may have identified that one of its products is vulnerable to ML/TF and TSL assesses that the likelihood of this product being used in ML/TF activity is probable. TSL judge the impact of the identified risk happening in terms of financial loss and assess the consequence as moderate.

Cross-referencing possible with moderate risk results in a final inherent risk rating of moderate. The program should then address this moderate risk with appropriate

control measures. TSL will need to undertake this exercise with each of the identified risks.

Risk Assessment (higher complexity)

TSL could assess risk likelihood in terms of threat and vulnerability. For example, you
may consider domestic tax evasion criminals as the threat, and accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, this could result in an inherent risk rating of almost certain. TSL may then want to assess the impact of this event on the business and the wider environment.

Determining the impact of ML/TF activity can be challenging but can also help focus AML/CFT resources in a more effective and targeted manner. When determining impact, you may want to consider a number of factors, including:

1) Nature and size of your business (domestic and international);
2) Economic impact and financial repercussions;
3) Potential financial and reputational consequences;
4) Terrorism-related impacts;
5) Wider criminal activity and social harm;
6) Political impact;
7) Negative media.

TSL may want to give more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

In addition, TSL may want to consider how your risks can compound across the various risk factors. For example, you may identify that one of these products is high risk and is being used in a high-risk jurisdiction that is directly involved in the production or transnational shipment of illicit drugs. As such, you assess the compounded risk of this scenario as presenting an inherent risk rating of severe. TSL would be expected to prioritize and allocate the resources accordingly.

Applying the Risk Assessment

The risk assessment should help rank and prioritize risks and provide a framework to manage those risks. The risk assessment must enable TSL to prepare a comprehensive program. It should enable to meet relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

The assessment should help in determining suspicion and consequently assist in the decision to submit an STR to the FMU. TSL must submit an STR to the FMU if it think activities or transactions are suspicious. For instance, TSL may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an STR.

TSL must conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD. For instance, TSL may want to undertake ongoing CDD on high-risk customers on a more regular basis than on lower-risk customers.

TSL must undertake account monitoring. The risk assessment will help you design the

triggers, red flags and scenarios that can form part of account monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in the risk assessment) to be subject to more frequent and in-depth scrutiny.

New and Developing Technologies and Products

New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. The risk assessment should consider whether the business is, or may be, exposed to customers involved in new and developing technologies and products. The program should detail the procedures, policies and controls that TSL will implement for this type of customer and technology.

Material Changes and Risk Assessment

The risk assessment should adapt when there is a material change in the nature and purpose of the business or relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

Material change could include circumstances where TSL introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when TSL start using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, TSL may need to refresh their risk assessment.

vii. TSL shall document their risk assessment in order to be able to demonstrate its allocation of compliance resources. An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. The TSL shall therefore update its risk assessment every 12 to 18 months to take account of these changes. TSL shall also have appropriate mechanisms to provide risk assessment information to the Commission, if required.

b) Examples of Risk Classification Factors

Below are some examples that can be helpful indicators of risk factors/indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

High-Risk Classification Factors

(1) Customer risk factors: The institution will describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the TSL for ML or TF, and the consequent impact if indeed that occurs. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances

(e.g. significant unexplained geographic distance between the RP and the customer).

(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders.
(e) Business that is cash-intensive.
(f) The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;
(g) Politically exposed persons
(h) shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
(i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
(j) Requested/Applied quantum of business does not match with the profile/particulars of client
(k) real estate dealers,
(l) dealers in precious metal and stones, and
(m) lawyers/notaries

Example Scenarios of Customer Types

Small and Medium Sized Enterprises:

Small and medium business enterprise customers usually entail domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons that can act on its behalf. The likelihood that funds deposited are from an illegitimate source is HIGH, since it can't be easily be identified and can have a major impact on a large number of SME customers. Thus, the risk assessment and risk rating result is HIGH.

International corporations:

International corporate customers have complex ownership structures with foreign beneficial ownership (often). Although there are only a few of those customers, it is often the case that most are located in offshore locations. The likelihood of Money Laundering is High because of the limited number of customers of this type and the beneficial ownership could be questionable, with two criteria that in this scenario result in a possible risk impact of moderate and a moderate risk assessment.

As an example, these descriptions can result in a table as depicted below:

Customer Type	Likelihood	Impact	Risk Analysis
Retail Customer/Sole Proprietor	Moderate	Moderate	Moderate
High Net worth Individuals	High	High	High
NGO/ NPO	High	High	High
International Corporation	High	Moderate	Moderate
PEP	High	High	High
Company Listed on Stock Exchange	Low	Low	Low

Note: The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures should be applied.

(2) **Country or geographic risk factors**: Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the RP itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. The factors that may indicate a high risk are as follow:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems.

(b)Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.

(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(e) Jurisdictions in which the customer and beneficial owner are based;

(f) Jurisdictions that are the customer's and beneficial owner's main places of business.

(3)**Product, service, transaction or delivery channel risk factors**: A comprehensive ML/TF risk assessment must take into account the potential risks arising from the products, services, and transactions that the TSL offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:

(a) Anonymous transactions (which may include cash).
(b) Non-face-to-face business relationships or transactions.
(c) Payments received from unknown or un-associated third parties.
(d) The surrender of single premium life products or other investment-linked insurance products with a surrender value.
(e) International transactions, or involve high volumes of currency (or currency equivalent) transactions
(f) New or innovative products or services that are not provided directly by the TSL, but are provided through channels of the institution;
(g) Products that involve large payment or receipt in cash; and
(h) One-off transactions.
(i) To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions.
(j) Any introducers or intermediaries the firm might use and the nature of their relationship with the TSL.
(k) Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?
(l) Has the customer been introduced by another part of the same

financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures?

(m) Has the customer been introduced by a third party, for example, a Financial Institution that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:

(n) The third party applies CDD measures and keeps records to standards and that it is supervised for compliance with comparable AML/CFT obligations;

Low Risk Classification Factors

(1) Customer risk factors:

A customer that satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT Regulations.

(2) Product, service, transaction or delivery channel risk factors:

The product, service, transaction or delivery channel that satisfy the requirement under regulation 11(2) (c) to (g) of the SECP AML/CFT Regulations

(3) Country risk factors:

a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.

(b) Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, TSL could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

Example Scenarios of Product Types, Services and Transactions

Group Life Insurance:

The group life insurance products are simple and premiums tend to be very low. Premiums can only be paid through a bank account and no cash is involved. The life insurance products are only sold to resident persons. The likelihood that insurance products are used for ML/TF is LOW, with minor impact, and can result in a LOW risk assessment.

As an example, these descriptions can result in a table as depicted below:

Transaction Type	Likelihood	Impact	Risk Analysis
Intermediaries	High	Moderate	Moderate
Online Transaction	High	High	High
Bank Transfer	Moderate	Moderate	Moderate

c) Risk Matrix

In assessing the risk of money laundering and terrorism financing, TSL is to establish whether all identified categories of risks pose a low, moderate, high or unacceptable risk to the business operations. The TSL must review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, the TSL must also review the differences in the manner in which the TSL establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low-risk product in combination with a customer from a high-risk country will combine carry a higher risk.

TSL can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, the TSL take into account its specificities, may also define additional levels of ML/TF risk.

The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the TSL, the customers to whom the products and services are offered, the TSL size and organizational structure, etc. A risk matrix is not static: it changes as the circumstances of the TSL change. A risk analysis will assist TSL to recognize that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high-risk areas in its business.

The following is an example of a risk matrix of client product combination, but TSL shall develop its own risk matrix based on its own risk analysis. Example only:

Customer Transaction	Intermediaries	Online Transaction	Domestic Transfer	Deposit or Investment	Life Insurance	Securities Accounts
Domestic Retail Customer	**Moderate**	**Moderate**	**Moderate**	**Moderate**	**Low**	**Low**
High Net worth Customer	**N/A**	**High**	**Moderate**	**High**	**N/A**	**Moderate**
SME Business Customer	**High**	**High**	**Moderate**	**High**	**Moderate**	**Moderate**
International Corporation	**Moderate**	**High**	**Moderate**	**High**	**Moderate**	**Moderate**
Company Listed on Stock Exchange	**Moderate**	**Moderate**	**Low**	**Moderate**	**Low**	**Low**
PEP	**High**	**High**	**Moderate**	**High**	**Moderate**	**Moderate**
Mutual Fund Transaction	**Moderate**	**High**	**Moderate**	**High**	**N/A**	**N/A**

Note: When conducting risk assessment, TSL does not have to follow the processes in this guideline. As long as it comply with its obligations under the Act and any other applicable laws or regulations, it can choose the method of risk assessment that best suits its business. For example, large financial institutions may have their own systems and methodology for conducting a risk assessment. However, it should be prepared to explain and

demonstrate to the Commission, the adequacy and effectiveness of procedures, policies and controls.

d) Risk Management

Risk Mitigation

i. TSL shall have appropriate policies, procedures and controls that enable it to manage and mitigate effectively the inherent risks that it has identified, including the national risks. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.

ii. The nature and extent of AML/CFT controls will depend on a number of aspects, which include:

1) The nature, scale and complexity of the RP's business
2) Diversity, including geographical diversity of the RP's operations
3) RP's customer, product and activity profile
4) Volume and size of transactions
5) Extent of reliance or dealing through third parties or intermediaries.

iii. Some of the risk mitigation measures that TSL may consider include:

1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
2) setting transaction limits for higher-risk customers or products;
3) requiring senior management approval for higher-risk transactions, including those involving PEPs;
4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;
5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

Evaluating Residual Risk and Comparing with the Risk Tolerance

iv. Subsequent to establishing the risk mitigation measures, TSL shall evaluate its residual risk, the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the TSL's overall risk tolerance.

v. Where the TSL finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risks, the TSL should enhance the risk mitigation measures that are in place.