Document History

Anti-Money Laundering/ Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

Document Name:	Anti-Money Laundering/ Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Policies, Procedures and Controls
Name of the Company:	Integrated Equities Limited
Approving Authority:	Board of Directors
Effective Date:	26 April 2016
First Approval Date:	26 April 2016
1st Amendments Approval Date:	18 September 2017
2nd Amendments Approval Date:	19 October 2018
3rd Amendments Approval Date:	08 November 2019
4th Amendments Approval Date:	22 February 2020
5th Amendments Approval Date:	30 September 2020
6th Amendments Approval Date:	20 May 2021
7th Amendments Approval Date:	31 May 2022
8th Amendments Approval Date:	29 December 2023
9th Amendments Approval Date:	22 March 2024
Notes/Remarks	Any changes/amendments in the regulatory regime and/or guidelines related to AML/CFT/CPF as notified by SECP or any other regulatory body to the extent applicable to the Company shall be deemed to be part of this document

Anti-Money Laundering/ Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

Policies, Procedures and Controls

1. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING:

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.

2. PURPOSE AND SCOPE OF AML AND CFT REGIME:

1. An effective Anti-Money Laundering/ Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) regime requires financial institutions to adopt and effectively implement appropriate ML, TF and PF control processes and procedures, as defined in Regulations, not only as a principle of good governance but also as an essential tool to avoid involvement in ML, TF and PF. AML/CFT/CPF Regime is governed under Anti-Money Laundering Act, 2020 (Second Amendment) ("AML Act"), Anti-Money Laundering Rules, 2008 ("AML Rules") made under the Anti-Money Laundering Ordinance, 2007 ("AML Ordinance"), Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2020 ("SECP AML/CFT/CPF Regulations") made under the Securities and Exchange Commission of Pakistan Act, 1997 ("SECP Act"), upon recommendation of Financial Monitoring Unit ("FMU") established under AML Act, Guidelines on SECP AML/CFT/CPF Regulations issued by SECP in April 2020 and Pakistan National Risk Assessment (PNRA) Report on Money Laundering and Terrorist Financing issued in September 2019.

3. GUIDELINES ON SECP AML/CFT/CPF/CPF REGULATIONS:

1. The Guidelines are applicable to all Regulated Persons ("RPs") including Securities Brokers as defined under the SECP AML/CFT/CPF Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. It supplements the Regulations and the AML/CFT/CPF regime by clarifying and explaining the general requirements of the legislation to help RPs in applying national AML/CFT/CPF measures, developing an effective AML/CFT/CPF risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities. The Guidelines are based on Pakistan AML/CFT/CPF legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

4. POLICY, PROCEDURES AND CONTROLS:

As required under clause 4 (a) of the SECP AML/CFT/CPF Regulations, a Security Broker is required to:

1. develop and implement policies, procedures and controls with the approval its Board of Directors for enabling the Integrated Equities Limited to effectively manage and mitigate the risk that are identified in the risk assessment of ML/TF or notified to it by the Commission;
2. monitor the implementation of those policies, procedures and controls and enhance them if necessary;
3. perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks; and
4. have an independent audit function to test the system.
5. The Policies, Procedures and Controls should 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.

As required under clause 4 of the SECP (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2020.
A regulated person shall take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks in relation to

(a) Its customers;
(b) The jurisdictions or countries its customers are from or in;
(c) The jurisdictions or countries the regulated person has operations or dealings in; and
(d) The products, services, transactions and delivery channels of the regulated person.

The appropriate steps referred to above, shall include-

(a) Documenting the regulated person risk assessments;
(b) Considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;
(c) Keeping the risk assessments up-to-date;
(d) Categorizing the overall entity level risk as high, medium or low based on the result of risk assessment; and
(e) Having appropriate mechanisms to provide its risk assessment information to the Commission.

5. APPOINTMENT OF COMPLIANCE OFFICER AND HIS ROLE:

1. The IEL is required to appoint a management level officer as compliance officer (**"CO"**), who shall report directly, and periodically to the Board of Directors (**"Board"**) or to another equivalent executive position or committee. The CO must be a person who is fit and proper to assume the role and who:

2. has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
3. has sufficient resources, including time and support staff;
4. has access to all information and records necessary to perform the AML/CFT/CPF compliance function
5. ensure regular audit of the AML/CFT/CPF program;
6. maintain various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and request from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigation ; and
7. respond promptly to requests for information by the SECP/LEAs.

6. HOW TO COMMUNICATE THE POLICIES AND PROCEDURES TO EMPLOYEES AND STAFF AS WELL AS BRANCHES:

1. As part of first line of defense, the CO shall clearly specify the Policies, Procedures and Controls duly approved by the Board in writing, and communicated to all employees including those employed at braches through Inter-Office Memo ("IOM").
2. The CO must have the authority and ability to oversee the effectiveness of IEL AML/CFT/CPF systems, compliance with applicable AML/CFT/CPF legislation and provide guidance in day-to-day operations of the AML/CFT/CPF Policies and Procedures especially at the branches. He will assist in compliance to other departments and branches of the regulated person

7. HOW TO REFLECT CHANGES TO AML/ATF LEGISLATIVE AND REGULATORY REQUIREMENTS:

1. The CO shall update/amend the Policies, Procedures and Controls in line with the changes/amendments in SECP AM/CFT Regulations with the approval of the Board or Equivalent and communicate in writing to all relevant employees through IOM; and
2. The CO shall provide amendments in the Policies, Procedures and Controls separately attached to amendment Policies, Procedure and Controls showing impact of such changes on AML/CFT/CPF Regime.

8. HOW OFTEN TO UPDATE POLICIES, PROCEDURES AND CONTROLS:

1. As and when any change/amendment is affected in AML/CFT/CPF legislation applicable to the Securities Brokers, the CO shall immediately update the Policies, Procedures and Controls in line with the changes/amendment in legislatives.
2. The CO will communicate in writing to all employees after getting Board's approval on such changes.
3. The CO will update the risk profile of the country to which the IEL or its Customers are exposed to as and when it comes it his knowledge.

9. HOW OFTEN TO CONDUCT AN INDEPENDENT AUDIT OF YOUR AML/ATF COMPLIANCE PROGRAM:

1. IEL shall, on a regular basis, conduct an AML/CFT/CPF audit to independently evaluate the effectiveness of compliance program as set out in 7G of AML Act and in AML/CFT/CPF Policies and Procedures;
2. The frequency of the audit shall at least be quarterly basis commensurate with the nature, size, complexity, and risks identified during the risk assessments by the IEL.
3. The AML/CFT/CPF audits shall be conducted to assess the AML/CFT/CPF systems which include:
4. to test the overall integrity and effectiveness of the AML/CFT/CPF systems and controls;
5. to assess the adequacy of internal policies and procedures in addressing identified risks, including;
   a) CDD measures;
   b) Record keeping and retention;
   c) Ongoing Employees trainings
   d) Third party reliance; and
   e) Transaction monitoring.
6. to assess compliance with the relevant laws and regulations;
7. to test transactions in all areas of the IEL , with emphasis on high–risk areas, products and services;
8. to assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
9. to assess the adequacy, accuracy and completeness of training programs;
10. to assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any); and
11. to assess the adequacy of the IEL 's process of identifying suspicious activity including screening sanctions lists.
12. The compliance officer shall also be responsible for the areas including, but not limited to;
    a. timely submission of accurate data/ returns as required under the applicable laws;
    b. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
    c. such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations.

10. POLICIES, PROCEDURES AND CONTROLS:

11. THREE LINES OF DEFENSE:

The IEL shall establish the following three (3) lines of Defense to combat ML/TF:

1. **Front Office (Customer-Facing Activity):**
   a) Front Office / Dealers/Sale Persons shall be required to know and carry-out the AML/CFT/CPF due diligence related policies and procedures when a customer opens an account with the IEL which include the following:
   b) Account Opening Forms should be completed in the presence of the Customer with mandatory fill-in fields and all not relevant spaces shall be market as "Not Applicable or Crossed";
   c) KYC forms shall be completed in the presence of the Customer;
   d) All attachments needed as per Customer Relationship Forms of CDC and PSX shall be completed;
   e) Account Opening amount shall be accepted in cheque/pay-order/demand draft on the bank of beneficial owner of the customer.
   f) Account Opening confirmation along with all details entered into IEL's back-office, CDC and NCCPL shall be communicated to the Customer on his/her registered address/email or handed over to the Customer if physically available.

2. **Compliance Checks:**
   a) The Compliance Officer shall check the account opening forms along with all annexures before allowing the Customer to start Business Relation with the IEL;
   b) If there is any discrepancy in the Account Opening process, the Compliance Officer shall communicate the same to Front Office/Dealer/Sale Person for rectification before start of Business Relation with the IEL;
   c) The Compliance Officer shall do the Risk Assessment of the Customer as per AML/CFT/CPF Risk Assessment Matrix annexed to SECP Guideline on AML/CFT/CPF Regulations; and
   d) The Compliance Officer shall do the Risk Profiling of the Customer based on Risk Assessment of the Customer.

3. **Internal Audit Process:**
   a) Internal Auditor shall periodically conduct AML/CFT/CPF audits on an Institution-wide basis;
   b) In case of discrepancies/non-compliances observed during audit process, he/she will communicate his/her findings and along with recommendations to the Senior Management including Compliance Officer;
   c) Internal Auditor shall follow-up their findings and recommendation until their complete rectifications.

12. IDENTIFICATION OF CUSTOMERS, ASSESSMENT AND UNDERSTANDING OF RISK:

1. The IEL shall understand, identify and assess the inherent ML/TF risks posed by its:
   a) customer base;

b) products and services offered;
c) delivery channels;
d) the jurisdictions within which it or its Customers do business; and
e) an other relevant risk category.

2. The IEL will measure MT/TF risks using a number of risk categories while applying various factors to assess the extent of risk for each category for determining the overall risk classification, such as
a) Very High
b) High
c) Medium
d) Low

3. The IEL may follow the Probability and Likelihood Risk Rating Matrix as defined in the SECP Guideline for AML/CFT/CPF Regulations; however, it will make their own determination as to the risk weights to individual risk factors or combination of risk factor taking into consideration the relevance for different risk factors in the context of a particular Customer relationship.

4. The IEL shall assess and analyze as a combination of the likelihood that the risk will occur and the impact of cost or damages if the risk occur. The impact of cost or damage may consist of:
a) financial loss to the IEL from the crime;
b) monitory penalty from regulatory authorities; and
c) reputational damages to the business or the entity itself.

5. The IEL shall analyze and 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;
a) High if it can occur several times per year;
b) Medium if it can occur once per year; and
c) Low if it is unlikely, but not possible.

6. The IEL should update its risk assessment every 12 to 18 months taking into account:
a) new products are offered;
b) new markets are entered;
c) high risk Customers open or close their account; or
d) the products, services, policies and procedures are changed.

7. IEL shall have appropriate mechanism to provide risk assessment information to the Commission if required.

8. IEL shall not form business relationship with entities and/or individuals that are:
(a) designated under the United Nations Security Council (Act XIV of 1948) Resolutions and adopted by the Government of Pakistan;
(b) proscribed under the Anti Terrorism Act, 1997(XXVII of 1997) and as by Regulations; and
(c) associates/facilitators of persons mentioned in (a) and (b)."

IEL shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification;

Government entities accounts shall not be opened in the personal names of the government officials and account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government. Explanation:- "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

The IEL staff also perform biometric scan of the finger prints of the individual domestic Customer (based or residing in Pakistan) through the specified system.

9. High-Risk Classification Factors:

a) The IEL shall describe all types or categories of Customers that it provides business to and make an estimate of the likelihood that these types or category of Customers may misuse the IEL for ML or TF, and the consequent impact if indeed occurs. Risk Factor that may be relevant when considering the risk associated with a Customer or a Customer's beneficial owner's business include:
b) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the IEL and the Customer);
c) Non-resident Customers;
d) Legal persons or arrangements;
e) Companies that have nominee shareholders;
f) Business that is cash-intensive;
g) 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;
h) Politically Exposed Persons;
i) Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
j) Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets; and
k) Requested/Applied quantum of business does not match with the profile/particulars of client.

10. Country or Geographic Risk Factor:

a) Due to location of a Customer, the origin of a destination of transactions of the Customer, business activities of the IEL itself, its location and location of its geographical units, Country or Geographical Risk may arise. Country or

Geographical risk combined with other risk categories provides useful information on potential exposure to ML/TF. The IEL may indicate High Risk to its Customers based on following factors:

b) 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/CPF systems;
c) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
d) Countries identified by credible sources as having significant levels of corruption or other criminal activity; and
e) 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.

11. Product, Service, Transaction or Delivery Channel Risk Factor:

a) The IEL taking into account the potential risks arising from the products, services, and transactions that it offers to its Customers and the way these products and services are delivered, shall consider the following factors:
b) Anonymous transactions (which may include cash);
c) Non-face-to-face business relationships or transactions;
d) Payments received from unknown or un-associated third parties;
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 IEL, but are provided through channels of the institution;
g) Products that involve large payment or receipt in cash; and
h) One-off transactions.

12. Low Risk Classification Factor:

a) **Customer risk factors:**

i. The IEL shall rate a Customer as Low Risk and justify in writing about whom IEL's senior management has a direct knowledge and is satisfied about the matching of the size of investment being made by such person and the known income and resources of that person, and, satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT/CPF Regulations as under:

ii. Regulated entities and banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF

recommendations and are supervised for compliance with those requirements;

iii. public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;

b) Product, service, transaction or delivery channel risk factors:

1. The IEL rate the product, service, transection or delivery channel that satisfy the requirement under regulation 11(2) (g) of the SECP AML/CFT/CPF Regulations, such as the financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

c) Country risk factors:

i. The IEL taking into account possible variations in ML/TF risk between different regions or areas within a country, shall rate the Customer as Low Risk who belongs to:

ii. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT/CPF systems; and

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

d) Risk Matrix:

i. The IEL may use risk matrix annexed as Annexure-1 to SECP Guideline on AML/CFT/CPF Regulations as a method of assessing risk in order to identify the types or categories of Customers that are;

ii. in Low Risk category;

iii. those that carry somewhat higher risk, but still acceptable risk; and

iv. those that carry a high or unacceptable risk of money laundering and terrorism financing.

13. RISK MANAGEMENT:

1. Risk Tolerance:

a) Risk Tolerance is the amount of risk that the IEL is willing and able to accept and correlate its Risk Mitigation Measures and Controls accordingly, for example:

b) If the IEL determines that the Risk associated with a particular type of Customer exceed its Risk Tolerance, it may decide not to accept or maintain that particular type of Customer(s).

c) Conversely, if the IEL determine that the Risk associated with a particular type of Customer are within the bound of its Risk Tolerance, it must ensure that Risk mitigation Measures it applies are commensurate with the Risk associated with that type of Customer(s).

d) Senior Management and the Board of the IEL shall establish their Risk Tolerance, based on which the IEL shall have sufficient capacity and expertise to effectively manage the Risk acceptable in line with their Risk Tolerance and the consequences such as legal, regulatory, financial and reputation, of AML/CFT/CPF compliance failure.

e) If the IEL decides to establish a high-risk Tolerance and accept high risk then it shall have Mitigation Measures and Controls in place commensurate with those high risks.

2. Risk Mitigation and Controls Measures:

a) The IEL shall consider the following Risk Mitigation Measures:

b) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;

c) IEL shall monitor the accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the IEL knowledge of the customer, the customer's business and risk profile, including, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with regulated person.

d) requiring senior management approval for higher-risk transactions, including those involving PEPs;

e) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers;

f) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)

g) (1)All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the regulated person' knowledge of the customer, its business and risk profile and where appropriate, the sources of funds..

(2) IEL shall obtain information and examine, as far as possible the background and purpose of all complex and unusual transactions, which have no apparent economic or visible lawful purpose and the background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required.

(3) IEL shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date and relevant, by undertaking reviews of the existing records, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by regulated person in their AML/CFT/CPF policies, as per risk based approach

(4) In relation to (3) above , customers' profiles should be revised keeping in view the spirit of Know Your Customer/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

(5) Where IEL files an STR on reasonable grounds for suspicion that existing business relations with a customer are connected with ML/TF the regulated person may considers it appropriate to retain the customer-

(a) to substantiate and document the reasons for retaining the customer; and

(b) the customer's business relations with the IEL shall be subject to proportionate risk mitigation measures, including enhanced ongoing monitoring.

h) IEL is required to immediately scan its customer data bases and their Beneficial Owners /associates for any matches with the stated designated/proscribed person(s)/entity(ies) on the receipt of notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding updates in list of proscribed persons under the Anti- Terrorism Act, 1997. In case of a true match or suspicion of a proscribed/designated person following actions shall be taken by the IEL immediately

(a) Freeze without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer;

(b) Reject the customer, if the relationship has not commenced;

(c) Lodge a STR with the FMU, and simultaneously

(d) Notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions, or the National Counter Terrorism Authority ("NACTA") in case that person is designated under the Anti-Terrorism Act, 1997.

3. Client Acceptance and Credit Worthiness of Client:

1. The clients should be accepted after proper KYC/CDD measures and a detailed scrutiny of the documents should be conducted. The account shall be opened after the approval of the Senior Management. Risk Based Approach as explained earlier shall be adopted for KYC/CDD measures.
2. In order to cope up with the credit risk associated with the clients, the Annual Income Limit shall be assigned to the client as per the KYC Form and the documents provided by the client. These limits shall be set in the Back Office and monitored regularly.

14. HOW OFTEN IEL WILL UPDATE THE RISK ASSESSMENT?

1. Once the identification procedures have been completed and the business relationship is established, the IEL 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.
2. The IEL shall conduct ongoing monitoring of their business relationship with its Customers. Ongoing monitoring helps the IEL to keep the due diligence information up-to-date, and review and adjust the risk profile of the customers, where necessary. Auto Track System
3. The IEL conduct on-going due diligence which include scrutinizing the transactions undertaken through the course of business relationship with a Customer.
4. The IEL will be required to update the Risk Assessment of their Customer as per following schedule or on the occurrence of a triggering event, whichever is earlier:
   a) For its High Risk Customers, their Risk Assessment shall continuously be reviewed and updated, but a comprehensive review should be done at least monthly.
   b) For its Medium Risk Customers, their Risk Assessment shall be updated quarterly basis.
   c) For its Low Risk Customers, their Risk Assessment shall be updated 6 monthly.
5. The IEL may update the Customer CDD record on triggering of following events:
   a) Material changes to the customer risk profile or changes to the way that the account usually operates;
   b) Where it comes to the attention of the IEL that it lacks sufficient or significant information on that particular customer;
   c) Where a significant transaction takes place;
   d) Where there is a significant change in customer documentation standards;
   e) Significant changes in the business relationship.
6. The IEL update Risk Profiling of the Customer in the following circumstances:
   a) New products or services being entered into;
   b) The stated turnover or activity of a corporate customer increases;
   c) A person has just been designated as a PEP;
   d) The nature, volume or size of transactions changes.
7. The IEL 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:
   a) transaction type;
   b) frequency;
   c) amount;
   d) geographical origin/destination;
   e) account signatories.

15. CUSTOMER DUE DILIGENCE (CDD):

15.1

(1) The regulated person shall conduct CDD in the circumstances and matters set out in section 7A(I) and 7(E) of the AML Act.
(2) For the purposes of conducting CDD as required under section 7A (2) of the AML Act every regulated person shall comply with regulations 9-25 of the Regulations.
(3) The regulated person shall categorize each customer's risk depending upon the outcome of the CDD process.

15.2 The regulated person shall:

(a) identify the customer; and
(b) verify the identity of that customer using reliable and independent documents, data and information as set out in Annex 1 of Regulations

15.3 Where the customer is represented by an authorized agent or representative, the regulated person shall:

(a) identify every person who acts on behalf of the customer,
(b) verify the identity of that person in using reliable and independent documents, data and information as set out in Annex 1 of Regulations; and
(c) verify the authority of that person to act on behalf of the customer.

15.4 The regulated person shall also identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner by using reliable and independent document, data or sources of information as set out in Annex 1 of Regulations, such that the regulated person is satisfied that it knows who the beneficial owner is.

15.5 (1) For customers that are legal persons or legal arrangements, the regulated person shall identify the customer and verify its identity by obtaining the following information in addition to the information required in Annex 1 of Regulations:

(a) name, legal form and proof of existence;
(b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and
(c) the address of the registered office and, if different, a principal place of business.

(2) For customers that are legal persons or legal arrangements, the financial institution should be required to understand the nature of the customer's business and its ownership and control structure.

15.6 (1) For customers that are legal persons, the regulated person shall identify and take reasonable measures to verify the identity of beneficial owners by:

(a) identifying the natural person(s) (if any) who ultimately has a controlling ownership interest (as defined under relevant laws) in a legal person; and
(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and
(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

15.7 For customers that are legal arrangements, the regulated person shall identify and take reasonable measures to verify the identity of beneficial owners as follows:

(a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);
(b) for waqfs and other types of legal arrangements, the identity of persons in equivalent or similar positions as specified in (a).
(c) Where any of the persons specified in (a) or (b) is a legal person or arrangement, the identity of the beneficial owner of that legal person or arrangement shall be identified

15.8 The regulated person should verify the identity the customer and beneficial owner before establishing a business relationship or during the course of establishing a business relationship.

15.9 (1) The regulated person may complete verification of a customer or beneficial owner's identity after the establishment of the business relationship, provided that-

(a) this occurs as soon as reasonably practicable;
(b) this is essential not to interrupt the normal conduct of business; and
(c) the ML/TF risks are low.

(2) The types of circumstances where the regulated person permits completion of verification after the establishment of the business relationship should be recorded in the CDD policies.

(3) The regulated person shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

16 ONGOING MONITORING

(1) The regulated person shall conduct ongoing due diligence on the business relationship, including:
   (a) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;
   (b) obtaining information and examining, as far as possible, the background and purpose of all complex and unusual transactions which have no apparent economic or visible lawful purpose. The background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required.
   (c) undertaking reviews of existing records and ensuring that documents, data or information collected for the CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.

(2) In relation to sub-regulation (b), customers' profiles should be revised keeping in view the CDD and basis of revision shall be documented.

(3) The regulated person shall implement the measures as set out in section 7D (inability to complete CDD and tipping off) the AML Act.

(4) The regulated person shall comply with the provisions of the AML Act and rules, regulations and directives issued thereunder for reporting suspicious transactions/currency transactions in the context of money laundering or financing of terrorism.

(5) Where regulated person files an STR with respect to a customer with whom it has an existing business relationship, and if the regulated person considers it appropriate to retain the customer, then the regulated person shall:-
   (a) substantiate and document the reasons for retaining the customer; and
   (b) subject the business relationship to proportionate risk mitigation measures, including enhanced ongoing monitoring

(6) The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

17 EXISTING CUSTOMERS

(1) The regulated person is required to apply CDD requirement to its existing customers on the basis of materiality and risk and should conduct due diligence on existing relations at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained

(2) For existing customers who opened accounts with old NICs, the regulated person

shall ensure that attested copies of identity documents shall be present in the regulated person record. The regulated person shall block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification, the block from the accounts shall be removed.

(3) For customers whose accounts are dormant or in-operative ("dormant or in-operative account" means the account in which no transaction or activity or financial service has been extended by the regulated person from last three years"), withdrawals shall not be allowed until the account is activated on the request of the customer. For activation, the regulated person shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfill the regulatory requirements.

18 ENHANCED DUE DILIGENCE (EDD)

(1) Regulated person shall implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer presents high risk of ML/TF. The regulated person shall apply EDD where a customer presents high risk of ML/TF including but not limited to the following circumstances:

a. business relationships and transactions with natural and legal persons when the ML/TF risks are higher;
b. business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;
c. PEPs and their close associates and family members

(2) EDD measures include but shall not be limited to the following measures:

a. Obtaining additional information on the customer (e.g. volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner
b. Obtaining additional information on the intended nature of the business relationship;
c. Obtaining information on the source of funds or source of wealth of the customer;
d. Obtaining information on the reasons for intended or performed transactions.
e. Obtaining the approval of senior management to commence or continue the business relationship;
f. 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

(3) In relation to 18(1)(c) above, the regulated person shall implement appropriate

internal risk management systems, to determine if a customer or a beneficial owner is a PEP or a close associate or family member of a PEP, both prior to establishing a business relationship or conducting a transaction, and periodically throughout the course of business relationship. The regulated person shall apply, at minimum the following EDD measures:

a. obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
b. take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and
c. conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP

19 COUNTER MEASURES AGAINST HIGH RISK COUNTRIES & TERRITORIES

(1) Regulated persons shall apply the countermeasures including but not limited to, enhance due diligence proportionate to the risk as indicated by the Federal Government, pursuant to recommendations by the National Executive Committee and when called upon to do so by the FATF

20 SIMPLIFIED DUE DILIGENCE (SDD)

(1) The regulated person may apply SDD only where low risk is identified through adequate analysis through its own risk assessment and any other risk assessment publicly available or provided by the Commission in accordance with regulation 6 of these regulations and commensurate with the lower risk factors.
(2) The decision to rate a customer as low risk shall be justified in writing by the regulated person.
(3) SDD measures include the following measures:
    a. Verifying the identity of the customer and the beneficial owner of the client
    b. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold as prescribed or as set out by the Commission;
    c. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established
(4) The regulated person shall not apply any simplified SDD whenever there is a suspicion of money laundering or terrorist financing.

21 RELIANCE ON THIRD PARTIES

(1) A regulated person may rely on third party to conduct CDD on its behalf, inline with

the requirements specified in these Regulations;

a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer;
c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

Provided that despite third party reliance the regulated person shall-

i. remain liable for any failure to apply the indicated CDD measures (a) to (c) above;
ii. immediately obtain from the Third Party the required information concerning the indicated CDD measures (a) to (c) above;
iii. take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; and

d. satisfy itself that the Third Party is supervised by an AML/CFT regulatory authority or an equivalent foreign authority and has measures in place for compliance with AML Act obligation of CDD and record keeping;

(2) Where a regulated person relies on a third party that is part of the same corporate group, the regulated person may deem the requirements of sub-regulation 24(1) to be met if

a. the corporate group applies CDD and record-keeping requirements in accordance with the AML Act and its associated regulations;
b. the implementation of the requirements in paragraph (a) is supervised by an AML/CFT/CPF regulatory authority or an equivalent foreign authority; and
c. the corporate group has adequate measures in place to mitigate any higher country risks

(3) In addition to sub-regulation 24(1), when determining in which country a third party may be based, the regulated person shall have regard to available information on the level of country risk

(4) Notwithstanding any reliance upon a third party, the regulated person shall ultimately remain responsible for its AML/CFT/CPF obligations, including generating STRs and shall carry out ongoing monitoring of such customer itself

22 TFS OBLIGATIONS

(1) The regulated person shall undertake TFS obligations under the United Nations (Security Council) Act 1948 and/or Anti-Terrorism Act 1997 and any regulations made

there under, including

a. develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.
b. If during the process of screening or monitoring of customers or potential customers the regulated person finds a positive or potential match, it shall immediately
    i. freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO
    ii. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
    iii. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced

c. In all cases referred to in (b), the regulated person shall file a suspicious transaction report to the FMU in case that person is designated under United Nations Security Council Resolutions, or proscribed under the Anti-Terrorism Act, 1997 and simultaneously notify the Commission in the manner as may be instructed from time to time by the Commission.
d. implement any other obligation under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under

(2) The regulated person is prohibited, on an ongoing basis, from providing any financial services 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. The regulated person should monitor their business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the regulated person shall take immediate action as per law, including reporting to the FMU

Explanation:- For the purposes of this regulation the expression associates means persons and entities acting on behalf of, or at the direction, or for the benefit, of proscribed/ designated entities and individuals that may be determined on the basis of appropriate screening of sanctions lists, disclosed nominee/beneficiary information, publicly known information, Government or regulatory sources or reliable media information, etc

23. POLITICALLY EXPOSED PERSONS:

23.1. DEFINITION OF PEP:

23.2.

1) A Politically Exposed Person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is, or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption, bribery, and conducting activity related to terrorist financing (TF). The potential risks associated with PEPs justify the application of additional anti-money laundering/counter-terrorist financing (AML/CFT/CPF) preventative measures with respect to business relationships with PEPs**.**

23.3. **POLITICALLY EXPOSED PERSONS CATEGORIES**

1) The difference between foreign and domestic PEPs *may* be relevant for firms making specific risk assessments. To help clients gain a holistic view of potential risk. In the first instance PEPs are classified at a high level in the following categories:

2) **Foreign PEPs**

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

3) **Domestic PEPs**

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

4) **International organization PEPs**

Persons who are, or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e. directors, deputy directors, and members of the board or equivalent functions.

5) **Family members**

"family member" of a politically exposed person includes—

i. a spouse of the PEP
ii. lineal ascendants and descendants and siblings of the PEP

6) **Close associates**

Individuals who are closely connected to a PEP, either socially or professionally.

(i) an individual known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP;

(i) any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP;

(ii) an individual who is reasonably known to be closely connected with the PEP for any other reason, including socially or professionally

23.4. How you will seek approval from senior management?

1) The IEL shall obtain Senior Management approval to determine the nature and extend of EDD where the ML/TF risks are high. In assessing the ML/TF risk of a PEP, the IEL shall consider factors such as whether the Customer who is a PEP:
   a) Is from a high risk country;
   b) Has prominent public function in sectors know to be exposed to corruption;
   c) Has business interests that can cause conflict of interests (with the position held).

23.5. How you will take adequate measures to establish source of wealth and source of funds?

1) The IEL shall consider other red flags include (in addition to the Red Flags that they consider for other applicants):
   a) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
   b) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
   c) A PEP uses multiple bank accounts for no apparent commercial or other reason;
   d) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.
2) The IEL 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:
   a) the level of (informal) influence that the individual could still exercise; and
   b) 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).
3) Additionally, where appropriate, IEL shall consider filing a STR.

24. *SUSPICIOUS TRANSACTION REPORTING:*

24.1. Defining what is a suspicious transaction?

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted.

24.2. How you and your employees/agents will identify suspicious transactions:

1) The IEL may assess the following transactions as suspicious where a transaction is inconsistent in amount, origin, destination, or type with a Customer's know, legitimate business or personal activities;
2) The IEL shall put on enquiry if transaction is considered unusual.
3) The IEL shall pay special attention to the following transactions:
   a) All complex transactions;
   b) Unusual large transactions; and
   c) Unusual pattern of transactions.
   d) Which have no apparent economic or visible lawful purpose.

24.3. Reporting to Compliance Officer:

Where the enquiries conducted by the IEL do not provide a satisfactory explanation of the transactions, respective dealer/sale agent/trader/employee should consider that there are grounds for suspicion requiring disclosure and escalating the matter to the Compliance Officer. The employees of IEL are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law.

24.4. Reporting to Relevant Authority:

1) The Compliance Officer of the IEL shall conduct enquiries regarding unsatisfactory due diligence, complex, unusual large transaction, and unusual patterns of transactions, their background and document their results properly. He may make such transaction available to relevant authorities upon their request.
2) 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:
   a) any unusual financial activity of the Customer in the context of the Customer's own usual activities;
   b) any unusual transaction in the course of some usual financial activity;
   c) any unusually-linked transactions;
   d) any unusual method of settlement;
   e) any unusual or disadvantageous early redemption of an investment product;

f) any unwillingness to provide the information requested.

3) **Cash Transactions:**

a) Where cash transactions are being proposed by Customers, and such requests are not in accordance with the customer's known reasonable practice, the IEL will need to approach such situations with caution and make further relevant enquiries.

b) Where the IEL has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. It is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment/ receipt, RS 25,000/ or and above to PSX while any CTR involving amount PKR 2 million or above will be reported to FMU as well.

c) If the IEL decides that a disclosure should be made, the law requires the IEL 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.

4) **Reporting to Commission and FMU:**

a) IEL 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.

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

i. the date of the report;
ii. the person who made the report;
iii. the person(s) to whom the report was forwarded; and
iv. reference by which supporting evidence is identifiable.

c) Where an applicant or a Customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), the IEL shall consider filing a STR.

d) Where an attempted transaction gives rise to knowledge or suspicion of ML/TF, the IEL shall report attempted transaction to the FMU.

e) Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity The IEL shall ensure that appropriate action is taken to adequately mitigate its risk being used for criminal activities.

f) The IEL may include a review of either the risk classification of the Customer or account or of the entire relationship itself.

g) 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.

h) IEL without disclosing the contents of STRs, shall intimate to the Commission on bi-annual basis the number of STRs reported to FMU and the regulated person shall ensure that status report (indicating No. of STRs only) shall reach the AML Department from the seven days of close of each half year.

24.5. Tipping-off & Reporting:

1) **The Law prohibits tipping-off:**

a) A risk exists that Customers could be unintentionally tipped off when the IEL is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF.

b) The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

c) If the IEL 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.

d) If the IEL reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR.

e) The IEL shall ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

25. *RECORD KEEPING PROCEDURES:*

25.1. The IEL shall ensure that all information obtained in the context of CDD is recorded. This includes both;

1) recording the documents the IEL is provided with when verifying the identity of the Customer or the beneficial owner; and
2) transcription into the IEL's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

25.2. The IEL 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.

Where there has been a report of a suspicious activity or the IEL 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. The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

25.3. The iel shall also keep following records of identification data obtained through the customer due diligence process that would be useful to an investigation for a period of 5 years after the business relationship has ended:

1) Account files;
2) Business correspondence;
3) Records pertaining to enquiries about:
   a) Complex;
   b) Unusual large transactions; and
   c) Unusual patterns of transactions.

25.4. Beneficial ownership information must be maintained for:

1) at least five (5) years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist; or
2) five (5) years after the date on which the customer ceases to be a customer of the IEL.

25.5. 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.

25.6. 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) 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.

25.7. 1) IEL Shall maintain shall maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of five years from completion of the transaction: Provided that IEL may retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority

(2) The records shall be sufficient, as set out in section 7C of AML Act, to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity and the transactions records may be maintained in paper or electronic form, provided it is admissible as evidence in a court of law. Where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority, the regulated person shall retain such records until such time as the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained.

(3) The records of identification data obtained through CDD process like copies of identification documents, account opening forms, Know Your Customer forms, verification documents, other documents and result of any analysis along with records

of account files and business correspondence, shall be maintained for a minimum period of five years after termination of the business relationship.

(4) IEL shall ensure, to timely make available, all CDD and transaction records to the Commission, FMU and law enforcement agencies whenever required.

26. EMPLOYEE SCREENING AND TRAINING:

26.1. As part of the IEL Anti Money Laundering program, all Employees are expected to be fully aware of its Anti-Money Laundering policies and procedures.

26.2. Each Employee is required to read and comply with this Compliance Manual, address concerns to the Compliance Officer and sign the acknowledgement form confirming that he/she has read and understands SECP AML and CFT Policies and Procedures.

26.3. To ensure the continued adherence to SECP AML and CFT Policies and Procedures, all Employees are required to reconfirm their awareness of the contents of this Compliance Manual by signing the acknowledgement form annually, or more frequently, as required by the Compliance Officer.

26.4. All Employees are required;

1) At a time specified by the Compliance officer, to undertake training programs on AML and CFT Policies and Procedures. Such training shall enable them to understand new developments, money laundering and financing of terrorism techniques, methods and trends. The training shall also include their responsibilities relating to AML/ CFT.
2) To get trained in how to recognize and deal with transactions which may be related to money laundering.
3) To timely escalate and report the matter to the Compliance Officer.
4) To get themselves acquainted with SECP AML & CFT Rules & Regulations.
5) To comply with the requirements of Rules & Regulations.

26.5 Integrated Equities Limited shall also follow the methodology for Internal Risk Assessment as required by PNRA Report. The concepts as defined by PNRA report, i.e. threat, vulnerabilities, inherent risk, consequences and likelihood of ML/TF and remedial measures / controls will be taken into consideration. The vulnerabilities will be assessed by considering the products and services offered, the customers, the geographical reach and delivery channels available.

27. COMPLIANCE PROGRAMS

Compliance Program

1) In order to implement compliance programs as set out in 7G of the AML Act, the regulated person shall implement the following internal policies, procedures and controls

i. compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the regulated person's compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws
ii. screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively
iii. an ongoing employee training program; and
iv. an independent audit function to test the system

2) For purposes of (a) the regulated person shall ensure that the compliance officer
   (a) reports directly to the board of directors or chief executive officer or committee
   (b) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer
   (c) be responsible for the areas including, but not limited to-
      i. ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the regulated person and are effectively implemented
      ii. monitoring, reviewing and updating AML/CFT/CPF policies and procedures, of the regulated person
      iii. providing assistance in compliance to other departments and branches of the regulated person
      iv. timely submission of accurate data/ returns as required under the applicable laws
      v. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
      vi. such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations

28 In the case of a corporate group, in addition to the obligations established in regulation 27, the regulated person shall implement

a. policies and procedures for sharing information required for the purposes of CDD and risk management;
b. the provision, at group-level compliance, audit, and/or AML & CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML & CFT purposes.
c. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off

29. The regulated person shall ensure that their foreign branches and majority-owned subsidiaries in countries which do not sufficiently apply the FATF Recommendations, apply AML, CFT & CPF measures consistent with Pakistan's AML/CFT/CPF requirements, to the extent that host country laws and regulations

permit. If the foreign country does not permit the proper implementation of AML/CFT measures consistent with that of Pakistan requirements, financial groups should apply appropriate additional measures to manage the risks, and inform the Commission when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures foreign branch or subsidiary is unable to observe appropriate AML/CFT measures;

30. Correspondent Relationship

1. A regulated person shall perform the following measures, in addition to other measures prescribed in these regulations, when forming a correspondent relationship
   a) assess the suitability of the respondent financial institution by taking the following steps
      i. gather adequate information about the respondent financial institution to understand fully the nature of the respondent financial institution's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates
      ii. determine from any available sources the reputation of the respondent financial institution and the quality of supervision over the respondent financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and
      iii. assess the respondent financial institution's AML/CFT/CPF controls and ascertain that they are adequate and effective, having regard to the AML/CFT/CPF measures of the country or jurisdiction in which the respondent financial institution operates
   b) clearly understand and document the respective AML/CFT/CPF responsibilities of the financial institution and the respondent financial institution;
   c) assess the respondent financial institution in the context of sanctions/embargoes and Advisories about risks; and
   d) obtain approval from the financial institutions' senior management before providing correspondent services to a new financial institution

2. Regulated person shall document the basis for its satisfaction that the requirements of this regulations are met
3. Regulated person shall pay special attention when establishing or continuing correspondent relationship with financial institutions which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML/CFT/CPF standards in the fight against money laundering and financing of terrorism
4. No regulated person shall enter into or continue correspondent relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the

relevant authorities or is a shell financial institution

Explanation:- For the purposes of this regulation the expression "shell financial institution" means a financial institution incorporated, formed or established in a country or jurisdiction where the financial institution has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

5. A regulated person shall also take appropriate measures when establishing a Correspondent Relationship, to satisfy itself that its respondent financial institutions do not permit their accounts to be used by shell financial institutions

31. RISK-BASED APPROACH DURING THE CHALLENGING ENVIRONMENT/EXTRAORDINARY CIRCUMSTANCES:

The criminals may take advantage of any unprecedented situation such as economic uncertainty, fears of pandemics, forced seclusions, etc, to carry out financial fraud and exploitation scams including but not limited to investment and product scams. In this extraordinary circumstance when there is a probability to face difficulties in carrying out CDD, the following risk-based approach will be used by the Company:

1. Scanned/Digital copies of documents will be accepted in such a situation as described above, to be followed by obtaining the originals at a reasonable later time when the situation has settled down;

2. The Company shall accept recently expired government-issued identification in order to verify the identity of an individual (although still required to determine the authenticity of the identification);

3. Where customer's identity will be verified face-to-face, delayed verification of identity for establishing new business relationships will be adopted as permitted under section 6(5) of the SECP AML/CFT/CPF Regulation, 2018 dealing with CDD, provided that;

a) this occurs as soon as reasonably practicable;

b) this does not interrupt the normal conduct of business; and

c) the ML/TF risks are effectively managed;

4. Once customers have provided copies of identification documents, additional verification will be done using immediately available video call feature to compare the physical identity of a customer with scanned copies of identification documents;

5. Procedures such as telephoning the customer to ask questions about their identification, understanding and obtaining information on the purpose and intended nature of the business relationship or other questions that would assist in ascertaining whether the customer is who they claim and categorize to be;

6. Obtaining disclosures from customers to verify certain types of information provided and the

accuracy and completeness of documents;

7. The Company shall use and allow digital/online payment methods to carry out transactions within the prescribed limits.

32. The Company shall maintain the database of all its customers, their beneficial owners/associates, board of directors, trustees, and office bearers of its customers, for the required matching, screening, etc.

1. Following the above, required actions will be taken immediately on the receipt of notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions, intimation from the National Counter Terrorism Authority or Securities and Exchange Commission of Pakistan regarding updates in the list of proscribed persons.

2. The Company shall allocate appropriate human/technological resources to immediately scan their customer databases, their beneficial owners/associates, board of directors, trustees, and office bearers of its customers, for any matches with the stated designated/proscribed person(s)/entity(ies).

3. The Company shall not form business relationship with the person(s)/entity(ies) if the name(s) are appearing in the said list.

4. The Company shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of false verification.

5. The requirements as contained in AML/CFT/CPF Regulations 2020 dated 28 Sept, 2020 shall be followed in letter and spirit.

33. REPORTING PROCEDURES:

Annual risk assessment and control/compliance assessment framework based on data and information as on 31 March,

to be filed by 30 th April of each financial year ("FY"), starting from the date of notification of this directive, and as instructed from time to time by the Commission.

a) Risk Assessment Framework:

Regulated Persons should undertake and submit their internal annual risk assessment which should be aligned with the risks identified in the latest National Risk Assessment of the country and cover the process adopted for risk identification. The risk assessment methodology should cover the risk emanating from customers, products, geography and delivery channels, elaborate risk tolerance level and assess residual risk after implementation of mitigation measures. Regulated Persons are encouraged to use the template given in Annex 1 to the Guidelines for reference, but may choose their own risk assessment methodology that best suits or represents their business covering the aforementioned risks, in light of the AML Act, 2010 and the Regulations.

The risk assessment report should be reviewed and approved by the board of directors of the Regulated Persons and shall be signed by the chief executive officer/ company secretary.

b) Compliance Assessment Checklist:

Regulated Persons should submit their annual compliance assessment checklist to demonstrate adequacy and effectiveness of AML/CFT/CPF compliance framework in light of the Regulations, and are encouraged to use the checklist provided in Annex 2 to the Guidelines for this purpose.

B. Quarterly information/ data on 30th of the subsequent month of every quarter, containing the following information:

a) Extracts of the discussion / deliberations on ML/TF risks and issues, by board of directors and/or management committees;

b) Number of new customer accounts opened during the period according to risk categorizations i.e. high, medium and low and their respective investment amount;

c) Total number of foreign and domestic politically exposed persons("PEP") and their total value of investments/deposits/financing etc. during the period;

d) Number of accounts/transactions closed and rejected for non-compliance of Customer Due Diligence ("CDD") process and due to identification in proscribed person/Targeted Financial Sanction ("TFS");

e) Documentation of any activity for which a Suspicious Transaction Report ("STR") was considered but not filed along with rationale, during the period;

f) Copies of reports/mechanism to identify unusual transactions warranting further review;

g) Number of suspicious transactions, attempted transactions and currency transaction reports submitted to Financial Monitoring Unit ("FMU");

h) Detail of complaints received on account of Know Your Customer ("KYC") / AML, including its status i.e. in process/ resolved / closed, during the period;

i) Details of trainings conducted on AML/CFT/CPF for new and existing staff including number of participants and topics covered;

j) Number of customers transferred from one risk category to another and their amount of investments;

k) Confirmation of having an automatic Transaction Monitoring System ("TMS") or otherwise? If yes, the name of TMS used;

l) Do you have automatic name screening solution? If yes, then what is the name of screening solution? If not, what are your future plans w.r.t.to automation;

m) Up-gradation in AML CFT policies/manuals during the reporting period;

n) How much human resource is deployed for AML CFT and Compliance Function? Details of increase in number of employees during the period.

C. Each RP is required to immediately scan its customer data bases and their Beneficial Owners /associates for any matches with the stated designated/proscribed person(s)/entity(ies) on the receipt of notifications issued by the Ministry of Foreign Affairs under United Nations (Security Council) Act 1948 or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding additions, deletions and updates in list/SRO under the Anti- Terrorism Act, 1997 and. In case of a true match or suspicion of a proscribed/designated person following actions shall be taken by the RP immediately;

(a) Freeze without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer;
(b) Reject the transaction or attempted transaction or the customer, if the relationship has not commenced;
(c) Lodge a STR with the FMU, and simultaneously
(d) Notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions or the National Counter Terrorism Authority ("NACTA") in case that person is designated under the Anti-Terrorism Act, 1997

D. Compliance report on Statutory Regulatory Orders issued by the Ministry of Foreign Affairs under United Nations (Security Council) Act, 1948 or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/Home Departments of Provinces/Ministry of Interior regarding updates in the list of proscribed person(s)/entity(ies) under the Anti-Terrorism Act, 1997, shall be submitted to the Commission within forty eight (48) hours of receiving the same in the manner as may be instructed from time to time by the Commission.

E. the Commission hereby directs all the Regulated Entities to comply with following requirements of Red Flags/ indicators for identification of persons or entities suspected to be acting on behalf of or at the direction of designated/proscribed individuals or entities:-

I. Red Flags Applicable to all SECP Sectors:

The following indicators should be used to identify suspected persons:

a) A customer appears to have conducted transactions on behalf of or at the direction of a designated/ proscribed individual.
b) A customer is an office bearer (trustee/ member/ director/ authorized signatory etc.) of a designated/ proscribed entity.
c) A customer is a business partner of an office bearer (trustee/ member/ director etc.) of a designated/ proscribed entity.
d) A customer is a close family member of a designated/ proscribed individual who is also suspected to be associated with the business of the designated/ proscribed individual by way of financial or other assistance.
e) An entity has a designated/ proscribed individual on its board or management.
f) Unilateral sanctions listing identifies linkage/ association of a customer with a designated/ proscribed individual or entity.
g) Media (Broadcast/ Print/ Social) news highlights customer's involvement in providing financial or other assistance to designated/ proscribed individual or entity.
h) Inquiry from law enforcement agency/ intelligence agency indicating linkage of a customer with designated/ proscribed individual or entity.

II. Red Flags that specifically relate to Non-banking financial institutions (NBFIs)

i) The customer declares a proscribed person as a guarantor of loan or nominee of the customer.
j) Customer has obtained a loan from an NBFC, but the loan shall be utilized by a proscribed person.
k) Repayment of a loan to the customer is made by a proscribed person.
l) In case of Mutual Funds account to account transfer involving transfer to a proscribed individual or entity.
m) A customer who is refused financial services/ loan due to association with a proscribed person approaches another financial institution for securing a loan

III. Red Flags based on behavior of an Account Holder associated with proscribed individuals or entities:

a) A customer has provided the same residential/ office address that matches the known residential/ office address of a designated/ proscribed individual or entity.
b) A customer has provided the same personal contact number that matches the contact number provided earlier by a proscribed/ designated customer.
c) A customer depositing funds in the account of a person or entity listed in an

international or foreign jurisdiction's sanctions lists maintained in accordance with UNSC resolution 1373

d) A customer listed in an international or foreign jurisdiction's sanctions list maintained in accordance with UNSC resolution 1373, is depositing funds in another customer's account.

Annex 1

S No.	Type of Customer	Minimum Documents required for CDD
1.	Individuals	A copy of any one of the following valid identity documents: (i) Computerized National Identity Card (CNIC)/Smart National Identity Card (SNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP/SNICOP) issued by NADRA. (iii) Form-B/Juvenile card/ Child Registration Certificate (CRC) issued by NADRA to children under the age of 18 years. (iv) Pakistan Origin Card (POC) issued by NADRA. (v) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (vi) Proof of Registration (POR) Card issued by NADRA (vii) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Joint Account	(i) A copy of any one of the documents mentioned at Serial No. I; (ii) In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the RP.
3.	Sole proprietorship	(i) Copy of identity document as per Sr. No. 1 above of the proprietor. (i) Attested copy of registration certificate for registered concerns. (ii) Sales tax registration or NTN, wherever applicable (iv) Account opening requisition on business letter head. (v) Registered/ Business address. (vi) Certificate or proof of membership of trade bodies etc., (if any)

4.	Partnership	(i) Copies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed' (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v) Registered/ Business address.
5.	Limited Liability Partnership (LLP)	(i) Copies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Certified Copies of: (a) 'Limited Liability Partnership Deed/Agreement. (b) LLP-Form-III having detail of partners/designated partner in case of newly incorporated LLP. (c) LLP-Form-V regarding change in partners/designated partner in case of already incorporated LLP; and (iii)Authority letter signed by all partners, authorizing the person(s) to operate LLP account.
6	Limited Companies/ Corporations	(i) Certified copies of: (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (ii) Certified copy of Latest 'Form-A/Form-B'. (iii) Incorporate Form II in case of newly incorporated company and Form A / Form C whichever is applicable; and Form 29 in already incorporated companies (iv) Copies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account; (v) Copies of identity documents as per Sr. No. 1 above of the beneficial owners.
7	Branch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Copies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) Certified copies of (v) Form II about particulars of directors, Principal Officer etc.

		in case of newly registered branch or liaison office of a foreign company (vi) Form III about change in directors, principal officers etc. in already registered foreign companies branch or liaison office of a foreign company (vii) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account; and (viii) Branch/Liaison office address.
8	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Copy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Registered address/ Business address where applicable
9	NGOs/NPOs/Charities	(i) Certified copies of: (a) Registration documents/certificate (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing (iii) body, for opening of account authorizing the person(s) to operate the account. (iv) Copy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (v) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer. (vi) Registered address/ Business address.

10	Agents	(i) Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii) Copy of identity document as per Sr. No. 1 above of the agent and principal. (iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person. (iv) Registered/ Business address.
11.	Executors and Administrators	(i) Copy of identity document as per Sr. No. 1 above of the Executor/Administrator. (ii) A certified copy of Letter of Administration or Probate. (iii) Registered address/ Business address.
12.	Minor Accounts	(i) Copy of Form-B, Birth Certificate or Student ID card (as appropriate). (ii) Copy of identity document as per Sr. No. 1 above of the guardian of the minor.
13.	Mentally Disordered Person Account: ("Person with Mental Disorder" means a person with mental illness as defined in the applicable laws on mental health defined in the applicable laws on mental health")	i. Copy of applicable valid identity documents of mentally disordered person and court appointed manager under the applicable laws related to mental health; ii. Certified true copy of court order for appointment of manager for mentally disordered person; iii. Verification of identity document through bio-metric verifications from NADRA for both persons i.e. mentally disordered person and the manager appointed by court; iv. Verification of court order from the concerned court (to be obtained by Regulated Person); v. Account would be opened in the name of mentally disordered person and the same will be operated by the court appointed manager; vi. All CDD requirements/formalities should be conducted / completed for both persons; and vii. In case of change of manager by the court, the CDD will be conducted for the new appointed manager by the Regulated Person afresh

Note:

(i) For due diligence purposes, at the minimum following information shall also be obtained and recorded on KYC (Know Your Customer)/CDD form or account opening form:

(a) Full name as per identity document;
(b) Father/Spouse Name as per identity document;
(c) Mother Maiden Name;
(d) Identity document number along with date of issuance and expiry;
(e) Existing residential address (if different from CNIC);
(f) Contact telephone number(s) and e-mail (as applicable);
(g) Nationality-Resident/Non-Resident Status
(h) FATCA/CRS Declaration wherever required;
(i) Date of birth, place of birth;
(j) Incorporation or registration number (as applicable);
(k) Date of incorporation or registration of Legal Person/ Arrangement;
(l) Registered or business address (as necessary);
(m) Nature of business, geographies involved and expected type of counter-parties (as applicable);
(n) Type of account/financial transaction/financial service;
(o) Profession / Source of Earnings/ Income: Salary, Business, investment income;
(p) Purpose and intended nature of business relationship;
(q) Expected monthly turnover (amount and No. of transactions); and
(r) Normal or expected modes of transactions/ Delivery Channels.

(ii) The copies of identity documents shall be validated through NADRA verisys or Biometric Verification. The regulated person shall retain copy of NADRA Verysis or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.

(iii) In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account.

(iv) For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing

instructions will continue to be permissible.

(v) The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.

(vi) The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where SECP RPs should obtain photocopies of identity documents of only those directors and persons who are authorized to open and operate the account. However, SECP RPs shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B'/ Form 29.

(vii) Government entities accounts shall not be opened in the personal names of a government official. Any account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

Explanation:- For the purposes of this regulation the expression "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

Explanation:- For the purpose of this Annexure I the expression "NADRA" means National Database and Registration Authority established under NADRA Act, (VIII of 2000

1. Introduction to AML/CFT Policy Amendments:

This section provides an overview of the amendments being made to the Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) policies of "Integrated Equities Limited" operating in the Pakistan Stock Exchange. The purpose of these amendments is to align the policies with the findings and recommendations outlined in the Pakistan National Risk Assessment 2023 document. This section will discuss the reasons for the amendments, highlight the importance of compliance with AML/CFT regulations, and provide an outline of the changes that will be implemented.

2. Overview of Pakistan National Risk Assessment 2023:

The financial sector has been assessed based on its clientele, the offered products and services, its geographic reach, and the channels it operates through. The summarised comparative position of vulnerability ratings of these sectors is given as under;

3. Implementation Plan for Stock Brokers:

The securities market contributes to economic growth, job creation, and overall prosperity. The securities brokers and the exchange itself are licensed by SECP. Companies listed on the PSX include almost all sectors, including manufacturing, services, trading, etc. Securities brokers in Pakistan operate under the following primary categories: Trading and Clearing; Trading and Self-Clearing, Trading Only; and Online Only Securities Broker.

4. Key Findings and Recommendations:

	NRA 2019	NRA 2023
Rating Scales	High	Very High
	Medium High	High
	Medium	Medium
	Medium Low	Low
	Low	

I. Banking Companies: The TF risk for the banking sector is rated as **High.**
II. Exchange Companies: The TF risk for exchange companies' channel is rated as **Medium.**
III. Securities Market: The TF risk for this channel is rated as **Low.**
IV. Insurance: The TF risk for this channel is rated as **Low.**
V. NBFCs and Modaraba: The TF risk for this channel is rated as **Low.**
VI. Microfinance Institutions: The TF risk for this channel is rated as **Low.**
VII. Legal Persons and Legal Arrangements: TF risk is reduced. The TF risk for this channel is rated as **Low.**

5. Conclusion and Next Steps

Changes in Risk measures are duly adopted.