Progressive investment management (pvt) limited

TREC-420 Holder: Pakistan stock exchange limited

AMl/CFT/PF & KYC policy & procedure

Updated up to September 2023

TABLE OF CONTENTS

What anti money laundering ("AMLI"), terrorist financing ("CFT") and proliferation financing ("PF") 4
Policy statement.....4
Goals & objectives:.....5
Scope:.....5
Business units.....6
Compliance officer:.....6
Conducting employee.....6
Internal audit function:.....7
Employee training:.....7
Senior management training:.....8
Employee due diligence screening:.....8
Customer due diligence.....8
Ongoing monitoring of customers, systems and controls.....10
Simplified due diligence to a high-risk customer.....11
Due diligence of existing customers.....11
Reporting of suspicious transactions.....12
Customer risk factors:.....12
List of information required for customer identity.....13
Basic identification information.....13
Other basic information.....13
Other relevant information for natural persons, as applicable.....13
Information for legal persons/ legal arrangements.....13
Additional information in case of "trusts".....14
Sectoral risk assessment of legal person and legal arrangements (lpla).....14
Client identification procedures:.....15
Client identification procedures for joint accounts:.....15
Client identification procedures for corporations, partnerships, trusts and other legal entities:.....16
List of authorized signatories.....16
Customer due diligence (cdd).....17
Politically exposed persons (peps).....17
High net worth individuals (hnwi).....18

Beneficial ownership: 19
Mentally disordered person account: 19
Biometric verification system 20
Nadra verisys: 20
Identification Of Geographic Areas That May Fall Into High Risk Geography 21
customer acceptance policy: 21
Targeted financial sanctions (tfs) under unsc resolutions 21
Sahulat accounts 22
Restricted personal list: 23
Pakistan's national refugee policy afghanistan, ... 23
Prohibition of personal accounts for business purposes 23
Risk assessment and applying a risk based approach 24
Simplified due diligence measures 25
Person with mental disorder 25
Enhanced due diligence 25
High net worth individuals (hnwis) 26
Record keeping procedures regulation statutory requirements under aml/cft legislations amla: 26
Internal controls 28
Payment mechanism: 29
for amounts less than or equivalent to pkr 25,000 29
Exceptional circumstances 29
General reporting procedures: 29
Reporting of suspicious transaction/currency transaction report: 30
Wire transfers 31
Record-Keeping Procedures 32
Approval from board of directors: 33
Effective date: 33

What anti money laundering ("AML"), terrorist financing ("CFT) and proliferation financing ("PF")

Anti-money laundering and countering the financing of terrorism and proliferation financing thereby strengthening financial sector integrity and contributing to safety and security. Ml is the method by which criminals disguise or attempt to disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence. The term "offence of money laundering" is defined in section 3 of the AMLA

Terrorists and terrorist organizations rely on money to sustain themselves and to carry out terrorist acts. Money for terrorists is derived from a wide variety of sources. Generally, individual terrorists or entities are not greatly concerned with disguising the origin of money, they are concerned with concealing its destination and the purpose for which it has been collected. Terrorists and terrorist organizations therefore employ techniques similar to those used by money launderers to hide their money, which may be from legitimate or illegal sources.

Proliferation Financing" means the financing of proliferation of weapons of mass destruction]

It includes the provision of funds or financial services in connection with the means of delivery of such weapons and other related goods and technology

There are 3 stages of PF:

Program fundraising.

Disguising the funds.

Procurement of proliferation-sensitive materials and technology.

Policy statement

PIML is committed to fully comply with all applicable laws and regulations regarding SECP- AMLI/CFT/PF regulation 2020 which is amended up to September 2023. PIML has adopted the procedure and will enforce the provisions set forth in AML/CFT/PF regulations in order to prevent and detect money laundering, terrorist financing and other illegal activities.

PIML shall appropriately comply with the requirements stipulated in these regulations considering their size, nature of business and complexities of operations; through proper documentation of the scope and applicability of requirements envisaged in these regulations.

Goals & objectives:

The objective of this policy is to ensure that the products and services of PIML are not used to launder the proceeds of crime and that all of the PIML's staff are aware of their obligations and the need to remain vigilant in the fight against money laundering and terrorist financing.

The document also provides a framework to comply with applicable laws, regulatory guidelines specially related with detection and reporting of suspicious activities. Other objectives pursued by this policy are as follows:

Promote a "know your customer" policy as a cornerstone principle for the brokerage firm's ethics and practices

Introduce a controlled environment where no business with a customer is transacted until all essential information concerning the customer has been obtained

Conduct self-assessments of compliance with AML policy and procedures

Introducing to the employees the stages of money laundering process and their individual duties

Establishing a review process which will be used to identify opportunities that might be used to launder money

Providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is detected or suspected

Adherence to this policy is absolutely fundamental for ensuring that the PIML is fully complied with applicable anti-money laundering rules and regulations.

The PIML is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML policy for its business. In case of any clarification contact compliance department of PIML at **sharifchaudhry@gmail.com**

Scope:

This policy is applicable to the PIML's operations including business. PIML shall ensure compliance with the regulations on KYC, CDD, AML AND CFT or that of the SECP whichever are more exhaustive. Our coverage will include:

- Compliance of AML act 2010
- Compliance of AML/CFT/PF, Regulation 2020 with amended up to 2023
- Compliance of SECP requirements on KYC, CDD, AML & CFT
- FATF recommendations
- International standards and guidelines including regulatory sanctions as applicable

Three lines of defense to combat ML/TF/PF:

Business units

PIML senior management is the first line of defense has day-to-day of risks and controls. For each decision or approval, they need to determine and ensure that sufficient resources are provided for carrying out policies and procedures related to AML/CFT/TF due diligence. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

Compliance officer:

As part of second line of defense, the compliance officer must have the authority and ability to oversee the effectiveness of RP'S AML/CFT systems. His responsibilities include compliance with applicable AML/CFT legislation, reporting of suspicious and currency transactions, and providing guidance in day to-day operations of the AML/CFT policies and procedures, including freezing of accounts/funds if subsequently identified on proscribed lists

To ensure that the PIML's policies and procedures are adhered to, PIML shall designate compliance officer. Responsibilities of the compliance officer include the following:

Review of account opening forms and sign off from compliance perspective

Coordination and monitoring of PIML's day-to-day compliance with applicable anti money laundering laws and regulations and PIML's own AML/CFT/PF policy & procedures

Conducting employee

Training programs for appropriate personnel related to the PIML's AML/CFT/PF policy & procedures and maintaining records evidencing such training

Receiving and reviewing any reports of suspicious activity from employees

Determining whether any suspicious activity as reported by an employee warrants reporting to senior management of the firm

Coordination of enhanced due diligence procedures regarding clients and responding to both internal and external inquiries regarding PIML's AML/CFT/PF policy & procedures

Sufficient skills and experience to develop and maintain systems and controls (including submitting written policies and procedures for management's approval

Reports directly and periodically to the board of directors, chief executive or equivalent competent authority on AML/CFT/PF systems and controls;

Access to all information and data within the RP necessary for performing the AML/CFT compliance function

Ensures independent audit of the AML/CFT/PF program; maintains or ensures maintenance of various logs, as necessary, with respect to declined business/rejected transactions, internal investigations, suspicious transaction reports, and freezing or blocking of payments under sanction regime

Responds promptly to requests for information by the SECP.

Internal audit function:

Third line of defense: internal audit function

PIML to ensure on a regular basis, conduct an AML/CFT/PF audit to independently evaluate the effectiveness of compliance with AMLI/CFT/PF policies and procedures are adhered to, PIML board of director's act as internal audit function.

Audit should be commensurate with the PIML nature, size, complexity, and risks identified during the risk assessments

The effectiveness of parameters for automatic alerts and the adequacy of process of identifying suspicious activity, internal investigations and reporting the adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.

Employee training:

PIML ensures that all appropriate staff receives training on AML/CFT/PF prevention on a regular basis;

Ensure that all staff fully understand the procedures and their importance, that they will be committing criminal offences if they contravene the provisions of the legislation.

Training to staff is provided semiannually& annually or more frequently where there are changes to the applicable legal or regulatory requirements.

PIML provide their staff training in the recognition and treatment of suspicious activities, risk assessments. Trainings are ensured to compliance with all of the requirements of applicable legislation.

All staff is encouraged to provide a prompt and adequate report of any suspicious activities.

All new employees are trained on AML/CFT/PF know the legal requirements to report and of their legal obligations in this regard.

PIML will consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT/PF matters, read the PIML's AML/CFT/PF manuals, policies and procedures, and understand the AML/CFT/PF obligations under the relevant legislation.

Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions.

All staff will be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. A customer with a personal account opening a business account. Although directors and senior managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT/PF policies and procedures.

Senior management training:

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

Supervisors, managers and senior management (including board of directors) be provided with a higher level of training covering all aspects of AML/CFT/PF procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

Employee due diligence screening:

PIML will maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions. PIMLs shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the PIML may:

Verify the references provided by the prospective employee at the time of recruitment

Verify the employee's employment history, professional membership and qualifications

Verify details of any regulatory actions or actions taken by a professional body

Verify details of any criminal convictions

Verify whether the employee has any connections with the sanctioned countries or parties

All employees are screened against lists of designated and proscribed individuals, on an ongoing basis, and maintain proper record of screening. Accordingly, employees shall become disqualified if they are designated/ proscribed or associated directly or indirectly

Monitoring the employees trading account activity on ongoing basis

Customer due diligence

- PIML shall ensure to adopt the methods applied by criminals to launder money or finance terrorism involve the use of the financial system to transfer funds as per the guide lines of AML/CFT/PF regulations.
- To ensure the application of strict customer due diligence (CDD) by PIML and a high degree of transparency is crucial to fight money laundering and the financing of terrorism effectively.

- PIML the procedure of CDD shall t be applied upon establishment of a business relationship and the basic steps of CDD measures are the appropriate identification of a customer and/or beneficial owner, the verification of the identity of the customer or beneficial owner, as well as the collection of information on the customer's purpose and nature of the business relationship to meet the standard of" financial action task force (FATF)".
- In case the PIML is not been able to satisfactorily completed required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an str.
- Anonymous or factious account shall not open or maintain
- Shall, at minimum, conduct CDD of their customers/ occasional customers in circumstances and matters set out in section 7a (1) of the act. (a) for the purposes of section 7a (1) (b) of the act, PIML shall conduct CDD in respect of every occasional customer
- Shall apply CDD measures as per section 7a (2) of the act. AML/CFT/PF regulations for identification of customer/ occasional customer, at the minimum,
- Shall obtain information for purposes of verification of identity of the customer/ occasional customer, at the minimum
- Shall obtain the documents mentioned for ensuring verification of documents and information obtained for CDD purposes,
- Shall refer the source from which the document or information originates (e.g. Nadra, etc.) Or use reliable and independent document, data or source while complying with CDD requirements given in the act and in these regulations
- Shall ensure compliance as per the relevance of the requirement with their business & operational model, nature & types of customers they deal with, features of financial services they offer, and level of risk posed by geographical location in which they in, depending AML/CFT/PF
- Shall complete the verification of the identity of the customer, occasional customer and beneficial owner before establishing a business relationship or conducting the occasional transaction or during the course of establishing a business relationship or occasional transactions.
- CDD information of customers categorized as "high risk" shall be reviewed/updated each year.
- CDD information of customers categorized as "medium risk" shall be reviewed/updated at least once in every three years while CDD information of customer categorized as "low risk" shall be reviewed/updated at least once in every five years.
- They may determine the respective frequency for review/update of customers falling in different risk categories and include the same in their internal policy.
- Moreover, CDD information of customers shall be updated immediately whenever material information regarding the customers becomes known or there is a suspicion of money laundering or terrorist financing or there are doubts about the veracity or adequacy of previously obtained data.

- SECP regulation 4 risk assessment, requires the regulated person to take appropriate steps in accordance with section 7f risk understanding of the AML act 2010 ("amla"),

- To identify, assess and understand its money laundering, and terrorism financing risks for customers, geographic areas, products/services, transactions and delivery channels.
- An assessment of all four factors will result in an applicable rating.
- Nra provides guidance for overall sector while risk rating of each client is dependent upon internal risk assessment by every entity after accommodating combination of abovementioned four factors.
- As a rule of thumb, national risk assessment (nra) allows a country to identify, assess and understand its money laundering and terrorist financing risks at the national/sectoral level.
- Once these risks are properly understood, appropriate aml/cft measures that correspond to the level of risk identified may be applied using the risk-based approach (rba) as prescribed by fatf recommendation
- For additional guidance please refer to chapter
- Risk and mitigation, secp aml/cft regulations 2020.
- Link: sro 921 (i)/2020 securities and exchange commission of pakistan (aml/cft) faqs on aml/cft/pf obligation – 6th edition page 3 of 7 regulations, 2020 | secp and section 5 of secp aml/cft guidelines 2021

Wealth statement reported with income tax return of a client for an enhanced verification of source of wealth (sow) and source of funds (sof) of a particular customer

Income tax returns and wealth statements do not completely establish the source of wealth/ funds of a customer and only provide evidence against income/wealth sources regarding predicate offense of tax evasion. It is useful to obtain wealth statement reported with income tax return for the verification of source of income/wealth. However, additional verification measures that could be applied for high-risk business relationships include, obtaining additional information on the intended nature of the business relationship, the reasons for intended or performed transactions, bank statements and obtaining approval of senior management to commence or continue the business relationship etc

Ongoing monitoring of customers, systems and controls

- PIML shall follow the requirement of (regulation 19 of AML/CFT/PF regulations 2020 for ongoing monitoring of customers. Once the identification procedures have been completed and the business relationship is established
- The PIML monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated, when the relationship/account was opened.
- Conduct ongoing due diligence on the business relationship
- Scrutinizing transactions undertaken throughout the course of the relationship
- To ensure that the transactions being conducted are consistent and with the knowledge of the customer their business and risk profile
- Examining the background and purpose of all complex and unusual transactions that have no apparent economic or visible lawful purpose. The background and purpose of these transactions will be inquired and findings documented with a view to making this information available to the relevant

- Carrying out reviews of existing records and ensuring that documents, data or information collected for CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.
- Review and revise the profiles of customers identified will assess the effectiveness of their risk mitigation procedures and controls, identify areas for improvement and update their systems as appropriate to suit the change in risks.
- PIML strictly monitor and has to check the significant change in customer documentation standards t changes in the business relationship transaction restructuring to circumvent the applicable threshold .
- To check the potentially suspicious activities or "red flags" for AML/CFT/PF enabling rps to recognize possible AML/CFT/PF schemes. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Simplified due diligence to a high-risk customer

As per regulation 6 of AML/CFT/PF regulations 2020, "the PIML may take simplified measures to manage and mitigate risks, if lower risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ml/tf/PF'. Based on the aforementioned, high risk customer can only be offered low risk product after performing EDD

Due diligence of existing customers

- PIML review the relation with existing customers on following grounds:
- Must be assigned a risk rating based on the risk matrix risk assessment in its risk based approach
- The CDD requirements entails that if suspicion of AML/CFT/PF or becomes aware at any time that it lacks sufficient information about an existing customer,
- Take steps to ensure that all relevant information is obtained as quickly as possible. Identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information.
- Should entertain filing a suspicious transaction report if there are any indicators that support such an action.
- Existing customers who opened accounts with old CNIC, ensure that attested copies of identity documents are present in the records
- The PIML will 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.
- For customers whose accounts are dormant or in-operative, withdrawals will 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.

- If an rp has a suspicion of AML/CFT/PF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Reporting of suspicious transactions

I. PIML examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose. Activities requiring further enquiry may fall into one or more of the following:

II. Any unusual financial activity of the customer not in line with the customer's profile

III. Any unusual transaction in the course of some usual financial activity

IV. Any unusually-linked transactions

V. Any unusual method of settlement

VI. Unusual or disadvantageous early redemption of an investment product

VII. Unexplained unwillingness to provide the information requested

VIII. Where the enquiries conducted by the PIML do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalation of matters to the co. Ultimately, PIML must decide whether to file a suspicious transaction report based on the above. If it decides not to file, reasons must be documented for this decision

IX. PIML may refuse business that they suspect, might be criminal in intent or origin

Maintain a comprehensive record of aml/cft reports w.r.t. Internal enquiries and reporting to fmu. Such documentation may include:

A. The report itself and all its attached information / documents in copy;
B. The date of the report;
C. The person who made the report and the recipient;
D. Any decision based on the str for the specific customer or a group of customers;
E. Any updating or additional documentation taken based on the report ; and
F. The reasoning underlying the decisions taken.

Customer risk factors:

The PIML considering the risk associated with a customer or a customer's beneficial owner's business includes:

A. The business relationship is conducted in unusual circumstances (e.g. Significant unexplained geographic distance between the rp and the customer)
B. Non-resident customers.
C. Legal persons or arrangements
D. Companies that have nominee shareholders.
E. Business that is cash-intensive.

F. Ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons.
G. Politically exposed persons.
H. Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions.
I. Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
J. Requested/applied amount of business does not match the profile/particulars of client.
K. Designated non-financial business and professions: real estate dealers, dealers in precious metal and stones, accountants and lawyers/ notaries

List of information required for customer identity

Basic identification information

1. Full name as per identity document
2. Mother maiden name
3. Date of birth
4. Place of birth
5. Permanent address
6. Identity document number, whichever applicable
7. Date of expiry of applicable identity document

Other basic information

1. Father/ spouse name as per identity document
2. Date of issuance of applicable identity document
3. Contact number: mobile number (s)/ land line number
4. Purpose of account/ transaction/ business relation
5. Beneficial ownership/ controlling rights

Other relevant information for natural persons, as applicable

1. Current/ mailing address
2. Personal email address (as applicable)
3. Nationality – resident/ non-resident status
4. Fatca/ crs declaration, wherever required
5. Profession/ source of income/ funds: salary, business, investment income
6. Next of kin
7. Attested passport size photo (in case of photo account instructions)
8. Live photo (in case of digital on boarding)

Information for legal persons/ legal arrangements.

1. Registration/ incorporation number or business registration number (as applicable)
2. Date of incorporation or registration of legal person or arrangement (as applicable)

3. Place of incorporation or registration of legal person or arrangement (as applicable)
4. National tax number (ntn)
5. Nature of business, geographies involved and expected type of counter-parties (as applicable) aml/ cft/ cpf regulations 34
6. Registered or business address
7. Intended nature of business relations
8. Purpose of account or transaction (where accounts are not maintained and transactions are done by walk in/ occasional customers)
9. Type of account/ financial transaction/ financial service
10. Expected monthly credit turnover (amount and no. Of transactions
11. Normal or expected modes of transactions/ delivery channels
12. Wherever instructed/ advised, regulatory limits imposed such as: credit and debits/ deposit and withdrawals/ execution of financial transaction/ types of financial services allowed/ restricted.

Additional information in case of "trusts"

1. Whether the trust is a public trust or private trust including foreign and national trust
2. Trust deed whereby the trust has been created;
3. Details of settlor (this will also be available in the trust deed);
4. Objects of the trust (this will also be available in the trust deed)
5. Trustee of the trust (whether trustee is associated person of the settlor
6. Description of each class or type of beneficiary (this information may also be checked from trust deed)
7. Details of any possibility of influence of any other person on trustee regarding management and control of trust property
8. In the case of "private trust" if the beneficiary of a trust is also the beneficial owner of the trust, identification and verification of the beneficiary is required otherwise the name and cnic of each beneficiary of a trust should be obtained

Sectoral risk assessment of legal person and legal arrangements (lpla)

The sectoral risk assessment is a comprehensive process to help a country identify, assess, and understand the risks that arise from vulnerabilities of a particular sector that may facilitate money laundering or terrorist financing. The sectoral inherent vulnerability assessment consisted of an assessment of inherent ml/tf vulnerabilities of legal person and legal arrangements as a whole secto

The lpla risk assessment provide the following factors in this regard: • entities possessing following inherent characteristics are more likely to be abused for ml/tf purposes o having foreign companies/entities/trusts (whether registered in pakistan or not) as member/ shareholder/investor/partner/trustee; o trust sponsored from abroad; o those waqf properties who are recipient of any foreign charity or donor agencies. O having foreign bank accounts; • moreover, the use of foreign trusts might convey risks of unlawful practices owing to criminals making the most of the differing treatment of these legal arrangements by tax authorities and of the potential lack of coordination between them

Client identification procedures:

For individual persons for identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on kyc / cdd form or account opening form:

1. Full name as per identity document of the applicant
2. Date of birth, gender, marital status, religion, occupation, and qualification
3. residential status, nationality, country of residence
4. details of employer/business « cnic/nicop/snic/poc/passport number
5. existing mailing and permanent address
6. residential telephone number, office telephone number, fax number, mobile number and email address
7. Ntn and stn number
8. Nature and type of account
9. details of bank account
10. Details of investor account maintaining with cdc and details of sub account maintaining with other broker(s)
11. Source of income, gross annual income, sources of fund for stock market, expected value of investment
12. Knowledge of stock market and investment experience
13. Normal or expected mode of transaction

Client identification procedures for joint accounts:

In case of joint account, the customer due diligence measures on all of the joint account holders shall be performed as if each of them were individual customers of the PIML. In order to confirm the identity of the client, copies of the following documents will be obtained and retained for PIML's record:

1. Duly filled and signed account opening form (aof) by title and joint account holder(s)
2. Bank verification on aof from the bank where title account holder is maintaining a bank account.
3. Physical presence of title and joint account holder(s) at any of the PIML office along with valid original id document.
4. Attested copies of valid id document of title and joint account holder(s).
5. attested copies of valid id document of witnesses.
6. Local mobile number and/or email address.
7. Copy of zakat declaration (cz-50) duly attested by notary public as per the prescribed format for zakat exemption (optional).
8. For non-muslims PIML, written request for zakat non-applicability.
9. Power of attorney duly attested by notary public on prescribed format duly signed by all account holders (optional).
10. Copy of ntn certificate, if ntn is provided in aof.
11. copy of nicop for non-resident pakistanis, passport for foreigners duly attested by consulate office of pakistan or notary public of respective country.

12. bank statement or utility bill; or other residential identifying information.
13. bank references.
14. Proof of employment/ business
15. If the account is opened by the officer of government, special resolution / authority from the federal / provincial / local government department duly authorized by the ministry of finance or finance department of the concerned provincial or local government.

Client identification procedures for corporations, partnerships, trusts and other legal entities:

PIML will take reasonable steps to ascertain satisfactory evidence of an entity client's name and address, its authority to make the contemplated investment. For identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on kyc / cdd form or account opening form:

1. Full name as per identity document
2. Company registration / incorporation number
3. Date and country of incorporation
4. Date of business commenced
5. Residential status
6. Type of business
7. Name of parent company
8. Email, website and contact number
9. Registered and mailing address
10. Ntn number and sales tax number
11. Details of contact person and authorized person to operate the account
12. Nature and type of account
13. Details of bank account
14. Details of investor account maintaining with cdc and details of sub account maintaining with other broker(s)
15. Financial and general information including investment experience, expected value of investment, recent change in ownership of the company, customer type
16. Normal or expected mode of transaction PIML will obtain the following documents, as appropriate under the circumstances certified true copy of board resolution (specimen provided as per annexure "a") / power of attorney*
17. Certified true copies of constitutive documents of the applicant (memorandum & articles of association, act / charter / statute / by-laws / rules & regulations, certificate of incorporation, certificate of commencement of business, prospectus for modaraba, relevant licenses and registration issued by regulatory bodies etc.)
18. Certified copy of list of directors / trustee (if applicable) *

List of authorized signatories

List of nominated persons allowed placing orders

1. Attested copies of C.N.I.C/ N.I.C.O.P/ passports of the authorized signatories

2. Attested copies of C.N.I.C/ N.I.C.O.P/ passports of the contact person
3. attested copies of C.N.I.C/ N.I.C.O.P/ passports of the witnesses
4. certified copy of N.T.N. Certificate. (if exempted please provide exemption certificate)
5. Latest audited accounts of the company

Customer due diligence (cdd)

In order to apply and comply secp/cft/pf regulation PIML shall take steps to know who all their customers are:

- PIML shall not keep anonymous accounts or accounts in fictitious names.
- PIML shall take steps to ensure that their customers are who they purport themselves to be
- Shall verify the identification of a customer using reliable independent source documents, data or information including verification of cnics from nadra verisys/biometric.
- PIML shall identify and verify the customer's beneficial owner(s) to ensure that the understands who the ultimate beneficial owner is.
- Must assess each customer's risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for peps and other designated categories as per the regulations.
- Necessary minimum customer risk rating categories are: (a) high (b) standard (c) low iv. Standard cdd is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer
- Verification of that information. For beneficial owners the verification is according to the level of risk involved.
- EDD must be conducted when rp considers that the level of risk involved is such that edd should apply.
- Edd requires the collection and verification of the same information as standard cdd as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (sow) and source of funds (sof) of the customer
- Are entitled to ask customers all relevant cdd questions and may refuse business if the
- Should assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, rps should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.

Politically exposed persons (peps)

In relation to peps and their close associates or family members, PIML shall

Implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a pep or a close associate or a family member of a pep, both prior to establishing a

business relationship or conducting a transaction throughout the course of the business relationship. Aml/ cft/ cpf regulations 20

Obtain approval from the senior management to establish or continue business relations or want to execute financial transaction where the customer or a beneficial owner is a pep or subsequently becomes a pep, a close associate or family member of pep.

Establish, by appropriate means, the sources of wealth and the source of funds of customers and beneficial owners identified as pep, a close associate or family member of pep.

Conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as pep, close associate and family member of pep.

Conduct enhanced ongoing monitoring of the business relationship.

Categorizing an individual as pep after relieved from assigned services

FATF recommendation 12 defines a pep as someone who is or has been (but may no longer be) entrusted with a prominent public function. FATF guidance on peps recommends an open-ended approach (i.e., "once a pep – could always remain a pep").

Accordingly, handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. The risk-based approach requires that financial institutions and dnfbp's assess the ml/tf risk factors of a pep who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors include: the level of (informal) influence that the individual could still exercise and the seniority of the position that the individual held as a pep; or 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). In line with risk-based approach outlined above, the period for which a pep, family members and close associates of a pep, who is no longer entrusted with a prominent public function will be dependent on an assessment of the risk posed by that specific pep

Please note that solely relying on self-declaration by a customer may not be an appropriate customer due diligence (cdd) measure in terms of aml/cft regulatory framework. Rps should undertake steps to not only identify but also verify that the self-declaration is valid. Moreover, many customers would not be able to determine if they are indeed a pep, or not, for example because the customer may not be aware of the definition of a pep, family member or close associate of a pep as defined in secp regulations 3(g), (m) and (q). To establish pep status, rps should actively engage with customers and obtain information relevant to establish different elements of the pep definition. To do this effectively, well-trained staff and effective information gathering using 'pep search softwares' or through public databases such as election commission, parliamentarian's tax directories, public website/disclosures by public sector organizations and other public search portal etc. Should be used and document for record keeping purposes

High net worth individuals (hnwi)

High net worth individuals while an attractive customer for rps, can expose the rp to higher risk of financial transactions that may be illicit. There is no standard size of hnwi. Every rp knows to whom it is offering its products and services, and can establish criterion for hnwi applicable to their particular business. Ii. Rp should scrutinize hnwi customers to determine, whether they carry a higher risk of ml/ft and require additional due diligence measures. Such scrutiny must be documented and updated as part of the risk assessment of the rp.

Beneficial ownership:

If a customer has authorized another person, than the additional documentation are required. These include:

Attested copies of id document of authorized person

Power of attorney duly attested by notary public on prescribed format duly signed by all account holders with the following minimum information:

Name of authorized person and his/her relationship

Cnic / nicop / passport number

Contact details and email address

specimen signature of the person authorized.

Nature of business of beneficial owner

The authorized person is only allow to issue instruction for buy or sale of securities on behalf of client and all payments or receipt of funds must be made to or from the client own accounts and must include cnic number clearly marked on all payment cheques.

Mentally disordered person account:

Copy of applicable valid identity documents of mentally disordered person and court appointed manager under the applicable laws related to mental health.

Certified true copy of court order for appointment of manager for mentally disordered person.

Verification of identity document through bio-metric verifications from NADRA for both persons i.e. Mentally disordered person and the manager appointed by court.

Verification of court order from the concerned court (to be obtained by regulated person).

Account would be opened in the name of mentally disordered person and the same will be operated by the court appointed manager.

All cdd requirements/formalities should be conducted / completed for both persons.

In case of change of manager by the court, the cdd will be conducted for the new appointed manager by the regulated person afresh.";

Technology solution provider for facilitating the process of kyc/cdd e.g. Technology solution for facial/biometric id verification, screening solution providers etc. Can we treat reliance on such service providers being "reliance on third party" under regulation 24

PIML may use the services of a technology solution provider or outsourcing agency for verifying customer against the identity evidence provided, for example by using biometric solutions like facial recognition and liveliness detection to identify and authenticate during the on boarding process. However, it is important to consider the application of 'third party reliance'

FATF recommendation 17 requires that a third-party reliance can only be made in case the "third party" is: - a financial institution i.e. Should be subject to cdd and record-keeping requirements in line with recommendations 10 and 11, and be regulated, supervised or monitored - have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the cdd measures; this can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the cdd measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity. Hence the interpretive note to the recommendation 17 states that it does not apply to outsourcing or agency relationships. Guidance in this regard is provided in

'fatf guidance on digital identity'. Link: documents - fatf digital identity guidance.

Biometric verification system

Means the technology enabled system (verifiable from nadra or the relevant government authority) that allows financial institutions to obtain biometrics of the customers at the time of opening of account or conducting the transactions.

Nadra verisys:

Verifying a cnic in Pakistan Via Nadra cnic verification portal

Once the account registration process is completed, log-in to your account using the registered email address and password. ...

After logging in, accept the terms and conditions.

Make sure you have read everything carefully.

Next, click 'accept and continue'.

Identification Of Geographic Areas That May Fall Into High Risk Geography

The national risk assessment (nra) 2019 has provided a detail of high-risk geographies at the overall national level beside identifying characteristics of customers from towns and cities near porous borders areas and some other areas that may pose high risk for money laundering and terrorist financing. Determination of risk from a particular client will be based on a complete evaluation of the risk profile of the customer, not only in terms of geography, but also other components of risk that include type of customer, product/ services, and delivery channel being used

The assessment of such areas should be based on following metrics:

1. Foreign geographies
2. Fatf's monitored jurisdictions with respect to ml
3. Countries sharing porous borders with pakistan
4. High risk foreign jurisdictions for transnational tf risk
5. Countries on fatf's public statement
6. Countries having a hostile♣
7. Relationship with pakistan
8. Local/domestic geographies
9. Residence of designated and proscribed persons in a particular area
10. Terrorism hit areas / no. Of terrorist attacks
11. Locations of attempted transactions by proscribed/designated person
12. No. Of terrorism related strs bordering areas with hostile nations
13. Negative media reports
14. Sectarian violence
15. No. Of high risk npos and madrassas
16. In case screening of database leads to potential match with designated person, what are the actions required from the secp

As per section ii (2.4.1.1.i.v. & 2.4.1.1.i.vi.) Of the mofa guidelines on the implementation of unsc resolutions concerning tfs, travel ban, and arms embargo and section ii (4.6.1.1(a)vi.) Of mofa guidelines on the implementation of the unsc resolutions concerning tfs on faqs on aml/cft/pf obligation – 6th edition page 7 of 7 proliferation financing, secp re is required to immediately place a temporary freeze on the assets of the potential match and convey this information to secp for onwards sharing with the focal point at the ministry of interior for verification.

customer acceptance policy:

At first the transaction from a customer is accepted, as per policy criteria set under the heading of restricted personal list. After this the understanding of the customer's business and its activities help a lot to contribute to the company's overall reputation, concentration, operations and legal risk management through the detection of potentially harmful activities.

Targeted financial sanctions (tfs) under unsc resolutions

Tfs obligations are provided under the following legal instruments: a) united nations (security council) act, 1948 (unsc act) b) united nations security council (freezing and seizure) order, 2019 c) statutory regulatory orders (sros) issued under unsc act d) anti-terrorism act, 1997 (ata) e) notifications issued under ata f) aml act, 2010 and rules, regulations and directives issued thereunder. 2. What are the unsc

and domestic sanctions regimes in pakistan? The government of pakistan under the unsc act gives effect to the decisions of united nations security council (unsc) whenever the consolidated list is updated maintained by the relevant sanctions committee. The details of sanctions imposed by the unsc along with the consolidated lists are available on the unsc sanctions committees' websites at the following links:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

https://scsanctions.un.org/search/ c) https://www.un.org/securitycouncil/sanctions/1267

https://www.un.org/securitycouncil/sanctions/1988
https://www.un.org/securitycouncil/sanctions/1718
https://www.un.org/securitycouncil/content/2231/background 3. Where can i find notifications issued by the ministry of foreign affairs on united nations security council resolutions? Mofa issues sros to provide legal cover for implementing sanction measures under unsc resolutions. These sros in respect of designated individuals/ entities require assets freeze, travel ban and arms embargo in addition to other measures in accordance with the unsc resolutions, and are available publicly at the following links: a) http://mofa.gov.pk/unsc-sanctions/ b) http://www.secdiv.gov.pk/page/sro-unscr-sanctions e)

A) https://nacta.gov.pk/proscribed-organizations-3/

B) https://nacta.gov.pk/pp/

C) https://nfs.punjab.gov.pk/

Sahulat accounts

All resident pakistani individual customers can open a sahulat account in a single capacity.

Can sahulat account be opened using online account opening facility

Provide digital /online account opening facilities to their customers

Maximum investment amount that can be maintained in a sahulat account is pkr 800,000.

Sahulat acount holder can only trade in regular market.

Trading in leverage and futures markets is not permitted for a sahulat acount holder. 5.

Computerized/smart national identity card (cnic/snic may be used as a proof of identity for opening of sahulat account

No additional document is required from customer for establishing his accounts can be classified as low risk normal accounts, and

same level ofsimplified due diligence (sdd) will be applied.

Restricted personal list:

The unsc sanctions committee, maintains the consolidated list of individuals and entities subject to title sanctions covering assets freeze, travel ban and arms embargo set out in the unsc resolution 1267 (1999) and other subsequent resolutions, concerning isil (daesh) / al-qaida and taliban and their associated individuals.

Government of pakistan publishes statutory regulatory orders (sros) under the united nations (security council) act, 1948 in the official gazettes to give effect to the decisions of the unsc sanctions committee and implement unsc sanction measures in pakistan. The regularly updated consolidated list is available at the un sanctions committee's website, at following link;

https://www.un.orq/sc/suborq/en/sanctions/1988/mateiials

https://www.un.0rg/sc/suborq/en/sanctions/1718/materials

http://www.un.org/en/sc/2231/iist.shtml

https://www.un.org/sc/suborq/en/sanctions/1718/prohibited-items

The ministry of interior issues notifications of proscribed individuals /entities pursuant to the antiterrorism act, 1997, to implement sanction measures under unscr 1373(2001), and the regularly updated consolidated list is available at the national counter terrorism authority's website, at following ink;

ittp://nacta.qov.pk/proscribed-orqanizations/ a/

Here there is a true match or suspicion, PIMLs shall take steps that are required to comply with the sanction's obligations including freeze without delay and without prior notice, the funds or other assets of designated persons and entities and reporting to the commission, if they discover a relationship that contravenes the unscr sanction or a proscription.

Pakistan's national refugee policy Afghanistan,

PIML shall not open afghan refugee account for trading.

Prohibition of personal accounts for business purposes

PIML shall not allow personal accounts to be used for business purposes except proprietorships, small businesses and professions where constituent documents are not available and the res are satisfied with kyc profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer.

Risk assessment and applying a risk based approach

PIML shall comply with these regulations and other instructions issued on risk based approach to aml/ cft

The first step in assessing ml/tf/pf risk is to identify the risk categories, i.e. Customers, countries or geographical locations, products, services, transactions and delivery channels

In order to document the identified ml/ tf/ pf risks, PIML shall ensure an entity level internal risk assessment report (irar). Irar shall cover ml/ tf/ pf risks including transnational tf risks and other emerging risks to and from

Shall identify, assess, and understand ml/ tf/ pf risks at entity level for customers, products, services, delivery channels, technologies, and their different categories of employees etc.

Shall take into account results of national risk assessment (nra) shared with sbp res, major international/ domestic financial crimes and terrorism incidents that have probability of posing ml/ tf/ pf risks to the entity itself,

Shall assess effectiveness of existing aml/ cft/ cpf policies/ controls/ obligations/ preventive measures including str/ ctr and tfs etc.

Shall be used for evaluating residual ml/ tf/ pf risks about which sbp res have to take decisions i.e. On-boarding of customers, allowing execution of financial transactions, provision of financial service, launching of product, use of technology, and initiating business and operation in particular geographical location, etc.

Shall formulate policy for application of sdd, cdd and edd in light of levels of ml/ tf/ pf risks identified as low, medium, or high time to time

Shall ensure that irar is a dynamic and up-to-date document, by periodically updating their irar when circumstances change or relevant new threats emerge shall be presented to the bod for approval.

It shall include recommendations for the bod along with a time bound action plan for mitigation of ml/ tf/ pf risks and ensuring effective aml/ cft/ cpf policies/ procedures/ controls/ obligations/ preventive measures including but not limited to str/ ctr and tfs.

Should cover measures for improvement in understanding of ml/ tf/ pf risks of employees, senior management and bod, and adequacy of resources i.e. Systems and human resource etc.

Shall develop aml/ cft/ cpf policies/ procedures/ controls/ obligations/ preventive measures considering their size, nature of business and complexities of operations.

Shall ensure adequate monitoring mechanism to assess ml/ tf/ pf risks and adequacy of aml/ cft/ cpf controls including str/ ctr and tfs through internal audit, transaction monitoring and name screening

The policies/ controls/ procedures/ preventive measures shall be developed/ updated/ implemented proportionate to level of ml/ tf/ pf risks as evaluated

The policies shall be approved by bod and controls/ procedures/ preventive measures shall be approved by senior management

The ultimate responsibility of ensuring effective aml/ cft/ cpf controls lies on bod. Therefore, bod shall ensure adequate, reliable, periodic management information system, from senior management, for ensuring effective oversight, monitoring and accountability.

Simplified due diligence measures

PIML may conduct sdd in case of lower risks identified through adequate analysis and assessment and in line with the latest national risk assessment.

While determining whether to apply sdd, rps should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity as mentioned in the latest national risk assessment.

PIML shall not apply sdd whenever there is a suspicious of ml/tf/pf.

Person with mental disorder

"person with mental disorder" means a person with mental illness as defined in the applicable laws on mental health; (f) after clause (pa), the following new clause shall be inserted, namely: - "(pb) "proliferation financing" means the financing of proliferation of weapons of mass destruction; and (g) after clause (q), the following new clauses shall be inserted, namely: - "(qa)

Enhanced due diligence

(regulation 21 ml/tf/pf risk or in cases of unusual or suspicious activity an increased level of cdd is required. This includes situations where the rp consider (based on risk assessment) that the level of risk involved is such that enhanced cdd should apply. In such situations the rp need to use increased or more sophisticated measures to obtain and verify customer's details

PIML should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Iii. In case of low risk customer, the regulated person should obtain information of source of income however, no specific evidence is required. In case of high-risk customers, where edd is required, evidence of source of income may be requested from the customer

List of examples of appropriate information and/or supporting documentation required to establish source of wealth and funds is as follows

1. (any one of the documents may be obtained): a) employment income:
2. Last month/recent pay slip; annual salary and bonuses for the last couple of years; • confirmation from the employer of annual salary; income tax returns/ wealth statement. B) business income/ profits / dividends
3. copy of latest audited financial statements;
4. rental statements • dividend statements c) savings / deposits/ assets/property:
5. statement from financial institution
6. bank statement

7. Taxation returns • accountant's statements
8. property ownership certificate • share certificates d) inheritance:
9. succession certificate. E) sale of property/ business:
10. copy of sale agreement/title deed f) loan
11. loan agreement g) gift: • gift deed;
12. source of donor's wealth;
13. Certified identification documents of donor. H) other income sources:
14. Nature of income, amount, date received and from whom along with appropriate supporting documentation.
15. Where there nature of income is such that no supporting documentation is available (for eg. Agricultural income) bank statement may be obtained

High net worth individuals (hnwis)

High net worth individuals while an attractive customer for rps, can expose the rp to higher risk of financial transactions that may be illicit. There is no standard size of hnwi. Every rp knows to whom it is offering its products and services, and can establish criterion for hnwi applicable to their particular business. Page 15 of 63 ii. Rp should scrutinize hnwi customers to determine, whether they carry a higher risk of ml/ft and require additional due diligence measures. Such scrutiny must be documented and updated as part of the risk assessment of the rp.

Record keeping procedures regulation statutory requirements under aml/cft legislations amla:

The amla section 2 defines record as follows: (xxxii) "record" includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed. The amla section 7c states the general record keeping requirements:

PIML shall ensure compliance with the following record keeping instructions for maintaining record of documents and information obtained digitally or in hard form for cdd and other purposes.

1. The records of identification data obtained through cdd process including but not limited to copies of identification documents, account opening forms, kyc forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a period of ten years after the business relationship is ended.
2. PIML shall maintain all necessary records of 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)
3. Shall also keep and maintain all record related to strs and ctrs filed by it for a minimum period of ten years from completion of the transaction.
4. the records shall be sufficient 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 to provide, when necessary, as an evidence if required by leas and aml/ cft/ cpf regulations other relevant authorities as per law.

5. The transactions' records may be maintained in paper or electronic form or on microfilm, provided it is admissible as evidence in a court of law.
6. where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority, sbp res shall retain such records until the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained.
7. PIML shall satisfy, as soon as possible, any enquiry or order received from the relevant competent authorities, including leas and fmu for supply of information and records as per law.
8. PIML shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through cdd and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship.
9. Further, section 7(4) requires the record to be maintained for a period of 10 years for submitted strs and ctrs after reporting of the transaction
10. PIML shall keep and maintain all record related to suspicious transaction reports and ctrs filed by it for a period of at least ten years after reporting of transaction under sub-sections (1), (2) and (3)." Secp aml/cft regulations: section 26 requires rps to maintain the required records as stated in section 7c of the amla. I.

PIML should ensure that all information obtained in the context of cdd is recorded. This includes:

A. Documents provided to the rp when verifying the identity of the customer or bo;
B. Verification of cnic through nadra verisys/ biometric;
C. Transcription into the rp's own it systems of the relevant cdd information. Ii. The rp will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification. Iii.

PIML maintain a comprehensive record of aml/cft reports with respect to internal enquiries and reporting to fmu.

Such documentation may include:

a) The report itself and all its attached information / documents in copy;
b) The date of the report;
c) The person who made the report and the recipient;
d) Any decision based on the str for the specific customer or a group of customers;
e) Any updating or additional documentation taken based on the report; and
f) The reasoning underlying the decisions taken

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 PIML will 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.

The PIML will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification.

The PIML will provide, when requested by the commission, investigating or prosecuting agency and fmu, any record within 48 hours after the request has been made or such time as may be instructed by the relevant authority

reporting suspicious transactions statutory requirements under aml/cft legislations amla: under section 7 (1) of the amla,

The PIML entity (as per section 2 (xxxiv) and 2 (xii) of amla) must file an str to the fmu promptly for a conducted or attempted transaction if the rp knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part:

a) involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;
b) is designed to evade any requirements of this act;
c) has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction; or
d) involves financing of terrorism, including fund collected, provided, used or meant for, or otherwise linked or related to, terrorism, terrorist acts or organizations and individuals concerned with terrorism: under section 34 disclosure of information.

The directors, officers, employees and agents of any reporting entity or intermediary which report an str or ctr pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with regulations made hereunder.

Internal controls

Shall recommend measures to bod through time bound action plan to ensure adequate introduction and implementation of aml/ cft/ cpf controls/ preventive measures to mitigate ml/ tf/ pf risks

Development and keeping the entity's business strategy up to date including entity risk appetite.

Development and keeping the entity's policy framework approved by board updated with regard to mitigation of emergent ml/ tf/ pf risks.

Development and keeping up to date aml/ cft/ cpf compliance program/ procedure manuals/ sops approved by senior management, for ensuring aml/ cft/ cpf controls (preventive measures) including implementation of tfs related to tf & pf and reporting of strs/ ctrs.
Secp aml/cft regulations: section 19(4) merely reminds of their filing obligations as prescribed under section 7 of the amla.

PIML should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose. Activities requiring further enquiry may fall into one or more of the following:

a) Any unusual financial activity of the customer not in line with the customer's profile;

b) Any unusual transaction in the course of some usual financial activity; (c) any unusually-linked transactions;
c) Any unusual method of settlement;
d) Unusual or disadvantageous early redemption of an investment product;
e) Unexplained unwillingness to provide the information requested

Payment mechanism:

For amounts greater than pkr 25,000

The PIML shall accept from / pay to the account holder(s) through "a/c payee only" crossed cheque, bank drafts, pay orders or other crossed banking instruments in case if amounts exceeds rs. 25,000/=.

Electronic transfer of funds through banks would be regarded as good as cheque. The PIML shall be responsible to provide the receipt to the account holder(s) in the name of account holder(s) duly signed by authorized agents / employee of the broker and the account holder(s) shall be responsible to obtain the receipt thereof.

for amounts less than or equivalent to pkr 25,000

In case of cash dealings, proper receipt will be taken and given to the account holder(s), specifically mentioning if payment is for margin or the purchase of securities. The PIML shall immediately deposit in its bank accounts all cash received in whole i.e. No payments shall be made from the cash received from clients.

Exceptional circumstances

However, in exceptional circumstances, where it becomes necessary for the PIML to accept cash in excess of rs. 25,000/=, the PIML shall immediately report within one business day, such instances with justification thereof, to the stock exchange in accordance with the mechanism prescribed by the exchange.

Copies of these payment instruments including cheques, pay orders, demand drafts and online instructions shall be kept in record for a minimum period of five years.

Secp regulations allow a mechanism for third party reliance on cdd. PIML may avail this facility after complying with the relevant requirements as specified in regulation 24, reliance on third parties". So, if banks share their cdd, and the PIML is in compliance with requirements of regulation 24, the PIML can rely on it, otherwise, the PIML must carry out its own customer due diligence measures

General reporting procedures:

The compliance officer on behalf of the organization is nominated to receive disclosures under this regulation

Anyone in the organization, to whom information comes in the course of the relevant business as a result of which he suspects that a person is engaged in money laundering, must disclose it to the compliance officer

where a disclosure is made to the compliance officer, the officer must consider it in the light of any relevant information which is available to PIML and determine whether it gives rise to suspicion

where the compliance officer determines in consultation with the senior management, the information must be disclosed to the regulatory authority after obtaining an independent legal advice

Reporting of suspicious transaction/currency transaction report:

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual and the PIML should put "on enquiry".

PIML's shall also pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Where the enquiries conducted by the PIML do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the aml/cft compliance officer.

Activities which should require further enquiry may be recognizable as falling into one or more of the allowing categories:

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
g) If the PIML decides that a disclosure should be made, the law require the PIML to report PIML 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.
h) PIML is required to report total number of strs filed to the commission (secp) on bi-annual basis within seven days of close of each half year. The compliance officer should ensure prompt reporting in this regard.

i) PIML is also obligated to file currency transaction report (ctr), for a cash-based transaction involving payment, receipt, or transfer of rs. 2 million and above.
j) PIML will maintain a register of all reports made to the fmu. Such registers should contain details of:
k) The date of the report
l) The person who made the report
m) The person(s) to whom the report was forwarded
n) Reference by which supporting evidence is identifiable

Wire transfers

The requirement under this regulation-11 shall apply, functions and powers prescribed under relevant law of secp/aml/cft/pf, regulation 2023.

PIML shall follow the instruction of AML/CFT/PF ,2020 Regulation regarding the wire transaction.

New technologies

Review of products and services including new technologies

PIML shall identify and assess the ml/ tf/ pf risks that may arise in relation to the development of new products, services and business practices including delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products, especially those that have vulnerability with regard to ml/ tf/ pf risks specially identity theft, anonymity and cyber-crimes.

Furthermore, ml/ tf/ pf risk assessments shall be undertaken prior to the launch or use of such products, services and business practices and technologies.

Appropriate measures shall be taken to manage and mitigate the identified risks. Aml/ cft/ cpf regulations 27 required ensuring automation of business and operational processes and use of systems for risk management and controls in area of aml/ cft/ cpf.

Further, wherever required, sbp res shall use mitigation measures in digital channels against identity theft such as live picture or video, electronic/ digital signature, two-factor authentication through email and registered on name mobile number, and biometric verification of customers. In this regard, sbp res shall ensure compliance with prevailing laws and regulatory instructions.

PIML as per requirement of their business and operational models shall make use of technology and upgrade their systems and procedures in accordance with the changing profile of various ml/ tf/ pf risks.

Shall implement automated transaction monitoring systems (tms) capable of producing meaningful alerts based on pre-defined parameters/ thresholds and customer profile, for analysis and possible reporting of suspicious transactions.

Shall establish criteria in their aml/ cft/ cpf policies and/ or procedures for management of such alerts. The adequacy of staff posted for effective monitoring and reporting of strs is a critical factor of cdd. Sbp res shall place adequate number of analysts for monitoring and reporting purpose.

Required to obtain prior approval from relevant department, before offering any new product/ service.

Record-Keeping Procedures

As per guidelines provided by secp:

- PIML ensure that all information obtained in the context of kyc / cdd / edd is recorded. This includes both;
- Recording the documents, the PIML is provided with when verifying the identity of the customer or the beneficial owner, and
- Transcription into the PIML's own it systems of the relevant cdd information contained in such documents or obtained by other means.
- PIML should 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: or prosecution of criminal activity.
- Where there has been a report of a suspicious activity or the PIML 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 should be retained until confirmation is received that the matter has been concluded.

Records relating to reporting by securities broker will generally comprise:

a) Monthly report prepared on reporting by securities broker under the circular no.10/2017 of secp.
b) Records relating to verification of identity will generally comprise:
c) A description of the nature of all the evidence received relating to the identity of the verification subject; and
d) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.
e) Records relating to transactions will generally comprise:
f) Details of personal identity, including the names and addresses of the customer;
g) The beneficial owner of the account or product; and
h) Any counter-party details of securities and investments transacted including:
i) The nature of such securities/investments;
j) Valuation(s) and price(s);
k) Memoranda of purchase and sale;
l) Source(s) and volume of funds and securities;
m) Destination(s) of funds and securities;
n) Memoranda of instruction(s) and authority(ies);
o) book entries;
p) Custody of title documentation;
q) The nature of the-transaction;
r) The date of the transaction;
s) The form (e.g. Cash, cheque) in which funds are offered and paid out.
t) policy review period:
u) call recording data

v) trade log data
w) screening of SRO,S data
x) back office system data
y) NCCPL screening data
z) CDC setup report
aa) All relevant data preserved and maintain in order to comply the instruction of SECP/AML/CFT/PF Regulation,2020 up to 2023.

The SECP-AML/CFT/PF policy & procedures will be reviewed on annual basis and updated as and when required.

Approval from board of directors:

This policy has been approved by the board of directors on October, 2023 and access has been provided to the relevant employees of PIML.

Effective date:

This policy shall become effective from the October, 2023.