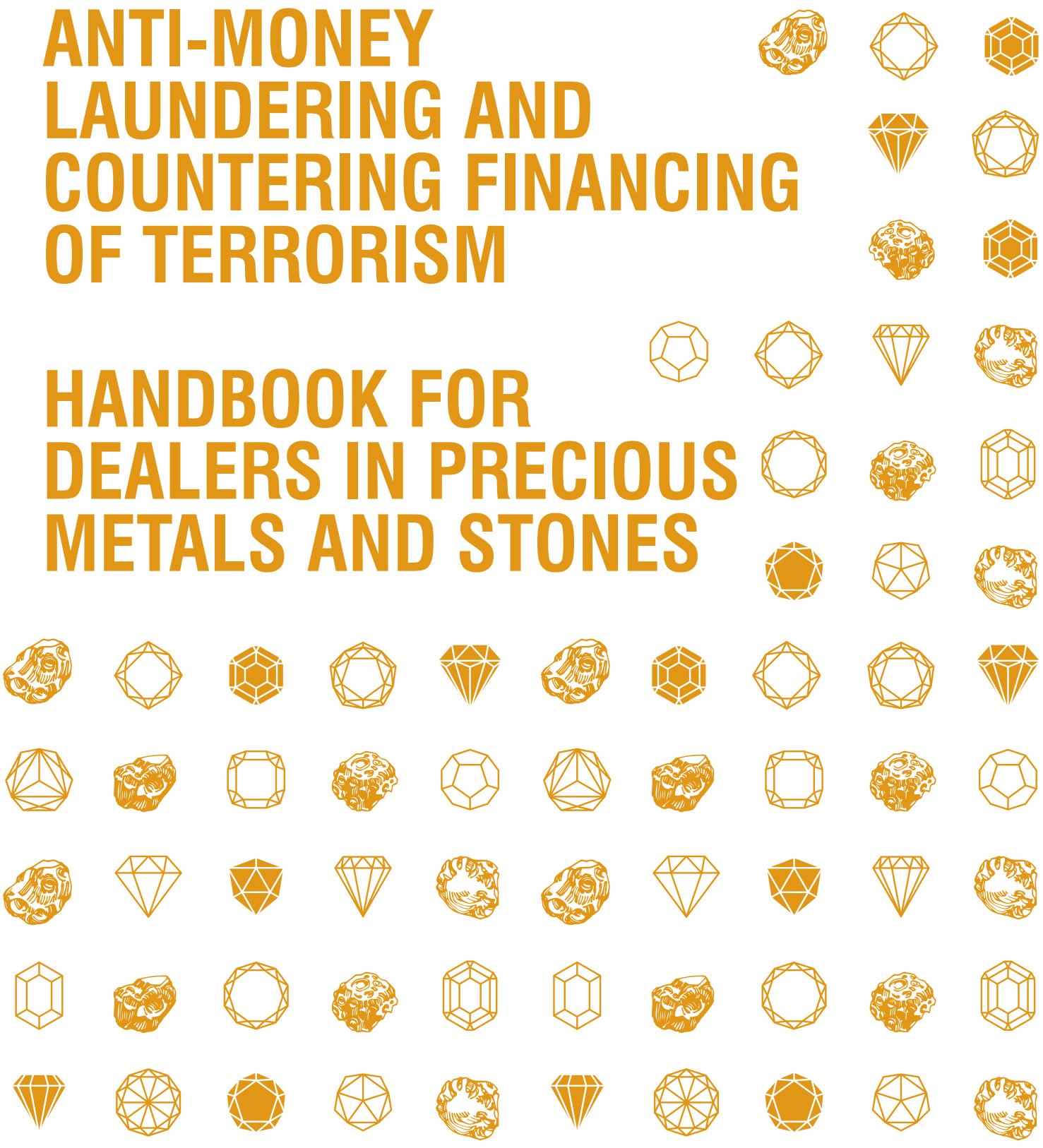
ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

HANDBOOK FOR DEALERS IN PRECIOUS METALS AND STONES



DISCLAIMER

This Handbook is designed to assist dealers in precious metals and stones in the implementation of the requirements related to Anti-Money Laundering/Countering Financing of Terrorism but is not intended to be a substitute for the respective laws, rules, and regulations on the same. Should discrepancies arise between the text of this Handbook and the text of the laws, rules, and regulations, the official text of the laws, rules, and regulations will always prevail. Furthermore, a dealer in precious metals and stones should utilize the Handbook in light of his or her professional judgment and the facts and circumstances involved, and each particular client relationship. Each dealer in precious metals and stones is encouraged to develop their own manual for the execution of their role. The Research Society of International Law and the American Bar Association Rule of Law Initiative disclaim any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of the Handbook.

ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

HANDBOOK FOR DEALERS IN PRECIOUS METALS AND STONES

RSIL | Research Society of International Law
IMPARTIAL ANALYSIS • LEGAL SOLUTIONS

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AMLA	Anti-Money Laundering Act, 2010
AML/CFT	Anti-Money Laundering/Countering Financing Of Terrorism
CDD	Customer Due Diligence
CTR	Currency Transaction Report
DNFBP	Designated Non-Financial Businesses and Persons
DNFBP Regulations	Federal Board of Revenue Anti-Money Laundering and Countering Financing of Terrorism Regulations for Designated Non-Financial Businesses and Persons 2020
DPMS	Dealers in Precious Metals and Stones
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FBR	Federal Board of Revenue
FMU	Financial Monitoring Unit
ML	Money laundering
MoFA	Ministry of Foreign Affairs
MoI	Ministry of Interior
NACTA	National Counter Terrorism Authority
Sanctions Rules	Sanctions Rules, 2020
SBP	State Bank of Pakistan
SECP	Securities & Exchange Commission of Pakistan
Simplified DD	Simplified Due Diligence
SRB	Self-Regulatory Body
Standard DD	Standard Due Diligence
SRO	Statutory Regulatory Order
STR	Suspicious Transaction Report
TFS	Targeted Financial Sanctions
TF	Terrorism Financing

1. INTRODUCTION

ML is the processing of assets generated by criminal activity with the intent to obscure the link between the funds and their illegal origins. This could be done through sale and purchase of a property. TF is the use of funds to carry out acts of terrorism.[1] The sources of TF may be legitimate or illegitimate, for example, sale of property or sale of drugs, respectively.

ML and TF continue to pose significant threats to Pakistan and its economy. Over the past several years, Pakistan has been advised by FATF, the international body that sets recommended standards for fighting ML/TF, that Pakistan's AML/CFT regime is significantly deficient. The FATF recommendations apply to the precious metals and stones sector, amongst other professionals.

Pakistan has a strong commitment at the political, government, and industry levels to play an active role in the international fight against ML/TF. Accordingly, the authorities of Pakistan take a strong position against any business that assists in ML/TF. DPMSs must recognize the role that they must play in protecting themselves from involvement in ML/TF and in protecting Pakistan's reputation of integrity.

DPMSs are likely to encounter ML activities in the course of their business activities. Criminals and terrorists are likely to use precious metals and stones for their illegal activities owing to a number of factors. They can be of very high value, yet very small and therefore very easy to carry, transport and conceal. Transferring ownership does not require any formal registration process, as is the case with real estate, motor vehicles, or shares ownership. The holder of the precious metal or stone is the owner which can be held anonymously without any record-keeping requirement. Gold can particularly be used to launder illegal earnings being a universally accepted form of currency. Thus, DPMSs must be aware of relevant AML/CFT obligations to ensure that their activities are not exploited by criminals.

DPMSs would not want to be a party to such activities. If DPMSs are not vigilant, the precious stone or metal transaction that they arrange may lead to access to criminal funds, which may be used to commit serious crimes. This includes terrorist attacks where innocent lives may be lost. DPMSs can play a part in combating ML/TF by complying with the various AML/CFT obligations as explained in this Handbook. This includes appointing compliance officers at a management level, conducting training programs, and implementing policies and procedures to ensure their compliance with the law.

1. Various legal systems, government and international bodies have used different definitions of the term 'terrorism', therefore, there is no universal definition.

1.1. OBJECTIVES OF THE HANDBOOK

This Handbook will assist DPMSs in complying with the requirements of the AML/CFT laws, rules, and regulations to prevent Pakistan's precious metals and stones system and operations from being abused for ML/TF. The particular objectives of the Handbook are to:

- Outline the requirements of AMLA and DNFBP Regulations to be followed by DPMSs;
- Assist DPMSs in complying with the requirements of such laws and regulations;
- Emphasize the responsibilities of compliance officers and key personnel belonging to the precious metals and stones sector;
- Promote the use of a proportionate risk-based approach; and
- Provide practical guidance on CDD, Simplified DD, Standard DD, EDD, filing of STRs and CTRs, and record keeping.

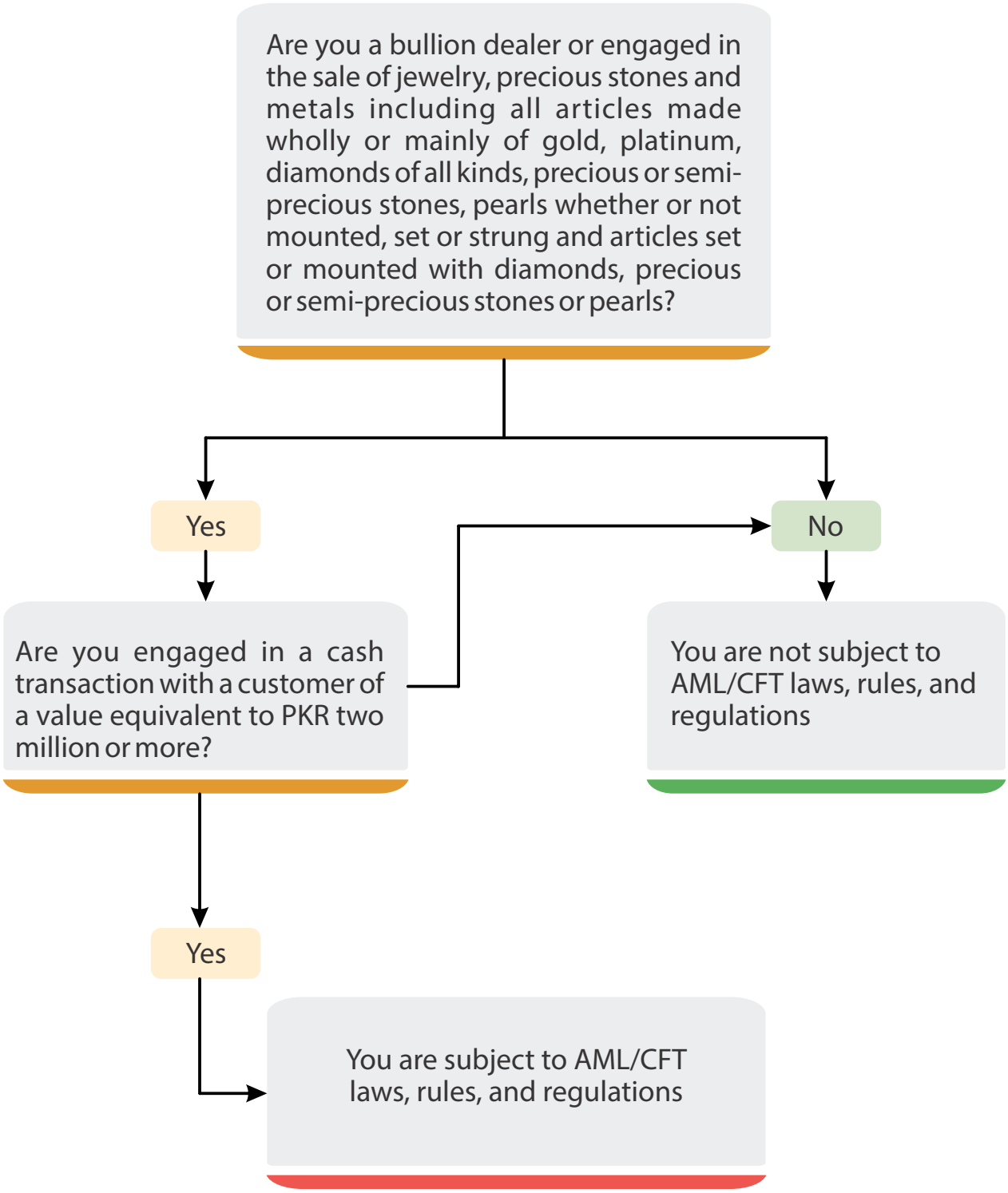
The Handbook does not include guidance on all the ML/TF risks a DNFBP may face and is not the only source of guidance on ML/TF. DPMSs are reminded that guidance produced by FATF, FMU, and FBR may also be relevant and useful.[2]

1.2. IS THIS HANDBOOK FOR YOU?

The AML/CFT laws, rules, and regulations, and hence this Handbook, would only be applicable to you if you are a DPMS which includes jewelers and gem dealers, and a jeweler has in turn been defined to mean a person who is a bullion dealer or engaged in the sale of jewelry, precious stones and metals including all articles made wholly or mainly of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semi-precious stones or pearls, when they engage in a cash transaction with a customer of a value equivalent to PKR two million or more.[3]

The following diagram will help you to determine whether your precious metal and/or stone business is subject to AML/CFT laws, rules, and regulations:[4]

2. See Annexure A for a non-exhaustive list of resources.
3. As defined in Section 2(xii)(b) AMLA read with Clause 2(1)(k) DNFBP Regulations.
4. This diagram is based on the definition of DPMS provided in Section 2(xii)(b) AMLA read with Clause 2(1)(k) DNFBP Regulations.



If you answer 'yes' to the first and second questions in the foregoing diagram, you would be subject to the AMLCFT laws, rules and regulations, and this Handbook is for you.

1.3. SANCTIONS FOR NON-COMPLIANCE

The legal requirements described in this Handbook are requirements prescribed by the AMLA and the Sanctions Rules. Non-compliance with the legal requirements can be addressed with the following instruments:

(a) Impose a monetary penalty up to PKR 100 million per violation, in accordance with the risk-based penalty scale;
(b) Impose any condition, limitation, or restriction on the reporting entity's business or product offerings, as it considers appropriate;
(c) Revoke license or de-registration of the reporting entities as applicable;
(d) Impose a temporary or permanent prohibition on any natural person who holds an office or position involving responsibility for taking decisions about the management of the reporting entity, including but not limited to:
    (i) Issuing a written warning;
    (ii) Imposing a temporary suspension; or
    (iii) Removal from service.
(e) Issue a statement of censure/warning/reprimand;
(f) Issue a direction to the person to undertake any given actions, including but not limited to:
    (I) Comply with the requirements within a specified time period through a remedial plan;
    (ii) Conduct internal inquiries; or
    (iii) Take disciplinary action against directors, senior management, and other officers.
(g) Impose any other sanction permitted under the enabling legislation and any rules, regulations, or directives issued thereunder.

Particularly for failure to file STRs or for providing false information, the punishment is imprisonment for a term which may extend to five years, a fine which may extend to five hundred thousand rupees, or both.[5]

It is also an offence for the directors, officers, employees and agents of any reporting entity or intermediary which report an STR or CTR or any other authority, to disclose, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with any regulations made under the AMLA. The punishment is imprisonment for a term which may extend to five years, or a fine which may extend to two million rupees, or both.[6]

5. Section 33 AMLA.
6. Section 34 AMLA.

Sanctions may be imposed on a "person" which means a reporting entity, directors, senior management, or officers in similar positions of that reporting entity.[7] "Senior management" means the Chief Executive Officer, Managing Director, Deputy Managing Director, Chief Operating Officer, Company Secretary, Chief Financial Officer, Chief Compliance Officer, Chief Regulatory Officer, and any holder of such positions by whatever name called.[8]

In the case of smaller reporting entities or when such entities are a partnership or a branch, there may not always be a Board or even the aforementioned officers. In the absence thereof, senior management would mean an officer or employee with sufficient knowledge of the reporting entity's ML/TF risk exposure and sufficient seniority and authority to take decisions affecting its risk exposure.

7. Rule 2(1)(d) Sanctions Rules.
8. Rule 2(1)(e) Sanctions Rules.

2. FURNISHING INFORMATION

2.1. LEGAL REQUIREMENTS

2.1.1. Filing of Suspicious Transaction Reports and Currency Transaction Reports

The law requires every reporting entity to file with the FMU promptly, a report of a suspicious transaction conducted or attempted by, at, or through such reporting entity, if it 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 funds collected, provided, used, or meant for, or otherwise linked or related to, terrorism, terrorist acts or organizations, and individuals concerned with terrorism.[9]

According to the law, all cash-based transactions of two million rupees or above, involving payment, receipt, or transfer are to be reported to FMU by filing a CTR, which is to be filed by the reporting entities with the FMU immediately, but not later than seven working days, after the respective currency transaction.[10]

Furthermore, any government agency, autonomous body, oversight body for SRB, AML/CFT regulatory authority, domestic or foreign, may share intelligence or report their suspicions within the meaning of the STR or CTR to the FMU in the normal course of their business and the protection provided under Section 12 of the AMLA shall be available to such agency, body or authority.[11]

Every reporting entity is required to keep and maintain all records related to STRs and CTRs filed by it for a period of at least ten years after reporting any of the aforementioned transactions.[12]

9. Section 7(1) AMLA.
10. Section 7(3) and 2(xi) AMLA, SRO No.73 (I)/2015 dated 21.01.2015.
11. Section 7(2) AMLA.
12. Section 7(4) AMLA.

These obligations under have effect notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any other law or written document.[13] Moreover, notwithstanding anything contained in any other law for the time being in force, any STRs required to be submitted by any person or entity to any investigating or prosecuting agency under the AMLA shall be solely and exclusively submitted to FMU to the exclusion of all others.[14]

2.1.2. Targeted Financial Sanctions

Specific individuals and entities identified as contributing to a particular threat to, or breach of, international peace and security can be imposed with TFS under national and international law.

The law imposes a duty to implement policies and procedures to ensure their compliance with the provisions of the AMLA, and any orders, rules, or regulations made thereunder, that impose TFS obligations upon reporting entities.[15]

If during the process of screening or monitoring of customers a positive or potential match is found then the DPMS shall:

(a) Freeze without delay in accordance with the respective SRO;
(b) Not provide any services or property or any other related funds in accordance with the respective SRO; or
(c) Reject the transaction, attempted transaction, or the customer if the relationship has not commenced.[16]

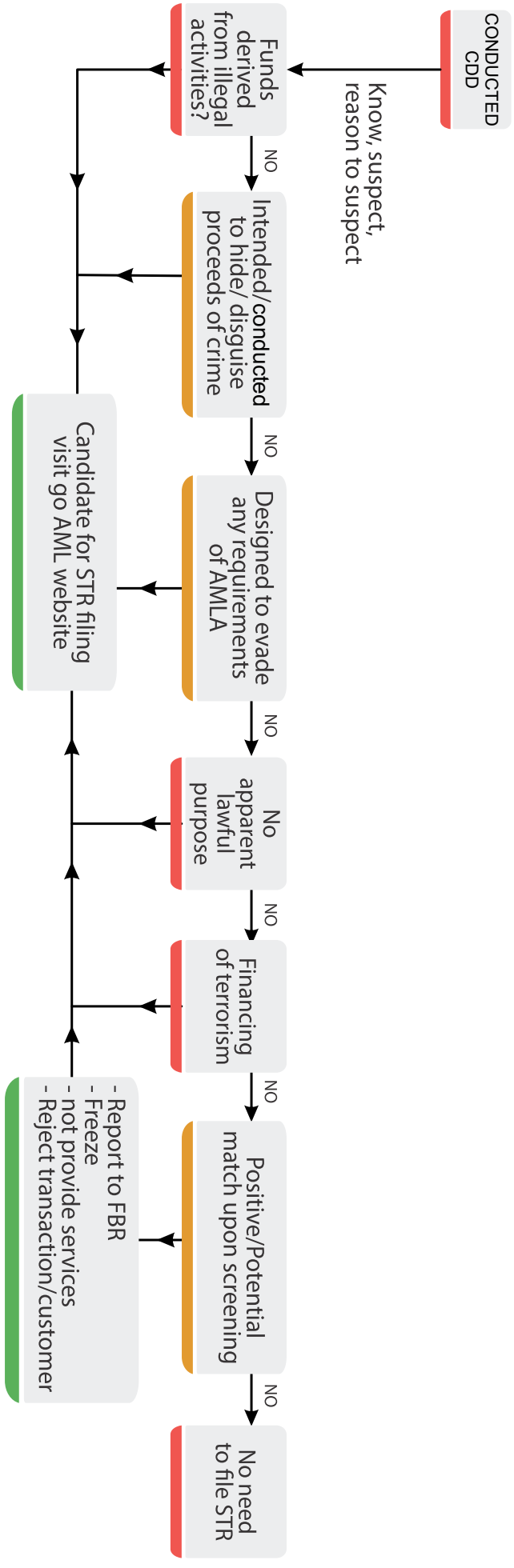
In all the cases mentioned above, the DPMS shall report to the FBR and FMU by filing an STR and/or CTR.[17]

2.2. Operating Procedures For Suspicious Transaction Reports

2.2.1. Should you file a Suspicious Transaction Report?

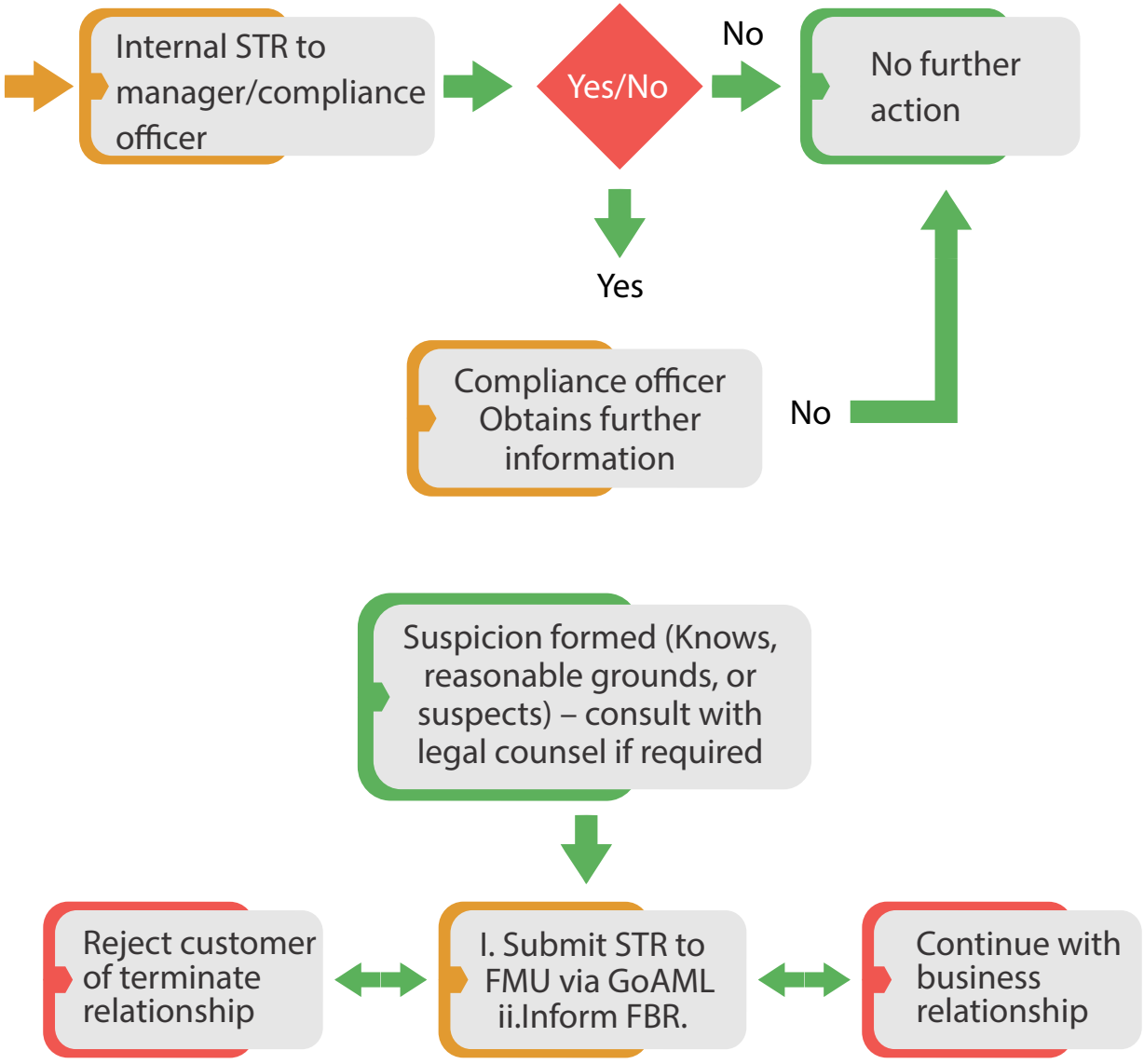
The following diagram is a decision-making framework for whether you should file an STR.

13. Section 7(5) AMLA.
14. Section 7(6) AMLA.
15. Section 7H AMLA.
16. Regulation 13(1)(b) DNFBP Regulations.
17. Regulation 13(1)(c) DNFBP Regulations.


CONDUCTED CDD
Know, suspect, reason to suspect
Funds derived from illegal activities?
NO
Intended/conducted to hide/ disguise proceeds of crime
NO
Designed to evade any requirements of AMLA
NO
No apparent lawful purpose
NO
Financing of terrorism
NO
Positive/Potential match upon screening
NO
No need to file STR
Candidate for STR filing visit go AML website
- Report to FBR
- Freeze
- not provide services
- Reject transaction/customer

2.2.2. Internal Reporting Procedure

The process map below illustrates the internal reporting procedure that DPMSs should follow with regard to filing of STRs



2.2.3. Types of Suspicious Transaction Reports

(i) STR-A

STR-A is to be reported when parties (person, account, or entity) are involved in any suspicious activity, which does not involve a transaction or transmission of funds. In this report, the suspected party details must be provided in the "Person/ Account/Entity" section. Multiple linked parties can be added by clicking the "+" button on goAML.

(ii) STR-F

STR-F is to be reported when parties (person, account, or entity) are involved in any suspicious transaction and/or financial activity. An activity/event in which funds are transmitted from one party to another must be reported as STR-F.

2.2.4. Information required for filing of Suspicious Transaction Reports

It is important to select the relevant party type involved in the transaction while filing an STR. The following are the three parties that can be selected in goAML: person, account, and entity. The relevant information corresponding to each party that is required for filing an STR is mentioned below.

A. Person

(i) Your client:

- First name;
- Last name;
- Father/husband name;
- Gender;
- Date of birth;
- CNIC/passport number;
- Nationality;
- Phone/cell number;
- Address.

(ii) Not your client:

- First name;
- Last name;
- CNIC/passport number (where available).

B. Account

(i) Your client:

- Account number;
- Account title;
- Institution name;
- Institution branch;
- Swift code or registration number;
- Account type;
- Account status;
- Account currency;
- Account signatory (details of account holders/operators);
- Entity and directors/owners details (in case of entity account)
- Aggregate credits (for the last 3 years at least);
- Aggregate debits (for the last 3 years at least).

(ii) Not your client:

- Account number;
- Account title;
- Institution name;
- Institution branch;
- Swift code or registration number.

C. Entity

(i) Your client:

- Name of entity;
- Entity type;
- Type of business;
- Registration number;
- Registration country;
- Tax number/sales tax number;
- Phone/cell number;
- Address;
- Directors'/owners' details.

(ii) Not your client:

- Name of entity;

- Any other information as identified above in paragraph C(i) that may be available to the reporting entity.

2.2.5. Contents of Suspicious Transaction Reports

(i) Reasons for filing STR

The reason(s) for suspicion should be supported with proper analysis and should contain the following elements:

- Information on the person/entity conducting the suspicious transaction/ activity;
- Details of the transaction, such as the pattern of transactions, type of products or services, and the amount involved;
- Description of the suspicious transaction or its circumstances;
- Tax profile of person/entity (if available);
- If the reported subject (e.g. client/customer) has been the subject of a previous STR then the reference number with the date should be provided;
- Information regarding the counter parties, etc.
- Any other relevant information that may assist the FMU in identifying potential offences and individuals or entities involved.

(ii) Action taken by the reporting entity

Provide detail of any action already taken by the REA on the customer, other than the filing of the STR. Examples include:

- Freezing action;
- Shared with LEA;
- Rejection of customer;
- Termination of the customer relationship.

(iii) Report indicators

Select the relevant indicator(s) while filing the STRs in goAML. The indicator(s) selected for the STR must be aligned with the reason for suspicion. Multiple indicators may be selected.

The following are some scenarios in which a single indicator is not sufficient and reporting entities must provide an additional indicator to enhance the quality of the STR:

- Attempted transaction/account;
- LEA Inquiry;
- Adverse Media Report;
- PEP.

2.2.6. Reporting of Transactions in STR-F

Below are some key points to keep in mind while reporting transactions in STR-F on goAML:

- There are three basic parties that could be involved in a transaction, i.e., person, account, and entity. Hence, the information of the appropriate party must be entered as 'From Party' and 'To Party'.
- At least two parties (out of three) would be involved in each transaction, depending on the nature of the transaction. Some of the various combinations of parties involved in transactions are as follows:
    - Person to person transaction (e.g. currency exchange transactions in cash, sale/purchase of prize bonds in cash);
    - Person to account transaction (e.g. cash deposit, wire transfer by a person to foreign account, payment of insurance premium, cash payment for investment);
    - Account to person transaction (e.g. cash withdrawal, currency exchange through an instrument, issuance of banker cheque from account favoring a person);
    - Account to account transaction (e.g. transfer of funds from one account to another, IBFTs, wire transfers, maturity/surrender of insurance policy to an account);
    - Account to entity transactions (e.g. banker cheque issuance in the name of an entity)
    - Entity to account transactions (e.g. banker cheque issued in name of an entity deposited into an account);
- The relevant transaction channel must be selected;
- Correct fund types should be used for both ends of the transaction. The fund type requires the form/nature of funds when the transaction was initiated ('From Fund Type') and the form/nature of funds after completion of the transaction ('To Fund Type');
- Transactions being reported must be supported by the reason for suspicion;
- The actual Transaction Number should be provided (note: do not use the goAML auto-generated transaction number);
- From Country' and 'To Country' information should be provided for wire transfers/cross-border transactions;

- If the transaction involves foreign currency, the details of such foreign currency must be provided in the foreign currency tab indicating the relevant currency type.

2.2.7. Reporting of Transactions in STR-A

Below are some key points to keep in mind while reporting transactions in STR-A on goAML:

- One or more of the three basic parties, i.e., person, account, and entity, must be selected and the relevant information provided;
- Some of the scenarios for reporting of parties in STR-A are as following:
    - If a suspected person/entity is maintaining any relationship and/or facility with the reporting entity, the party type should be reported as 'Account';
    - With walk-in customers or persons to whom the service was declined, the party type should be reported as 'Person';
    - If a service was declined to an entity, the party type should be reported as 'Entity';
- Complete available information of the person including the NTN (if available) must be provided while reporting party type person;
- Details of signatories must be provided in the signatory tab while reporting a personal account in party type;
- Details of the entity and its signatories must be provided in the entity tab when reporting an entity account in party type;
- Complete available information of the entity including the NTN and registration number (if applicable) must be provided while reporting party type entity;
- Details of directors/owners must be provided in director(s)/Owner(s)/Trustee(s)/others tab while reporting party type entity.

2.2.8. Attachments and Supporting Documents

Below are some key points regarding submission of attachments and support documents along with STRs on goAML:

- It is mandatory to submit the relevant supporting documents as attachments to the STR. FMU will not accept STRs without any attachments. The supporting documents may include the following:
    - Identification documents;
    - Sources of income;
    - KYC/CDD documents;
    - Account opening forms (if applicable);

18. Circular No.2 of 2019 issued by the FMU.

  - Statement of accounts (if applicable);
  - Copies of transaction vouchers;
  - Copy of SWIFT messages;
  - Account details annexure (if applicable);[18]
  - The LEA's letter seeking information and the reporting entity's response letter, if information is shared with any LEA;
  - Other documents may vary on a case-to-case basis.
- Documents attached with the STR must be in Optical Character Recognition (OCR) format;
- Each document must be attached separately with its unique file name;
- Do not collate more than one document in the same file;
- goAML can support attachments of up to 20 megabytes.

2.2.9. Rejection of Suspicious Transaction Reports

FMU reserves the right to reject STRs that are incomplete, suffer from technical deficiencies, or do not meet the basic requirements of goAML. The STRs submitted on goAML pass through three stages:

(i) Data validation by the system to check the structure of STRs;
(ii) System-based rules developed by FMU to review STRs in line with the guidelines issued by the FMU;
(iii) Verification of the quality of the STR by the FMU compliance team which ultimately decides to accept or reject the STR.

FMU keeps track of accepted and rejected STRs filed by reporting entities. FMU also provides guidance against queries raised by reporting entities via the goAML Help Desk that can be reached at goamlhelpdesk@fmu.gov.pk and the goAML Message Board.

2.2.10. Resubmission of Rejected Suspicious Transaction Reports

Reporting entities are required to resubmit rejected STRs promptly. FMU does not ask the reporting entity to resubmit their STR in case of rejection and the filing status of a rejected STR shall be considered to be unreported unless it is resubmitted. Below are certain guidelines regarding re-submission of rejected STRs:

- It is the reporting entity's responsibility to ensure following up on rejected STRs;
- Reporting entities should resubmit their STR with the same goAML identification number;
- Reporting entities should not create a new report for resubmission. However, if the STR is rejected due to the selection of the incorrect report type, then the

reporting entity should create a new report as the report type cannot be changed after submission;

- Each rejected STR shall be submitted after the necessary correction indicated by FMU without delay;
- STRs shall only be considered as reported when the reporting entity receives an acknowledgment of STR acceptance from FMU through the message board on goAML;
- These acknowledgments will be archived after 30 days (or any other period as determined by FMU), therefore reporting entities should ensure that they save the acknowledgments from the message board;
- Submitted STRs will be reflected in the reporting entity's goAML account for a period of 30 days (or any other period as determined by FMU), therefore, reporting entities should ensure that they maintain their records of STRs submitted on goAML;
- FMU will not provide the record of submitted STRs to any reporting entity, neither will it provide any information required for the purpose of audit of reporting entities or any other related purpose.

2.3. OPERATING PROCEDURES FOR CURRENCY TRANSACTION REPORTS

2.3.1. Should you file a Currency Transaction Report?

Given the AML/CTF requirements only apply to cash transactions valued at PKR 2 million or more, every time you complete a cash sale transaction over such threshold, you are required to file a CTR. This includes cash sales transactions below the threshold which are linked and the total value of which meets the threshold mentioned above.

A DPMS would not be required to file any CTR if the sales transaction is via wire transfer or credit/debit card. If a DPMS pays cash to the sales staff as remuneration or purchases an asset such as a computer, and such amount meets the threshold, such transaction would not need to be reported in a CTR as they would not be considered as cash sales transactions. However, if your buyer or supplier is another DPMS, and the transaction otherwise meets the threshold provided under the law, then CTR filing obligations apply.

2.3.2. Types of Currency Transaction Reports

There are two types of CTRs:

(i) CTR

This type of report is to be filed by all financial institutions[19] and DNFBPs[20] involving a cash transaction of PKR 2 million or above.

(ii) CTR-A

This type of report is to be filed by exchange companies only for transactions involving multiple currencies aggregating PKR 2 million or above.

The following table will help you determine which type of CTR you should file:

19. Defined in Section 2(xiv) AMLA.
20. Defined in Section 2(xii) AMLA.

CRITERIA	CTR	CTR-A
Who can file	All reporting entities	Exchange companies only
Number of currencies involved	Single currency	Multiple currencies
Number of transactions in the report	Can contain one or multiple CTRs in a report	Will contain at least two transactions aggregating PKR 2 million or above in a report
Parties involved in the report	Transactions related to multiple parties can be reported	Transactions related to a single party will be filed in a report
Type of transaction	Cash transactions of PKR 2 million or above involving cash deposit, cash withdrawal, currency exchange, wire transfer, etc.	Currency exchange transactions of more than one foreign currency by a single person at one time aggregating PKR 2 million or above

2.3.3. Information required for filing of Currency Transaction Reports

All CTRs are filed as bi-party transactions in goAML, therefore there will be a 'From Party' (the originator of the funds) and a 'To Party' (the beneficiary of the funds). It is important to select the relevant party type involved in the transaction while filing a CTR. The following are the three parties that can be selected in goAML: person, account, and entity. The parties do not necessarily need be to your client. The relevant information corresponding to each party that is required for filing an STR is mentioned below.

A. Person

(i) Your client:

- First name;
- Last name;
- Father/husband name;
- Gender;
- Date of birth;
- CNIC/passport number;
- Nationality;
- Occupation;
- Phone/cell number;
- Address.

(ii) Not your client:

- First name;
- Last name;
- Father/husband name;
- Gender;
- Date of birth;
- CNIC/passport number;
- Nationality;
- Phone/cell number;
- Address.

B. Account

(i) Your client:

- Account number;
- Account title;
- Institution name;
- Institution branch;
- Swift code or registration number;
- Account type;
- Account status;
- Account currency;
- Account opening date;
- Account signatory (details of account holders/operators);
- Entity and directors/owners details (in case of entity account)

(ii) Not your client:

- Account number;
- Account title;
- Institution name;
- Institution branch;
- Swift code or registration number.

C. Entity

(i) Your client:

- Name of entity;
- Entity type;
- Nature of business;
- Registration number/tax number/CNIC of proprietor or partner(s);
- Phone/cell number;
- Address;
- Directors'/owners' details.

(ii) Not your client:

- Name of entity;
- Any other information as identified above in paragraph C(i) that may be available to the reporting entity.

2.3.4. Selection of Fund Code

The fund code in a transaction represents the nature of the transaction or type of funds involved. For every transaction, the reporting entity has to provide unique fund codes for both the 'From' and 'To' parties.

2.3.5. General Guidelines for filing of Currency Transaction Reports

Below are general guidelines to ensure the quality of CTR reporting by reporting entities:

- Only those cash transactions worth PKR 2 million or above are required to be reported;
- Reporting entities shall not report account to account, account to entity, and entity to account transactions as CTRs;

- If an account of an entity is being reported as 'My Client', the details of the entity along with the sole proprietor/partners/directors/trustees are also to be provided in the entity tab within the account party type;
- While reporting an account with multiple signatories in a cash transaction, it is mandatory to provide the details of all signatories along with their necessary information;
- If a transaction involves foreign currency, a foreign currency node needs to be created on the 'To/From' side of the transaction where the foreign currency was involved;
- Attachments and indicators are not required for CTRs;
- No information shall be provided in the 'Conductor' tab. The information related to the person conducting the transaction is required to be filed on either 'From/To' side depending on the nature of the transaction.

2.3.6. Rejection of Currency Transaction Reports

FMU reserves the right to reject CTRs that are incomplete, suffer from technical deficiencies, or do not meet the basic requirements of goAML. The CTRs submitted on goAML pass through three stages:

(i) Data validation by the system to check the structure of CTRs;
(ii) System-based rules developed by FMU to review CTRs in line with the guidelines issued by the FMU.

FMU keeps track of accepted and rejected CTRs filed by reporting entities. FMU also provides guidance against queries raised by reporting entities via the goAML Help Desk that can be reached at goamlhelpdesk@fmu.gov.pk and the goAML Message Board.

2.3.7. Resubmission of Rejected Currency Transaction Reports

Reporting entities are required to resubmit rejected CTRs promptly. The filing status of a rejected STR shall be considered to be unreported unless it is resubmitted within the prescribed time period. Below are certain guidelines regarding re-submission of rejected CTRs:

- Reporting entities should resubmit their CTR with the same goAML identification number;
- Reporting entities should not create a new report for resubmission. However, if the CTR is submitted through an XML upload, the reporting entity would have to upload the report again without any delay after making the necessary corrections indicated by the FMU in its reasons for rejection. This would result

in the generation of a new report ID;

- If the CTR is rejected due to an incorrect selection of report type, the reporting entity should create a new report as the report type cannot be changed after submission;
- Each rejected CTR shall be submitted after the necessary correction indicated by FMU without delay;
- CTRs shall only be considered as reported when the reporting entity receives an acknowledgment of CTR acceptance from FMU through the message board on goAML;
- These acknowledgments will be archived after 30 days (or any other period as determined by FMU), therefore reporting entities should ensure that they save the acknowledgments from the message board;
- FMU will not provide the record of submitted CTRs to any reporting entity, neither will it provide any information required for the purpose of audit of reporting entities or any other related purpose.
- Accepted CTRs will be reflected in the reporting entity's goAML account for a maximum period of 1 day (or any other period as determined by FMU), therefore, reporting entities should ensure that they maintain their records of CTRs submitted on goAML.

2.4. General Guidelines for filing of reports on goAML

All errors should be removed prior to submission of the report to ensure high-quality reporting and to avoid any subsequent follow-ups and violations. The following are some general guidelines to be kept in mind while filing STRs or CTRs on the goAML website:

- Be mindful of typographical errors, particularly in the transaction date, amount, and CNIC/passport number fields;
- Fields must not contain dummy values, hyphens (-), 'N/A', or any other such value;
- Reporting entities are encouraged to develop a proper mechanism to ensure correct data entry;
- Complete names along with correct spelling must be provided;
- Abbreviations should be avoided in fields like reporting district, province/state, and city;
- Person, account, and entity information must be provided in the person, account, and entity tabs, respectively;
- Country information on both the 'From' and 'To' sides is mandatory for each transaction. The correct country name needs to be selected in both the 'Source Country' and 'Destination Country' fields while reporting cross-border transactions;
- Reporting entities are encouraged to fill in the non-mandatory fields (such as email address, employer name, tax number) if such information is available in their systems;
- Reporting entities shall periodically review the XML files of their CTRs to check for any errors or incorrect filling of fields;
- Reporting entities are required to provide their own system-generated transaction numbers in the transaction number field in goAML, so that the transaction can be traced back as and when required.

3. CONDUCTING CUSTOMER DUE DILIGENCE

Risk-based CDD aids in the implementation of AML/CFT laws. It can involve changes in the customer acceptance policies of REAs or the introduction of engagement policies.

3.1. Legal Requirements

Reporting entities need to identify and verify the identity of the customer and the beneficial owner, understand and if appropriate gather information regarding the purpose and nature of the business relationship, as well as continuously monitor the business relationship.[21] A third party can be relied upon by the reporting party to carry out CDD.[22]

Where CDD requirements are not fulfilled, the reporting entity will not be allowed to open accounts, commence or terminate business relations, or perform the transaction and will instead have to file an STR. Also, where the reporting entity is suspicious of ML/TF the CDD process will not be performed and an STR will be filed, to avoid tipping off.[23]

A reporting entity entering into a relationship with a customer who gives a fictitious name or is anonymous is prohibited.[24]

The DNFBP Regulations provide for the following matters:

(a) The obligatory CDD requirements regarding the verification and identification of the customer, beneficial owner and person claiming to be acting on the customers behalf using independent documents, information or data which is authentic;[25]
(b) Delayed verification, subject to certain conditions;[26]
(c) Ongoing due diligence on existing customers which entails inspecting transactions and keeping the record of CDD up to date, as well as reviewing them.[27]

Furthermore, REAs are to apply enhanced due diligence where the risk is greater,

21. Section 7A AMLA.
22. Section 7B AMLA.
23. Section 7D AMLA.
24. Section 7E AMLA.
25. Regulation 8(1) to 8(12) DNFBP Regulations.
26. Regulation 8(13) and 8(14) DNFBP Regulations.
27. Regulation 8(15) and 8(16) DNFBP Regulations.

which is called upon by the FATF for certain countries and PEPs, including their family members and close associates.[28] If the risks are lower, the REA can apply due diligence which is simple, but not where ML/TF is suspected.[29] Countermeasures must be used by the REA in countries where the risk is high,[30] while third parties can be relied upon under certain conditions.[31]

3.2. Operating Procedures

3.2.1. Whom is Customer Due Diligence conducted upon?

CDD is conducted upon:

1) The DPMS's customer (both buyer and seller)

A customer includes any natural or legal person, or legal arrangement which engages a DPMS to request, acquire or use any service or carry out any business or transaction with a DPMS, but only for certain services and transactions.[32]

2) The DPMS's customers beneficial owner

Beneficial owner of the customer refers to any natural person who eventually controls or owns a customer or a natural person on whose behalf a transaction is being carried out, or a natural person who exercises ultimate effective control over a legal arrangement or a legal person.[33]

3) A person acting on behalf of the DPMS's customer

A person who acts on behalf of a customer, but is not a beneficial owner of the customer:

(a) A person exercising a power of attorney for your customer;
(b) A legal guardian who acts on behalf of a minor who is a customer;
(c) A person who exercises the power of attorney for the customer.

28. Regulation 9(1) to 9(3) DNFBP Regulations.
29. Regulation 10 DNFBP Regulations.
30. Regulation 11 DNFBP Regulations.
31. Regulation 12 DNFBP Regulations.
32. Regulation 2(1)(f) DNFBP Regulations.
33. Section 1(iv) AMLA.

3.2.2. Requirements of Customer Due Diligence

CDD should commence after the DPMS and the customer have begun discussion regarding potential sales, but must be completed before the sales transaction is completed.[34] Given most DPMSs are retail in nature, e.g., jewelry shops selling to walk-in customers, the time available to complete the CDD process is limited if the customers want to pay in cash and the sales transaction is worth PKR 2 million or above.

The DPMS is to obtain necessary information regarding the identity of the customer, beneficial owner and any person who acts on behalf of the customer and also should verify information which is collected.[35]

CDD = Identification (including Beneficial Ownership) + Verification + Purpose

Each step of CDD, i.e., identifying the customer, documents required for verification, and determining the purpose of the transaction or business relationship, have been elaborated upon below.

(i) Identification

As part of the CDD process, you are required to know your customer, whether they are an individual, a company, or a trust. For individual and corporate customers, it is also important to determine whether there is any beneficial owner or authorized representative. The CDD requirements for each type of customers has been highlighted in the three charts below.

CDD requirements for individual customers (or beneficial owner or authorized representative)

34. Section 7A AMLA.
35. Regulation 8 DNFBP Regulations.

Table A: CDD Requirements for individual customer(or Beneficial Owner or Authorized Representative) *		
Information Required:	Documents to verify information: original, or original of certified true copy of document, or electronic verification via NADRA (where applicable)	**DATE DOCUMENT COPIED/ SIGHTED/ VERIFIED**
Full Name:	Resident: NADRA identity card (CNIC) Non-resident: NADRA NICOP or POC, alien registration card (ARC), or passport https://id.nadra.gov.pk/identitydocuments/verification-services/	
Date of Birth:	NADRA identity card, ARC or passport	
Residential Address:	Recent utility bill	
NADRA identification number/Passport	NADRA identity card, ARC or Passport https://id.nadra.gov.pk/identitydocuments/verification-services/	
To identify whether customer is acting on their own behalf or on behalf of another person	If yes, and the individual is acting on behalf of another individual(s) – refer to this table (Table A. if the customer is acting on behalf of legal entities – refer to Table B.	
Source of wealth or funds (necessary for higher risk customers and PEPs)	Bank statement, accountant's statement, taxation return etc.	

Table B: CDD Requirements for Company Customer (and Beneficial Owner and any Authorised Representative)		
INFORMATION REQUIRED	**DOCUMENTS TO VERIFY INFORMATION**	**DATE DOCUMENT COPIED/ SIGHTED / VERIFIED**
Full name of business:	**Company incorporation certificate**	
Registration number	Company incorporation certificate SECP website: https://eservices.secp.gov.pk/eServices/NameSearch.jsp	
Tax payer number Permanent business address	Tax authority document company incorporation certificate Utility bill, rental agreement	
Structure of company	Legal documents to establish company/ ownership e.g., Articles and memorandum, articles of association. Securities and exchange commission of Pakistan (SECP) registration declaration for commencement of business as required under the companies' act, 2017 (XIX of 2017), as applicable.	
Beneficial ownership information	**Company:** Register of members of a company section 119 of the companies' act, 2017 (Act no. XIX of 2017) Register of ultimate beneficial ownership information, section 123A of companies Act **Individual:** For all individuals identified as beneficial owners (e.g., major shareholders – 25% and more – verification documents are the same as for individual customers – refer Table A above.	
Source of wealth or funds (necessary for higher risk customers and PEPs)	Bank statement accountant's statement etc.	
Details of individual acting for the company	Same as in Table A for individual customer and official letter from business authorizing person to represent the customer.	

CDD requirements for customers that are trusts

The Trusts Act 1882 defines a trust as an obligation annexed to the ownership of property and rising out of a confidence reposed in, and accepted by the owner, or declared and accepted by him, for the benefit of another, or of another and the owner.

Simply put, a trust is an obligation wherein the author of the trust known as the settlor transfers their property into the name of the trustee who holds the property for the benefit of the beneficiary and is not allowed to use the property for their benefit.

This means that when a trust is created, the legal title to the property or its ownership lies with the trustee however, he does not derive any benefit from it. In the context of money laundering and terrorism financing then, trusts may be used to hide true ownership of the beneficiary who is responsible for the commission of the offence and hides behind the trust.

Example: Mr. A established a trust with himself as a settlor, and beneficiary and a local trusts and company service provider as the trustee. The company is directed by Mr. A to buy gold jewelry valued at 2 million PKR. A representative of the company walks into Mr. A's preferred jewelry store and buys jewelry worth 1 million PKR in cash. He then comes back later and buys more jewelry worth 1 million PKR in cash. During both these transactions the dealer in precious metals and stones conducts CDD and identifies the company as the owner of the money through which jewelry is being bought. However, as money was held on trust, the DPMS must have identified whether any beneficial ownership existed or not, and considered the information presented in the table below to identify who the real owner of the property is to ensure that any risk of ML/TF offences being committed is dealt with in accordance with the law.

Table C: CDD Requirements for Trust Customer		
INFORMATION REQUIERED	**DOCUMENTS TO VERIFY INFORMATION**	**DATE DOCUMENT COPIED/ SIGHTED / VERIFIED**
Full name of trust (as in trustdeed/agreement)	Trust deed/agreement and trust registration certificate.	
Registration number (if applicable)	Trust deed/agreement and trust registration certificate.	
Tax payer number	Tax authority document	
Permanent address	Trust deed/agreement and trust registration certificate.	
Type of business/ ownership structure	Legal document to establish business / Trust deed/agreement and trust registration certificate.	
Beneficial ownership information -Trustee -Protector (if any) -Settlor (or donor) -Beneficiaries	Table A information on company must be obtained and verified, if any trustee of beneficiaries are companies. Table B information on company must be obtained and verified, if any trustee or beneficiaries are companies. Table C on trust if a beneficiary is another trust.	
Source of wealth or funds (necessary for higher risk customers or PEPs)	Bank statement, accountant's statement etc.	

(ii) Verification

The following types of verification procedures may be employed to verify the identity of the customer:

Original	Certificate True Copy of Document	Electronic/Digital Verification
For purposes of verification, original documents need to be sighted, photocopies and attested by the REA e.g., stamped "Original Seen"	Where the customer is unable to produce original documents, the REA may consider accepting documents that are certified to be true copies by an independent and qualified person (such as a lawyer, a notary public, etc.) The original of the certificate true copy must be provided – not just a photocopy of the certified true copy.	Alternatively, if feasible, electronic verification may be undertaken. NADRA is a good source of verification of individuals and SECP for companies and some NPOs. A number of subscription services give access to identity-related information. Many of them can be accessed on-line and are often used to replace or supplement paper-based verification checks. If onboarding is non-face-face and only email copies of documents are provided, in addition to the above mitigation measures, a live virtual meeting (Video Call) should be undertaken. However, a video call is not equivalent to electronic verification.

(iii) Additional guidance regarding identification and verification or beneficial ownership

Legal ownership is separate and distinct from beneficial ownership. With respect to identifying and verifying beneficial ownership, reasonable measures are to be taken, i.e. appropriate measures which are commensurate with the money laundering or terrorist financing risks.[36]

Beneficial owners of the following needs to be identified:

(a) Natural persons;

The legal and beneficial owners of natural persons are usually the same. However, there may be circumstances where this is not the case. Therefore,

36. Regulations 2(1)(o) DNFBP Regulations.

unless there are reasons to doubt, the REA may assume the individual customer is also the beneficial owner. However, the REA should ask the seller and buyer whether they are selling or buying for another person.

(b) Legal persons (e.g. companies);

There are three tests for identifying the beneficial owner of a corporation.

IDENTIFYING BENEFICIAL OWNERSHIP FOR LEGAL PERSONS – THREE CASCADE TESTS

Limited Companies/ Corporation

TEST 1: The Legal Ownership Test

This is normally the first test used to identify the beneficial owner as provided Section 8 (9) (a) of the FBR AML/CFT Regulations for DNFBPs.

This test is trill about control, but control primarily through legal ownership. In general, the threshold to use is 25% or more to determine controlling legal ownership, but there may be a need to use a lower threshold.

Ownership threshold approach: The natural person(s) who directly or indirectly holds a minimum percentage of ownership interest in the legal person, so that he/she can exercise controlling ownership interest (e.g., voting rights).	Any individual owning more than a certain percentage of the company i.e., 25%. If the threshold there can only be a maximum of 4 beneficial owner as provided in section 123A of the companies Act. While 25% or more may be used for the controlling ownership test, if the 25% threshold does not identify any beneficial owners, or there are concerns or doubts that the 25% threshold has correctly identified all the beneficial owners, it is recommended that a lower threshold of 20% be used, and then 10%, if needed. Individuals may not meet the ownership threshold (e.g., below 25%) but because they are connected (e.g., family or extended family), collectively they can exercise control – refer to Test 2.

TEST 2: THE CONTROL TEST

This is normally the second test used to identify beneficial owner as provided under Section 8 (9) (b) of the AML/CFT Regulations for DNFBPs.

This test is used when where there is doubt that the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest. For example, no one owns more than 25% or more, or there are so many layers of indirect ownership it is difficult to identify the individuals who owns the company in the top layer.

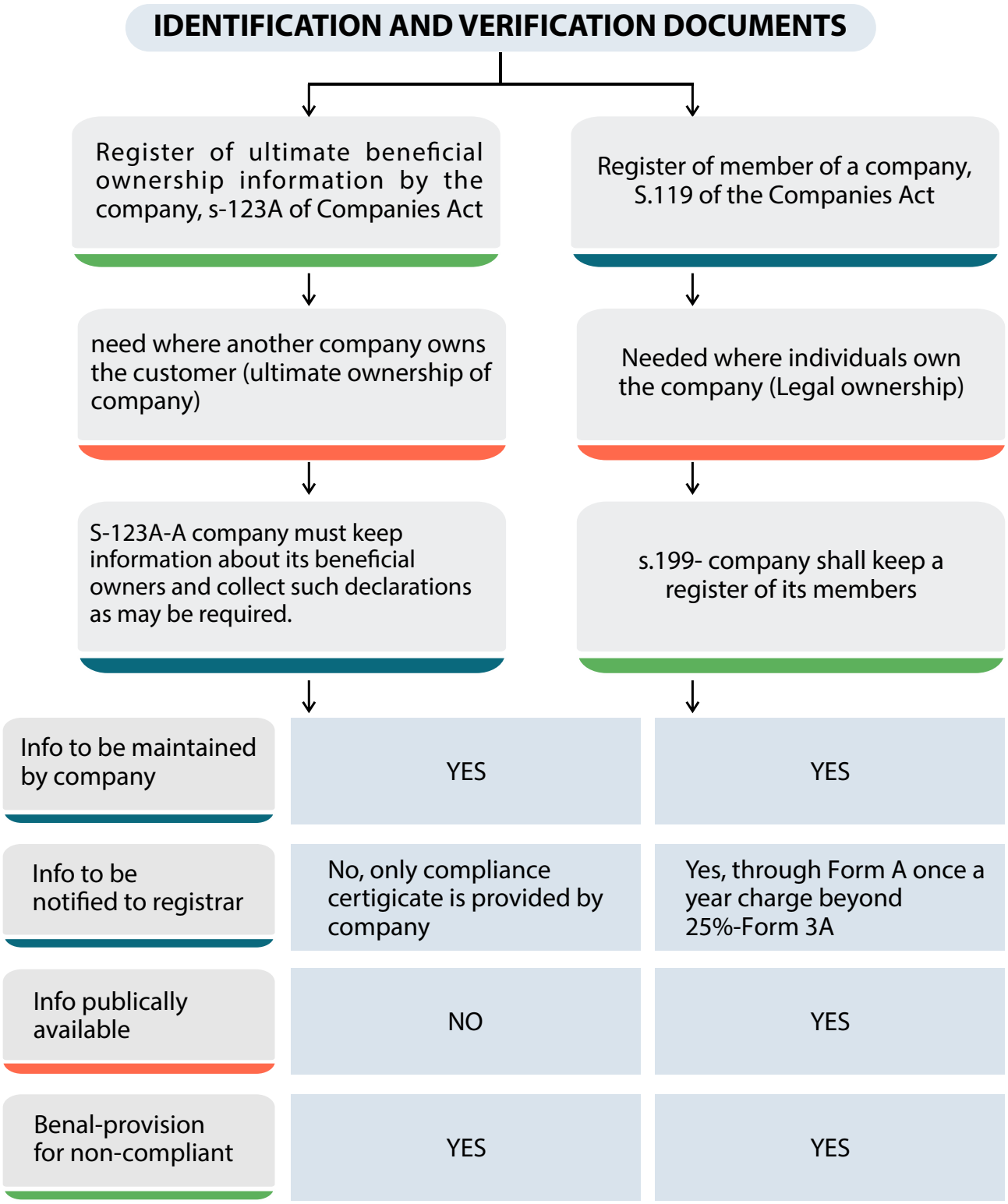
2. Majority interest approach: Shareholders who exercise control alone or together with other shareholders, including through any contact, understanding, relationship, intermediary or tiered entity.	For example, to appoint or remove the majority of the board of directors. or its chair, or COD of the company For example, exercise 2S% or more voting rights other than through legal ownership e.g. shareholders agreement to vote collectively to control a company even though indtviclually they do not have 2S% or more.
3. Connections or Ontrac foal relations approach: Natural persons who may control the legal person through other means	For example, the natural Person(s) who exerts control of a legal person through other means such as personal connections to persons in positions described above or that possess ownership. The natural Person(s) who exerts control without ownership by participating In the financing of the enterprise, or because of close and intimate family relationships, historical or contractual ass-ociations, or If a company defaults on Certain payments.
4. Company director's position approach: The natural person(s) responsible for strategy decisions that fundamentally affect the business practices or general direction of the legal person	The identification of the directors may still Provide useful information. However., information on directors may be of limited value if a country allows for nominee directors acting on behalf of unidentified interests.

TEST 3: The Senior Management Test:

In the event the beneficial owner cannot be identified or verified as above Tests 1 and 2, Section 8 (9) (c) of the FBR AML/CFI Regulations for DNFSPs provide for the use of the senor management approach as the alternative test of beneficial ownership

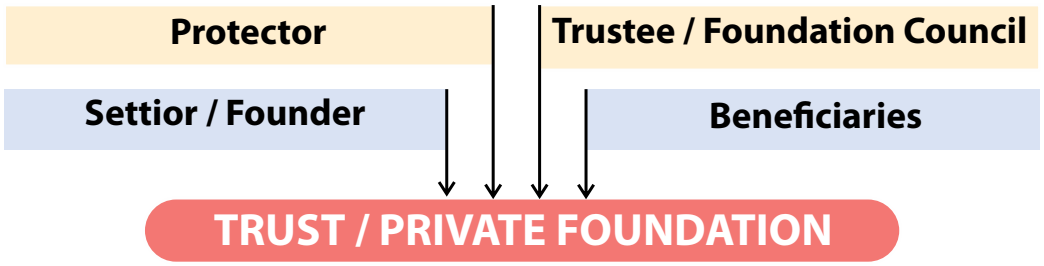
5. Senior management approach (alternative test): The natural Person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position	This is only permitted when the REA cannot Identtly or Verify the beneficial owner in limited circumstances, for example: • Dispersed ownership: • Multiple layers of ownership, including in overseas secrecy jurisdiction, or bearer shares are permitted: The senior management test. for, example, may include the chief executive officer IEE0). chief financial officer (CFO). managing or executive or rector, or president. It is the natural person(s) who has significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.

The documents required for identification and verification of beneficial owners of legal persons is as follows:



(c) Legal arrangements (trust or waqf)

Identifying which individual is the beneficial owner of a trust is more challenging as these arrangements have much more complex structures because they usually do not have owners but parties with different roles, rights, and obligations as illustrated below. Therefore, all parties to a trust are treated as beneficial owners.



DPMSs are required to identify and take reasonable measures to verify the identity of beneficial owners as follows:[37]

(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 above 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.

IDENTIFYING BENEFICIAL OWNERSHIP FOR LEGAL ARRANGEMENTS	
Express trusts/Waqf/or other legal arrangement	
Category	**Identification and verification**
1. Settlor (or equivalent) natural, legal person or arrangement who transfers ownership of their assets to trustee by means of a trust deed or similar arrangement.	Trust deed/agreement Once verified based on the trust deed/agreement, the identification and verification is the same as if the person is an individual. legal person or legal arrangement Itrustl customer of the REA.
2, Trustee for equivalent! may be professional (e.g. a lawyer, accountant or trust company) if they arc paid to act as a trustee in the course of their business, or nonprofessional le.g. a person acting without reward on behalf of family)	Once verified based on the trust deed/agreement, the identification and verification is the same as if the person is an individual, legal person or legal arrangement (trust, customer of the REA. If the trustee is a corporate trustee, the individual authorised to represent the corporate trustee e.g. director needs to be identified and verified.

37. Regulation 8(10) DNFBP Regulations.

3. Protector (or equivalent) not all trusts have a protector - protector is a person or group of people not the settlor, beneficiary, or trustee) who are appointed to exercise one or more powers affecting a trust and the interest of the beneficiaries. The concept of a trust protector is to protect beneficiaries from a rogue trustee.	Once verified based on the trust deed/agreement. the identification and verification is the same as if the person is an individual. legal person or legal arrangement Itrustl customer of the REA. If the protector is a corporate protector, the individual authorised to represent the corporate e.g. director needs to be identified and verified.
4. Beneficiaries (or equivalent) a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement.	A beneficiary would be a beneficial owner if it has 25% (depending on the threshold used) or more entitlement to the trust distribution. Not all trust specifies a specific unit value e.g. discretionary trust do not, or there are too many potential beneficiaries. In some cases, the beneficiaries are not even born e.g. the children of the son and daughter of X. When it is not possible to identify and verify a beneficiary, the class of beneficiary should be identified e.g. the grandchildren of Mr X, or displaced persons living in region A. Once verified based on the trust deed, the identification and verification are the same as if the person is an individual or legal person customer of the REA. If the beneficiary is a corporate beneficiary. then all CDO requirements of a legal person would need to be undertaken. If the beneficial is another trust - then all the CDC requirements of a trust would need to be undertaken.

3.2.3. Politically Exposed Person

PEPs are individuals who, by virtue of their position in public life, may be vulnerable to corruption. EDD must be applied to all PEPs and their close associates and family members, unlike for other customers, where enhanced due diligence will depend on whether the customer (and beneficial owner) is rated high risk or not.

A PEP is an individual who is or has been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization and includes but is not limited to:[38]

(i) For foreign PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and political party officials;
(ii) For domestic PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, political party officials;
(iii) For international organization PEPs, members of senior management or individuals who have been entrusted with equivalent functions.

Examples of PEPs in Pakistan are:

(i) Heads of states, heads of governments, ministers, and deputy or assistant ministers;
(ii) Members of senate, provincial assembly, or national assembly;
(iii) Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
(iv) Government servants equivalent of BPS-21 or above;
(v) Ambassadors;
(vi) Military officers with a rank of Lt .General or higher and its commensurate rank in other services;
(vii) Directors and members of the board or equivalent function of an international organization;
(viii) Members of the governing bodies of political parties;
(ix) Members of the board or equivalent function in corporations, departments, or bodies that are owned or controlled by the state.

EDD must be applied to:[39]

(a) All PEPs;
(b) Family members;[40]
    (i) Spouse of the PEP;
    (ii) Lineal descendants and ascendants and siblings of the PEP;

38. Regulation 2(1)(m) DNFBP Regulations.
39. Regulation 9(1) DNFBP Regulations.
40. Regulation 2(1)(i) DNFBP Regulations.

(c) Their close associates:[41]
   (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;
   (ii) 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;
   (iii) An individual who is reasonably found or believed to be closely connected with the PEP for any other reason, either socially or professionally.

3.2.3.1. What should Dealers in Precious Metals and Stones do?

DPMSs are required to do the following with respect to PEPs:

(a) Risk management system to identify PEPs;
(b) Identify the source of wealth and funds;
(c) EDD (senior management approval);
(d) Enhanced ongoing monitoring/CDD.

3.2.3.2 When should Dealers in Precious Metals and Stones conduct Enhanced Due Diligence?

You should conduct EDD if your customer is any of the following:

PEP (& family members and close associates) who is an individual customer
PEP (& family members and close associates) who is abeneficial owner of a company or legal person
PEP (& family members and close associates) who is a Trustee of a trust
PEP (& family members and close associates) who is settlor or protector (if any) of a trust
PEP (& family members and close associates) who is a beneficiary of trust's income or wealth

41. Regulation 2(1)(e) DNFBP Regulations.

3.2.3.3. How can Politically Exposed Persons be identified?

PEPs can be identified through the following method:

(a) DPMSs should ask all customers to declare if they are a PEP, or family member, or close associate of a PEP. This should be in a signed declaration as part of the customer acceptance/application form;

(b) The DPMS should undertake an independent check. The DPMS's procedures may include:
   (i) An internet search of the customer's or beneficial owner's background;

(c) Engaging the services of a commercial risk screening service provider. While they may be good for foreign PEPs, they may not be as good for Pakistani PEPs and their family and close associates. They may be too expensive for sole practitioners or small DPMSs.

(d) DPMSs may not identify a PEP during the acceptance stage of a new customer, but ongoing monitoring may later identify the customer and/or the beneficial owner as a PEP.

3.2.3.4. How to identify the Source of Wealth and Funds?

There is a requirement to obtain information on the source of wealth or source of funds for customers subject to EDD.[42] Sources of wealth mean the customer's total body of wealth (such as total assets) whereas the source of funds means the origins of such funds/assets that form the subject matter of the business relationship between the DPMS and the customer. Note that this requirement is only for real estate agents to obtain information. There is no requirement for DPMSs to verify such information through supporting documentation unless there are doubts on the veracity of the information provided, or because of risk. This would be a decision for DPMSs to make based on the information that the particular customer has provided.

For PEPs which require EDD, reasonable measures to establish the source of funds and source of wealth of the customer and beneficial owners who are PEPs and their close associates or family members must be taken.[43] Since not all PEPs are high risk, their level of due diligence will vary. Even though verification has not been explicitly specified, reasonable measures being taken by the PEP may require verifying the source of wealth and funds. Establishing the source of funds will depend on the specific service provided by the DPMS.

42. Regulation 9(2)(c) DNFBP Regulations.
43. Regulation 9(3)(b)(ii) DNFBP Regulations.

If the DPMS has suspicion over the accuracy of the source of wealth or funds, it can request documents, such as tax returns to confirm the accuracy.

Examples of sources of wealth and funds are:

INFORMATION AND VERIFICATION OF SOURCE OF WEALTH OR FUNDS			
a) Employment Income • 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** • Copy of latest audited financial statements; Board of Directors approval • Rental statements • Dividend statements	**c) Savings / deposits/assets/ property/** • Statement from financial institution • Bank Statement Taxation returns • Accountants Statements • Property ownership certificate • Share certificates	**d) Inheritance** Succession Certificate.
e) Sale of Property/Business Copy of sale agreement/Title Deed	**f) Loan** Loan agreement	**g) Gift:** **Gift Deed:** Source of donor's wealth; Certified Identification documents of donor.	**h) Other income/wealth sources:** • Nature of income, amount, date received and from whom along with appropriate supporting documentation. • Where there nature of income is such that no supporting documentation is available (for e.g. Agricultural Income) Bank Statement may be obtained.

3.2.4. Customer Risk Assessment

DPMSs are required to conduct both enterprise risk assessment and individual customer risk assessment, particularly of new customers.[44] The enterprise risk assessment gives a macro assessment of risk in the DPMS, while the induvial customer risk provides a micro perspective. The customer risk assessment determines only the individual customer's risk profile. Once you have completed your enterprise risk assessment, the conclusions on the risk variables (i.e. customer, geography, products and services, and delivery channel) will inform your customer risk assessments.

Customer risk can be divided into the following groups:

(a) High risk;
(b) Medium risk;
(c) Low risk.

The high-risk indicators for the four main risk categories (i.e. customers, products/ services, delivery channels, and geographic locations) are as follows:

INDICATORS FOR CUSTOMER RISK ASSESSMENT		
Higher risk customers		
1. Politically Exposed Persons (PEP). Of a family member or known close associate of a PEP.	2. Customers paying in physical cash significantly above the RKR 2 million threshold	3. Customers wants to make cash payments in instalments with each cash payment below PKR 2 million threshold?
4. Customers wants to trade in of another item so cash payment by customer is below the PKR 2 million threshold for an item that is above this threshold.	5. The business relationship will be conducted in unusual circumstances (e.g. significant unexplained geographic distance between the OPMS and the client)	6. Customers conducting frequent online transactions from locations having tax amnesty to avoid taxes.
7. Customer buying an item that appears to be beyond customer's economic means e.g. stated occupation or business	8. Customer conducts numerous cash transactions over a short period of time without a business purpose. but the cumulative amount is substantial.	9. Discretionary trust (e.g. family trusts).

44. Regulation 4 DNFBP Regulations.

10. Non-Government Organization (NO), Not for Profit Organisation (NPO) or charity.	11. Legal persons or arrangements that are personal asset-holding vehicles.	12, Companies that have nominee shareholders or shares in bearer form/ or with complex ownership structures.
Higher risk products/services		
13. Accepting large cash payment from the customer.	14. Higher monetary value items (e.g. diamond) but small in size	15. Conducting transactions for the customer that would involve receipt of funds (cash) from unknown or un-associated third parties
16. Allowing for trade in as partial payment from the customer which results in the cash transaction to be under the threshold of PKR 2 million	17. Allowing for staggered cash payments (separate payments below PKR 2 million)	
Higher risk delivery channels		
18. Services or products provided exclusively via website (online sales), telephone. email. etc, where non face-to-face approach is used` Higher risk geographic locations		
Higher risk geographic locations		
19. The jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called for by FATF for taking counter-measures	20. Countries subject to sanctions, have been identified for embargos, for example, the United Nations	21. Countries identified by credible sources as having significant levels of corruption, or other criminal activity
23. Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities	24. Locations identified as high risk in NRA (including in Pakistan)	

3.2.4.1 Which type of Due Diligence is to be performed?

Once the customer risk has been determined i.e. low, medium, or high, the required customer due diligence is determined.

3.2.4.2 Simplified Due Diligence

Simplified DD may be applied to both the customer or beneficial owner, but only where lower risks have been identified through:[45]

- Adequate analysis through its own risk assessment;
- Any other risk assessments publicly available or provided by FBR; and
- In accordance with the AML/CFT regulations and commensurate with the lower risk factors.

After customer onboarding, under Simplified DD, legal identity and beneficial ownership can be verified, and the degree of continuous CDD can be decreased. Below are listed the main requirements for Simplified DD:

- Information to identify and verify identity;
- Information to identify and verify address;
- Take reasonable measures to verify identity of beneficial owner;
- If necessary, identify and verify natural person representing the customer;
- Scope for delayed verification of customers identity and beneficial ownership;
- Reduce the degree of ongoing monitoring and scrutinizing transactions.

It would be unlikely an individual customer paying for an expensive item in cash worth PKR 2 million or above would be considered as low risk. Use of cash payments, particularly for amounts over the threshold for expensive and highly portable items is normally associated with higher risk.

There may be lower risk circumstances when one DPMS is conducting a sales transaction with another DPMS. For example, if your supplier of items is a publicly listed company, it may be rated low risk and simplified due diligence may apply. This is subject to a risk assessment confirming low risk (publicly listed companies in

45. Regulation 10 DNFBP Regulations.

Pakistan, a FATF member country or a country with equivalent transparency standards for such companies).

There may be instances where the buyer is an authorised representative of a publicly listed company or financial institution regulated by the State Bank of Pakistan. The purchase may be for the purposes of a gift for a departing senior officer, e.g. CEO or Chairman of the Board, in which case the payment would be by cheque. Subject to the risk assessment, this may be a lower risk situation and suitable for Simplified DD.

3.2.4.3. Standard Due Diligence

The DNFBP Regulations do not expressly state the requirements for Standard DD. By assumption, standard due diligence applies if the customer is:

- Not at higher risk and not subject to EDD; or
- Lower risk and subject to Simplified DD.

Standard DD measures on customers include the following:

- Information to identify and verify identity;
- Information to identify and verify address;
- If necessary, identify and verify the natural person representing the customer
- Information to identify the identity of the beneficial owner;
- Take reasonable measures to identify the identity of the beneficial owner;
- Ongoing due diligence.

3.2.4.4. Enhanced Due Diligence

EDD applies to:

- PEPs and their families and close associates;
- Customers and transactions to, or from countries when called upon by the FATF;
- Any other customer rated high risk.

Given the risk associated with cash transactions, a customer paying in cash above the stipulated threshold or significantly above such threshold may be indicative of higher risk.

Examples of possible higher risk customers include:

- Customers that are discretionary trusts;
- Complex ownership structures (except for publicly listed companies);

- Bearer share ownership (if an owner is another company based overseas);
- Based offshore in a high-risk country.

For retail DPMS providers, the customers are most likely individuals for which the indicators of higher risk are different, particularly how the retail customer pays for the precious metal and/or stone, and may include the following:

- Customers whose economic/financial profile may not match the value of the precious metal and/or stone and still pay in cash;
- Customers who want to make cash payments in installments with each cash payment below PKR 2 million;
- Customers who want to trade in another item so that cash payment by the customer is below the threshold of PKR 2 million for an item that is otherwise worth PKR 2 million or more.

Enhanced CDD measures are:

- Information to identify and verify identity;
- Information to identify and verify address;
- If necessary, identify and verify natural person representing the customer;
- Information to identify and verify the identity of the beneficial owner;
- Information on the source of funds or wealth of the customer;
- Establish the source of funds or wealth, if a PEP;
- If a PEP, determine the source of funds and wealth;
- Senior management approval before accepting customer;
- Enhanced ongoing monitoring.

3.2.4.5 Customer Risk Assessment Template

Explanatory Notes:

- This is an example template for customer risk assessment for voluntary use. The DPMS may wish to amend this template to suit its own circumstances;
- The factors contained therein should be considered by the DPMS in carrying out its risk assessment for new customers. The list is non-exhaustive and the DPMS may consider additional factors relevant to their working environment;
- If the response to any of the questions listed in Section 1.1 is 'Yes', this means that the DPMS must not establish a business relationship with the customer;
- ·If the response to any of the questions listed in Sections 1.2 to 1.6 is 'Yes', this accounts for the indicators of higher risk factors. When there are multiple 'Yes' responses in the aforementioned sections or a 'Yes' to a PEP, the DPMS is required to conduct EDD which involves approval by senior management of the DPMS prior to accepting the new customer. The concerned staff member

should also consult with the designated compliance officer with regard to the risk factors identified;

- Note that this template is for risk assessment only. Separate templates for CDD which contain mandatory requirements can be found later in this Handbook. After the completion of CDD, the DPMS can then decide whether to accept the new customer or not.

SECTION 1.1: PROHIBITED PERSONS/ORGANISATIONS SCREENING

(refer point # 3 of the explanatory note)

	Response	
The customer. beneficial owner of the customer, person acting on behalf of the customer, or connected party of the customer matches the details in the following lists? (a) The "Lists of Proscribed Individuals and Entities" issued by the Ministry of Interior available on NACTA website; (b) Designated by. or under the authority of. the United Nations ("UN") Security Council under Chapter VII of the Charter of the UN. including in accordance with UN Security Council Resolutions. UN Sanctions: https://www.un.org/securitycouncial/countent/un-condolidated-list http://scsanctions.un.org/search/ Ministry of Foreign Affairs: http://mofa.gov.pk/unsc-sanctions/ http://www.secdiv.gov.pk/page/sro-unscr-sanctions	YES	NO
Ministry of Interior/NACTA http://nacta.gov.pk/proscribed-organizations-3/ http://nacta.gov.pk//pp/ http://nfs,punjab.gov.pk/ *Note: If there is a true match, the DPMS must also submit (i) a Suspicious Transaction (STR) to the FMU and (ii) a report to the FBR of match against a sanctions list.*		

SECTION 1.2: CUSTOMER'S RISK FACTORS

(refer point #4 of the explanatory note)

	Response	
Is the customer or its beneficial owner a Politically Exposed Person (PEP). family member of a PEP or close associate of a PEP? *Note "Politically exposed persons- or "PEPs" - means any person entrusted with a prominent public function by the State of Pakistan, a foreign country or an international organization and includes Heads of state or government, and member and senior officials of legislature. judiciary. executive. military and regulatory authorities. and senior executives of corporations, departments or bodies that are owned or controlled by the state*	YES	NO

Customers wants to pay in physical Cash for item that is significantly above the PKR 2 million threshold?	YES	NO
Customers wants to make cash payments in instalments with each cash payment below PKR 2 million threshold?	YES	NO
Customer buying an item in cash that appears to be beyond customer's economic means e.g. stated occupation or business?	YES	NO
Customer conducts numerous cash transactions over a short period of time without a business purpose. but the cumulative amount is substantial?	YES	NO
The customer is non-resident in Pakistan?	YES	NO
The customer or potential customer is a Non-Government Organization (NGO). Not for Profit Organization (NPO) or charity? *Note: The list of registered charitable organzations / NGOs / NPOs can be obtained from http://pcp.org.pk/pagestyle.php*	YES	NO
Business that is cash-intensive?	YES	NO
Is the customer in a high - risk industry? *Note: High risk industry includes (but not limited to) following businesses;* • Businesses dealing with precious metals (gold, saver, diamond mid stones etc.)- Real Estate dealers • High risk sectors identified in the NRA (except publicly listed companies and financial institutions regulated by the State Bank of Pakistan)	YES	NO
Is the customer a shell company. especially in cases where there is foreign ownership which is spread across jurisdictions? Note: Shell Company means an inactive company used as a vehicle for senors financial manoeuvres or kept dormant for future use in some other Capacity.	YES	NO
Does the customer have unusual or complex shareholding structure (e.g. involving 3 layers or more of ownership structure, different jurisdictions. trusts), given the nature of its business? *Note: The above excludes publicly listed companies in Pakistan and FATF member countries, or other countries with equivalent transparency standards for such countries.*	YES	NO

The business relationship will be conducted in unusual circumstances (e.g. significant unexplained geographic distance between the REA and the customer), non-resident customers?	YES	NO
The customer is a legal persons or arrangement that is a personal asset-holding vehicle?	YES	NO

SECTION 1.3: COUNTRY / GEOGRAPHICAL RISK FACTORS

(refer point # 4 of the explanatory note)

	Response	
Countries identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering/terrorism financing or subject to a FATF statement? Note: - For countries in black list, please refer http://www.fatfgaft.org/countries/#gigh-risk - For countries in grey list, please refer http;//www.fatfgaft.org/countirs/#other-monitored-jurisdictins	YES	NO
Countries subject to sanctions. embargos or similar measures issued by. for example. the United Nations? United Nations: http://scsanctions.un.org/search/	YES	NO
Countries identified by credible sources as having significant levels of corruption other criminal activity? Transparency International: https://www.transparency.org/en/cpi/2019/results	YES	NO
Countries or geographic areas identified by credible sources as providing finding or support for terrorist activities, or that have designated terrorist organizations within their country? Institute of Economics and Peace: http://www.economicsandpeace.org/GlobalTerrorism index	YES	NO
Does the customer. beneficial owner or person acting on behalf of the customer lave dealings in high risk geographic regions, including Pakistan as identified in he National Risk Assessment 2019? Note: The high risk areas / jurisdictions includes western borders / FAT./Southern Punjab and the eastern border.	YES	NO

Countries known for high levels of financial secrecy or with low tax rates? Tax Justice Network: http://fsi.taxiustice.net/en/	YES	NO

SECTION 1.4: SERVICES / PRODUCTS RISK FACTORS

(refer point # 4 of the explanatory note)

	Response	
Accepting large cash payments (significantly above the PKR 2 million threshold) from the customer?	YES	NO
Accepting cash payments from an unknown or un-associated third party on behalf of the customer?	YES	NO
Delivering the high value item or accepting collection from a person who is unknown to the DPMS i.e. the customer who paid for the item is not the beneficiary	YES	NO
Allowing for trade in as partial payment from the customer which results in the cash transaction to be under the threshold of PKR 2 million	YES	NO

SECTION 1.5: DELIVERY / PRODUCTS RISK FACTORS

(refer point # 4 of the explanatory note)

	Response	
Will services or products be exclusively via telephone, email. etc. Where non face-to-face approach is used?	YES	NO

SECTION 1.6: REPUTATIONAL RISK SCREENING

(refer point # 4 of the explanatory note)

	Response	
Has the REA performed further screening of details of customer. beneficial owmer of the customer, person acting on behalf of the customer, or connected party of the customer against other reliable sources. for example. Google. the sanctions lists published by the Office of Foreign Assets Control of the US Department of the Treasury? Are there adverse news or information arising?	YES	NO

CUSTOMER RISK RATING

Low Risk ⟶ Simplified Due Diligence
Medium Risk ⟶ Standard Due Diligence
High Risk ⟶ Enhanced Due Diligence

Note: Please complete CDD before making the recommendation below. If rejected because of failure to complete CDD or suspicion of ML/TF, a suspicious transaction report should be made to the FMU

Customer Acceptance Recommendation:

☐ **Accept** ☐ **Reject**

Assessed by:	**Approved by:**
Name: _____	Name: _____
Designation: _____	Designation: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

3.2.5. Prohibited Customers and Risk Screening

REAs are prohibited from providing services to any persons or entities and their beneficial owners that are designated/proscribed by SROs or notifications issued by MoFA, NACTA, and MoI.[46] All new customers must be screened against the SROs issued, and existing customers on a regular basis. This is covered in detail in the section of the Guidelines on targeted financial sanctions.

If the customer is a legal person, it is important to check whether it is still registered with the SECP. The company may have been deregistered. In this scenario, the REA cannot accept the new customer as the legal person no longer exists. The REA can check online at the SECP website: https://eservices.secp.gov.pk/eServices/NameSearch.jsp.

While not mandated in the AML/CFT legislations, the REA should for higher risk customers, do a reputational risk screening of the customer for any adverse reports e.g. media reports, fines, punishments, corruption etc. This could be a time consuming process if the REA does not have a subscription to a commercial risk screening provider. So, if the REA does not have such a subscription, this is on a risk basis only which includes higher risk customers such as PEPs.

3.2.6. Delayed Verification

CDD measures must normally be completed before entering into a business relationship with the customer. When most of the information needed has been

46. Regulation 8(1) DNFBP Regulations.

collected before the business relationship has begun, it may be acceptable to have a short extension to allow for verification of beneficial ownership, or source of wealth or funds. Circumstances of delayed verification outside of simplified CDD when the risk is not rated low will be infrequent.

Delayed verification is permitted under the law subject to certain conditions as mentioned below:[47]

MANAGING DELAYED CDD VERIFICATION

When there is delayed in **the verification process,** there are clear conditions associated with this exception:

- it is completeld as soon as reasonably practicable;
- this is essential not to interrupt the normal conduct of business;
- the ML/TF risks are effectively managed; and
- the REA shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

To avoid any contractual disputes, it must be made clear to the customer that if CDD cannot be completed. the REA may have to end the relationship.

3.2.7. Unable to complete Customer Due Diligence

Where a DPMS is unable to complete CDD, the DPMS shall:[48]

(a) Not open the account, commence business relations or perform the transaction; or terminate the business relationship, if any; and
(b) Promptly consider filing an STR in relation to the customer.

If the DPMS cannot complete the CDD process, even when verification is delayed after the start of the business relationship, the DPMS must not provide, or cease to provide services. These circumstances could be:

(a) If a prospective customer refuses to provide evidence of identity or other information properly requested as part of CDD;
(b) Where the DPMS is not satisfied with the information and verification commensurate with the higher risk profile of the customer; and

47. Regulation 8(13) to (14) DNFBP Regulations.
48. Section 7D AMLA.

(c) Where too many questions may be tipping off the customer of suspicion by the DPMS.

Tipping off in this context means the customer may become aware that you are suspicious of the purpose of the transaction, or source of wealth or funds.

3.2.8. Customer Due Diligence and Tipping Off

If the DPMS forms a suspicion of ML/TF and reasonably believes that performing the CDD process will tip-off the customer, the DPMS shall not pursue the CDD process and shall file an STR.[49]

3.2.9. Ongoing Monitoring of New Customers

In most instances, the business relationship is one-off and there will not be a need for ongoing CDD. However, there are some customers who may be regular or repeat customers, in which case DPMSs must conduct ongoing due diligence of the business relationship.[50] Once a new customer has been accepted after CDD has been completed, there is no need to repeat the CDD process every time the customer returns. Ongoing CDD is important to maintain up-to-date information on customers so that:

(a) The risk assessment of a particular customer in case of change in circumstances can be updated, e.g. from medium to higher risk; and
(b) Further due diligence measures can be carried out, if necessary.

3.2.10. Existing Customers[51]

It is important for DPMSs, especially larger companies, to have a centralized database of customers with all the information collected which will:

(a) Allow information collected on the customer from various business lines to be accessed by all staff interacting with the customer;
(b) Help avoid the same questions and information asked of the customer and will enhance customer satisfaction.

49. Section 7D(2) AMLA.
50. Regulation 8(6) DNFBP Regulations.
51. Existing customers refer to customers of the DPMS prior to 29th September 2020, i.e. when the DNFBP Regulations came into force.

TABLE ON EXISTING AND NEW CUSTOMERS

Exiting customers (prior to AML/CFT requirements)		New customers (Agter AML/CFT requiremetns Coming into force and effect)
Dormant	**Active**	
No ongoing business relationship or services	Ongoing services	Subject to the full CDD requirements (if paying in cash above the threshold)
They will need senior management decision whether they should be treated as new customers, or existing. For example, if dormant for 2-3 years they could be treated as new customers to minimise risk .	CDD would be trigger if suspicion of ML/TF, or material change in the customer's profile based on a new engagement, or ongoing monitoring. There should also be a periodic review of exiting customers, particularly those that may be in the higher risk categories e.g. those that are engaging in cash sales transaction over the threshold.	

3.2.11. Third-party conducting Customer Due Diligence

A third party can also conduct CDD on behalf of the DPMS.[52] The conditions placed upon the DPMS when relying on third parties are as follows:

(a) DPMSs are liable for all CDD requirements;
(b) The information required for CDD is to be acquired immediately;
(c) The records of CDD obtained from the third party should be kept;
(d) The DPMS should be satisfied that the third party is under the supervision of an AML/CFT regulatory authority;
(e) The DPMS should be satisfied that if the third party is overseas, the country it is based in has a satisfactory level of AML/CFT and country risk.

52. Section 7B AMLA and Regulation 12 DNFBP Regulations.

If the third party is in the same corporate group as the DPMS, the DPMS can consider the five requirements mentioned above to be satisfied if:

1) The corporate group applies CDD and record-keeping requirements in accordance with the AMLA and its associated regulations;
2) The implementation of the group CDD, record keeping and PEP requirements is supervised by an AML/CFT regulatory authority or an equivalent foreign authority;
3) The corporate group has adequate measures in place to mitigate any higher country risks.

For a retail DPMS servicing walk-in customers, reliance on third parties may not be practical as these are individual customers. For example, it is much more practical for a jewelry store to obtain the NADRA issued identification document of a domestic customer and the passport of a foreign customer, rather than relying on a third party for CDD.

3.3. Customer Due Diligence Templates

A. Customer Due Diligence Form Template (Individual/Sole Proprietor)

Explanatory Notes:

- All the information and documents requested in this form must be provided by any new client/customer in order to comply with Pakistan's AML/CFT legal regime;
- The information collected shall remain confidential unless formally requested by government authorities pursuant to AML/CFT laws.

PART 1. BASIC IDENTIFICATION INFORMATION	VERIFICATION DOCUMENTS
Full Legal Name (as per ID document):	**Residents:** CNICs/ Smart National Identity Card (SNIC) issued by NADRA **Non Residents:** National Identity Card for Overseas Pakistanis (NICOP) and/or Passport issued by NADRA for Non-resident overseas Pakistanis or those who have dual nationality: or Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistani who have given up Pakistan nationality: or Form B or Juvenile card issued by NADRA to children under the age of 18 years: or Where the natural person is a foreign national, either an Alien registration card (ARC) issued by NADRA or a Passport having valid visa on it or any other proof of legal stay along with passport. **Note:** If only photocopies and not originals or certified true copies provided of the above. electronic verification is required of the authenticity and information contained in the photocopies. http://id.nadra.gov.pk/identity-documents/verification-services/
Date of Birth:	As above
Place of Birth:	As above
If non-resident, country of residence:	As above
Physical Address:	Certificate of Registration. Utility statement with address, telephone account statement with address. etc
Landline Number:	N/A
Email Address:	N/A

PART 2: POLITICALLY EXPOSED PERSON	
Are you or any beneficial owners entrusted with a prominent public function by the State of Pakistan, a forequi country or an international organization and includes Heads of state or government. and members and senior officials of legislature, judiciary. executive. military and regulatory authorities, and senior executives of corporations, departments or bodies that are owned or controlled by the state?	Yes/No
Are you or a beneficial owner a family member of the above?	Yes/No
Are you or a beneficial owner a family member of the above?	Yes/No
PART 3: DETAIL ON THE BUSINESS **Note: Only complete if the customers is a sole trader/proprietor. If not, the part3 is not applicable.**	**VERIFCATION DOCUMENTS**
Business Name:	Certificate of Registration
Business Address:	Certificate of Registration Utility statement with address, telephone account statement with address. etc
Registration Number:	Certificate of Registration
Please provide details of the industry and business (e.g. Products/services)	N/A
Does the company have operations in other geographic regions in Pakistan? If the above is "Yes", please provide the names of those regions?	N/A
Which are the primary countries in which the business has dealings with, if any?	N/A
PART 4: SOURCE OF FUNDS OR WEALTH	
Occupation or business	
What is the main source of income or wealth of the customer?	

Note: For customer subject to enhanced due diligence.

PART 5: ARE YOU ACTING FOR SOMEONE ELSE?

If No, just marked as Not Applicable (N/A) If Yes, please provide details below

	Verification Details (Original, certified true copy or electronic verification)
Name:	CNICs/ Smart National Identity Card (SNIC) issued by NADRA or Equivalent for non-residents (refer Part 1 above)
Address:	Utility or telephone bill with physical address: or Other document with evidence of physical address
Relationship to customer: e.g. lawyer/accountant.	**Attach original of official company letter** authorising individual to enter into contractual relations with DPMS on behalf of the customer e.g. from the governing body/board if not a company director.

PART 6: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION

Certificate of Registration, if sole trader/proprietor
Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA
If non-resident. Original or certified true copies of National Identity Card for Overseas Pakistanis (NICOP). Pakistan Origin Card. Alien Registration Card or foreign passports
Utility statement, telephone account statement etc with physical address
If applicable, letter authorising individual to act on behalf of the customer

Note: If only photocopies and not originals provided of the above, electronic verification is required of the authenticity and information contained in the photocopies.

DECLARATION BY PERSON
I declare that the information provided in this form is true and correct. I have reviewed the answers and I confirm that I an satisfied that, to the best of my knowledge, after undertaking all reasonable inquiries, all answers are true and correct.
Signature:
Name of person:
Date:
Location:

B. Customer Due Diligence Form Template (Company)

Explanatory Notes:

- All the information and documents requested in this form must be provided by any new client/customer in order to comply with Pakistan's AML/CFT legal regime;
- The information collected shall remain confidential unless formally requested by government authorities pursuant to AML/CFT laws.

PART 1. IDENTIFICATION INFORMATION	VERIFICATION DOCUMENTS
Full Legal Name:	Certificate of Incorporation Check online: http://eservice.secp.gov.pk/eServices/NameSearch.jsp
Director Name (s):	CNICsJ Smart National Identity Card (SNIC) issued by NADRA of all directors Foreign passport
Company information (ownership and control)	Article of Association Memorandum of Association
Registration Number:	Certificate of Incorporation
Country of Incorporation:	Certificate of Incorporation
Date of Incorporation:	Certificate of Incorporation

Registered Address:	Certificate of Incorporation
Physical Address:	Certificate of Incorporation, Utility statement with address, telephone account statement with address, etc
Landline Number:	N/A
Email Address:	N/A
PART 2: BENEFICIAL OWNERSHIP INFORMATION	**VERIFICATION DOCUMENTS**
1. Shareholders: e.g. Names of individuals (natural persons) shareholders holding 25% or above ownership Note: This includes where the customer is owned by one or more companies.	**Details of company:** 1. SECP website to confirm registration: https://eservices.secp.gov.pk/eServices/NameSearch.jsp 2. SECP registered declaration for commencement of business as required under the Companies Act. 2017 (XIX of 2017). as applicable: 3. Register of Members of a Company. Section 119 of the Companies Act. 2017 (Act no. XIX of 2017) 4. Register of beneficial Ownership maintained by the Company. as required under Section 123A of the Companies Act 5. Articles of Association/ Memorandum of Association
2. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g. - appoint or remove the majority of the board of directors. or its chair, or CEO of the company:	
3. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g. - personal connections to persons in positions described above or that possess ownership - close and intimate family relationships - historical or contractual associations if a company defaults on certain payments	**Details of individuals (beneficial owners):** **Originals or certified true copies of:** **1. Residents:** CNICs/ Smart National Identity Card (SNIC) issued by NADRA **2. Non Residents:** National Identity Card for Overseas Pakistanis (NICOP) and/or Passport issued by NADRA for Non-resident / overseas Pakistanis or those who have dual nationality: or

4. Senior managing official: Where no natural person is identified under 1 to 3 above after reasonable measures have been made - the identity of the relevant natural person who holds the position of senior managing official.	Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistanis who have given up Pakistan nationality: or Form B or Juvenile card issued by NADRA to children under the age of 18 years: or Where the natural person is a foreign national, either an Alien registration card (ARC) issued by NADRA or a Passport having valid visa on it or any other proof of legal stay along with passport. Note: If only photocopies and not originals or certified true copies provided of the above, electronic verification is required of the authenticity and information contained in the photocopies. http://id.nadra.gov.pk/identity-documents/vericationservices/

PART 3: POLITICALLY EXPOSED PERSON

	Response	
1. Are you or any beneficial owners entrusted with a prominent public function by the State of Pakistan, a foreign country or an international organization and includes Heads of state or govenument, and members and senior officials of legislature. judiciary. executive. military and regulatory authorities, and senior executives of corporations. departments or bodies that are owned or controlled by the state?	YES	NO

2. Are you a family member of the above?	YES	NO
3. Are you a close associate of the above?	YES	NO
PART 4: DETAILS ON THE BUSINESS		
1. Please provide details of the industry and business (e.g. products / services)		
2. Number of staff employees?		
3. Does the company have operations in other geographic regions in Pakistan? 4. If the above is "Yes", please provide the names of those regions?		
5. Which are the primary countries in which the company has dealings with. if any?		
6. Does the company deal with any individual or entity from countries that are subject to UN sanctions or embargoes? 7. If the above is "Yes", please indicate the specific countries and the nature of those dealings?		
PART 5: SOURCE OF FUNDS OR WEALTH		
4. What is the main source of funds or wealth of the business?		
5. Income last financial year?		
6. Assets held by the customer?		
Note: For customer subject to enhanced due diligence.		

PART 6: INDIVDIUAL ACTING ON BEHALF OF COMPANY

Where any individual is acting on behalf of the Company.
please fill the following section:

	Verification Details (Original, certified true copy or electronic verification)
Name:	CNICs/ Smart National Identity Card (SNIC) issued by NADRA or Equivalent for non-residents (refer Part 2 above)
Address:	Utility or telephone bill with physical address: or Other document with evidence of physical address
Relationship to customer: e.g. company director, employee or lawyer/accountant.	**Attach original of official company letter** authorising individual to enter into contractual relations with REA on behalf of the customer e.g. from the governing body/board if not a company director.

PART 7: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION

1. Certificate of Incorporation

2. SECP registered declaration for commencement of business as required under the Companies Act. 2017 (XIX of 2017)

3. Register of Members of a Company. Section 119 of the Companies Act. 2017 (Act no. XIX of 2017)

4. Register of Beneficial Ownership Information. Section 123A of Companies Act and Compliance Certificate

5. Article of Association. Mentorandum of Association

6. Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA of all directors and beneficial owners

7. Originals or certified true copies of National Identity Card for Overseas Pakistanis (NICOP), Pakistan Origin Card. Alien Registration Card or foreign passports of directors and beneficial owners

8. Utility statement, telephone account statement etc with physical address
9. Letter authorising individual to act on behalf of the customer

Note: If only photocopies and not originals provided of the above, electronic verification is required of the authenticity and information contained in the photocopies.

DECLARATION BY PERSON AUTHORISED TO ACT ON BEHALF OF COMPANY:

I declare that the information provided in this form is true and correct. I have reviewed the answers and information and I confirm that I am satisfied that. to the best of my knowledge. after undertaking all reasonable inquiries. all answers are true and correct.

Signature:

Name of person acting on behalf of company:

Position in or relationship with the company:

Date:

Location:

C. Customer Due Diligence Form Template (Trust)

Explanatory Notes:

- All the information and documents requested in this form must be provided by any new client/customer in order to comply with Pakistan's AML/CFT legal regime;
- The information collected shall remain confidential unless formally requested by government authorities pursuant to AML/CFT laws.

PART1. BASIC IDENTIFCATION INFORMATION	VERIFCATION DOCUMENTS
Full Legal Name of Trust:	Trust deed/agreement
Date of Trust Formation:	
Physical Address of Trust:	
TRUST DEED/SETTLOR/PROTECTOR	
Name (s) of Trustees:	Trust deed CNIC # and address for each individual trustee
If the trustee is a corporate trustee, the name of the individual authorised to represent the corporate trustee:	Trust deed Certificate of Incorporation CNIC # and address for each individual representing the corporate trustee
Name of Settlor:	Trust deed CNIC # and address of the protector
Name of Protector. if any:	Trust deed CNIC # and address of the protector
BENEFICIARIES	
Names of all beneficiaries with 10% or above share:	Trust deed CNIC # and address for each beneficiary

If a beneficiary is a corporate beneficiary. the name of the individual authorised to represent the corporate beneficiary:	Trust deed Certificate of incorporation CNIC # and address for each authorised representative
If a beneficiary is another trust. the full details of that trust (as required in this form).	Trust deed and information required on the trust
If more than 10 beneficiary. or beneficiaries are not names, the names of the different groups of beneficiaries e.g. grandchildren. children. groups benefiting from the charity etc	Trust deed Memorandum of Association and Rules & Regulations of your Trust.
CONTACT DETAILS	
Landline Number:	N/A
Email Address:	N/A
PART 2 : POLITICALLY EXPOSED PERSON	
Are you or any beneficial owners entrusted with a prominent public function by the State of Pakistan. a foreign country or an international organization and includes Heads of state or government. and members and senior officials of legislature. judiciary. executive. military and regulatory authorities, and senior executives of corporations. departments or bodies that are owned or controlled by the state?	Yes/No
Are you or a beneficial owner a family member of the above?	Yes/No
Are you or a beneficial owner a close associate of the above?	Yes/No

PART 3 : DETAILS ON THE BUSINESS
Please provide details of the industry and business (e.g. products / services):
Does the company have operations in other geographic regions in Pakistan? If the above is -Yes". please provide the names of those regions?
Which are the primary countries in which the business has dealings with. if any?

PART 4: SOURCE OF INCOME OR WEALTH	
What is the main source of income of the business?	
Income last finacial year?	
Asset held by the customer?	

PART 5: CHECK LIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION
Certificate of Registration
Trust deed/agreement
Original or certified true copy CNIC's/Smart National Identity Card (SNIC) issed by NADRA
If non-resident, original or certified true copy of foreign passport of trustee or beneficiaries
Utility statement, telephone account statement etc with physical address

Note: If only photocopies and not originals provided of the above, electronic verification is required of the authenticity and information contained in the photocopies.

DECLARATION BY TRUSTEE

I declare that the information provided in this form is true and correct. I have reviewed the answers and information and I confirm that I am satisfied that. to the best of my knowledge. after undertaking all reasonable inquiries. all answers are true and correct.

Signature:
Name of person acting on behalf of company:
Position in or relationship with the company:
Date:
Location:

4. RECORD KEEPING

4.1. LEGAL REQUIREMENTS

The main purpose for record-keeping by DPMSs is evidentiary, both to showcase their implementation efforts of AML/CFT legislation and to facilitate investigations by law enforcement authorities. The DNFBP is required to promptly satisfy any inquiry or order from the FBR, designated law enforcement agencies, or FMU, for the supply of CDD information and transaction records under AMLA.[53]

Records can be maintained in paper form (in the form of books) or stored in a computer or any electronic device (or on microfilm).[54] As per the law, every reporting entity is to maintain:

(a) A record of all transactions for at least five years after their completion.[55]
(b) Records of account files, business correspondence, documents, records obtained by CDD (including copies of identification documents, applications forms, and verification documents), and the results of any analysis undertaken, for at least five years after the termination of the business relationship.[56]
(c) All records related to filed STRs and CTRs for at least ten years after reporting of transaction under Sections 7(1), (2), and (3) of AMLA.[57]

Furthermore, although not expressly mentioned, as a rule of thumb, DPMSs should maintain records of enterprise risk assessments, procedures, and AML/CFT training records including staff attendance for at least 5 years. However, where transactions, customers, or instruments are involved in litigation or the same are required by a court of law or other competent authority, the DNFBP shall retain any 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. [58]

According to the law, the records mentioned above are sufficient to permit the reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved, and the customer involved in the transaction so as to provide, when necessary, evidence for the prosecution of criminal activity.

53. Regulation 6(5) DNFBP Regulations.
54. Section 2(xxxii) AMLA and Regulation 6(2) DNFBP Regulations.
55. Section 7C AMLA and Regulation 6(3) DNFBP Regulations.
56. Ibid.
57. Section 7(4) AMLA.
58. Regulation 6(4) DNFBP Regulations.

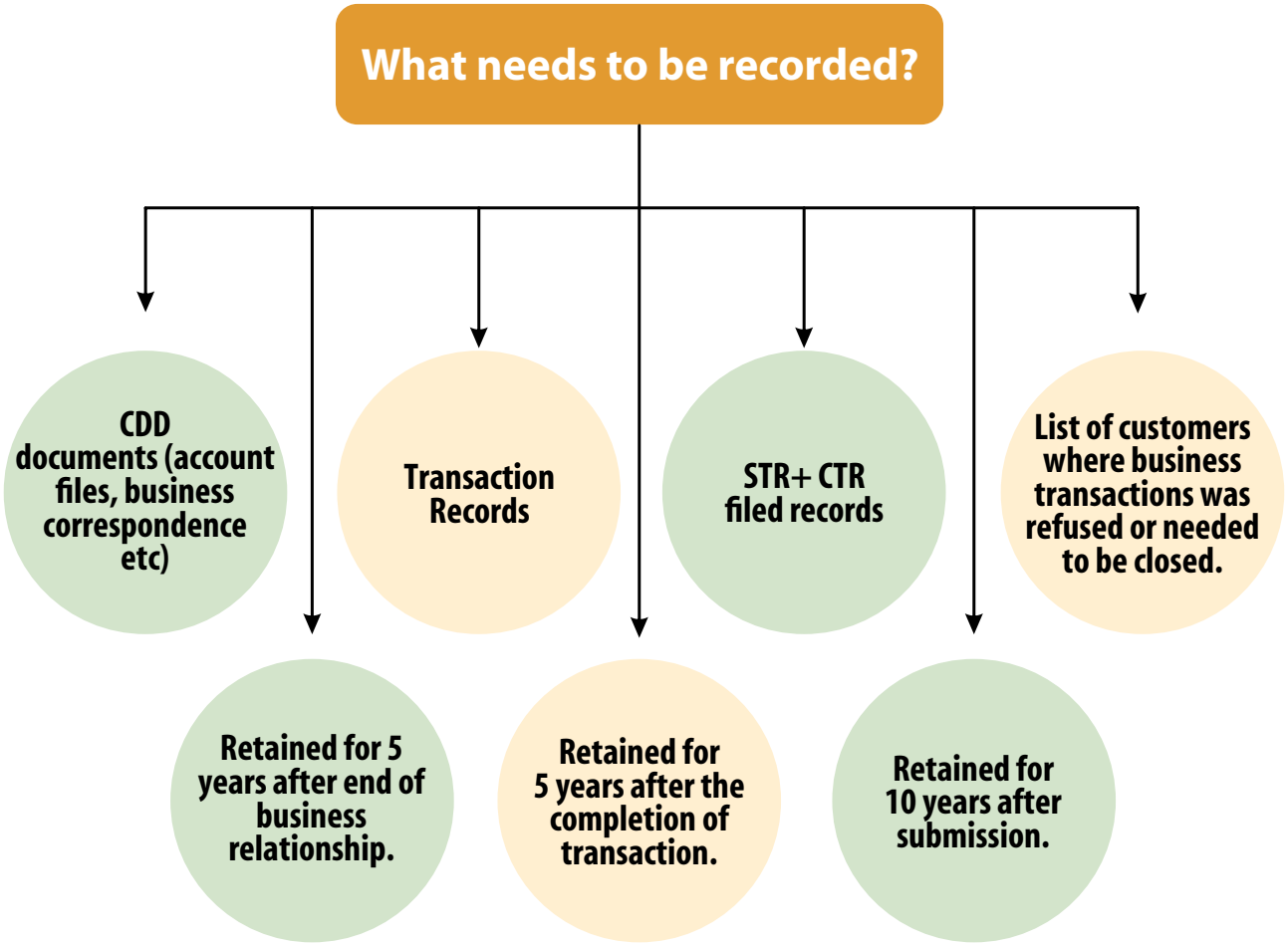
DPMSs must keep a list of all such customers where the business transaction was refused or needed to be closed either on account of the failure of the customer to provide:

(a) Relevant documents under Regulation 6(1) of the DNFBP Regulations; or
(b) Original document for viewing as required under Regulation 6(2) of the DNFBP Regulations.[59]

4.2. OPERATING PROCEDURES

4.2.1 Record-keeping Requirements

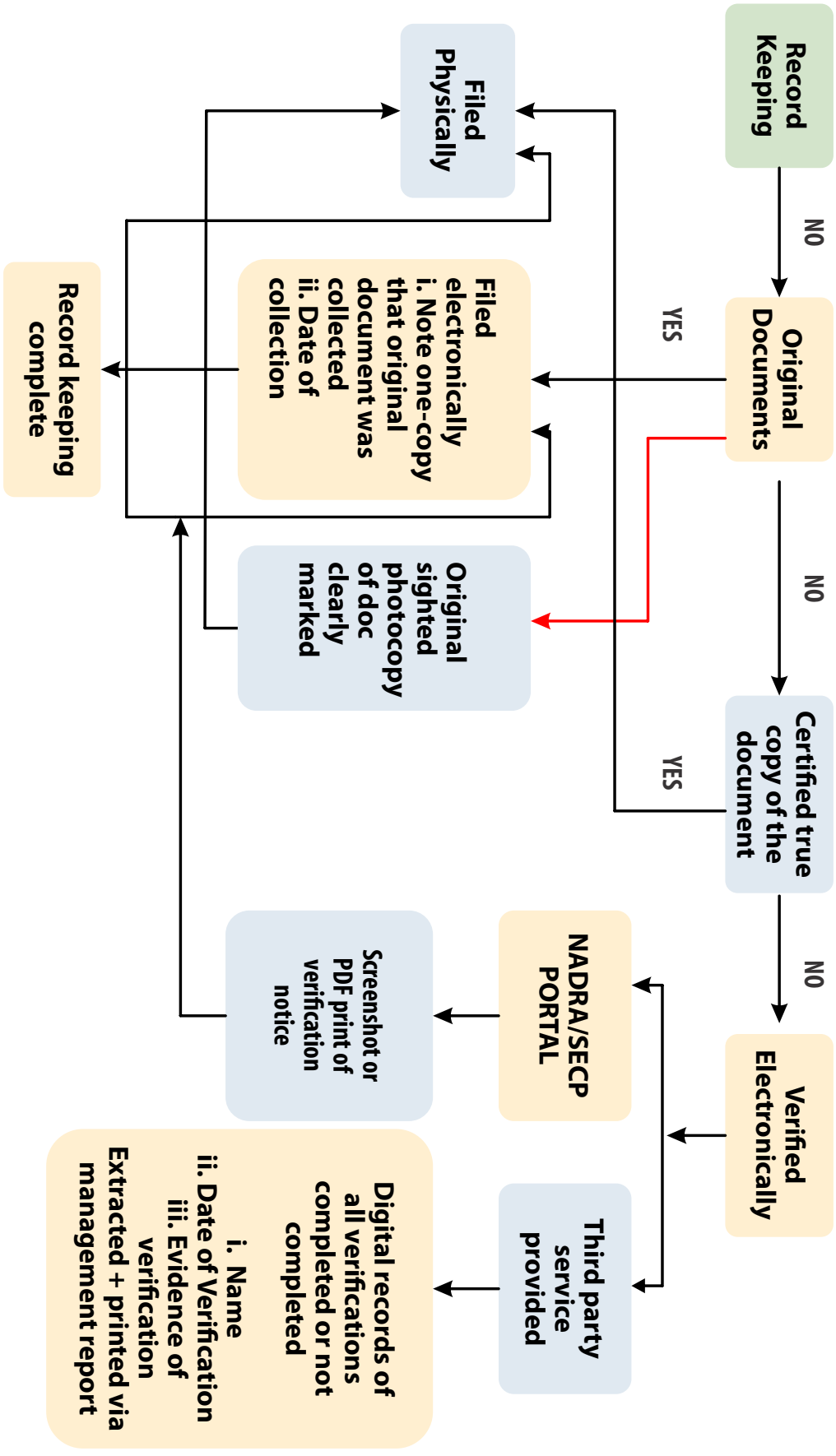
The type of documents that need to be kept as part of the DPMS's record and the respective durations are as follows:



59. Regulation 6(7) DNFBP Regulations.

4.2.2. How to Maintain Records

Below is a process chart that explains the record keeping process:



5. RISK ASSESSMENT AND MITIGATION

5.1. LEGAL REQUIREMENTS

Every reporting entity is to take proper steps, according to AMLA and any rules or regulations issued thereunder, to recognize, assess, evaluate, and understand the risks which can be faced by its business particularly in regards to countries or geographic areas, customers, products, transactions, services or delivery channels.[60] This means undertaking an enterprise risk assessment for ML/TF which would include:

(a) Documenting their risk assessment;
(b) Considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
(c) Keeping the assessment up to date; and
(d) Having appropriate mechanisms to provide risk assessment information to FBR.[61]

DNFBPs are also required to do the following:

(a) Have policies, controls, and procedures, which are approved by senior management, to enable them to manage and mitigate risks that have been identified in its own risk assessment and any other risk assessment publicly available or provided by FBR;
(b) Monitor the implementation of those controls and enhance them if necessary; and
(c) Take enhanced measures to manage and mitigate the risks where higher risks are identified.[62]

DNFBPs may take simplified measures to manage and mitigate risks, if lower risks have been identified. However simplified measures are not permitted whenever there is a suspicion of ML/TF.[63]

Where there is the development of new products, businesses and practices, including new delivery mechanism, and the use of new and pre-existent technology, DNFBPs are to identify and assess the ML/TF risks that may arise.[64] Moreover, prior to

60. Section 7F AMLA and Regulation 4(1) DNFBP Regulations.
61. Regulation 4(1) DNFBP Regulations.
62. Regulation 4(2) DNFBP Regulations.
63. Regulation 4(3) DNFBP Regulations.
64. Regulation 5(1)(a) DNFBP Regulations.

the launch or use of product, practice or technology, DNFBPs shall undertake the risk assessment and take appropriate measures to manage and mitigate the risks.[65]

5.2. OPERATING PROCEDURES

5.2.1. Money Laundering and Terrorist Financing risks associated with Precious Stones and Metals

There are many ML/TF risks associated with precious stones and metals, some of which are listed below:

General:

- Can be easily hidden, transported domestically or internationally, and dispersed to third parties;
- Luxury items such as jewelry can be used to bribe government officials;
- High-value goods are a practical option for ML/TF because there is often no paper trail, transactions are quick and easy to undertake, and they are facilitated with cash that is legal tender;
- These goods may be attractive to criminals because they are sometimes difficult to authenticate. As a result, certain items may appear less valuable than they are and therefore are not recognized as items used to launder illicitly derived funds.

Use of cash:

Cash remains a popular vehicle for transactions associated with criminal offences because it:

- Is anonymous and flexible;
- Exists outside of formal financial institutions;
- Does not require any record keeping;
- There is no paper trail.

Gold:

- Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily and it can also be used as currency itself, e.g., by hawaladar;
- Gold is available in a variety of forms, e.g., bars, coins, jewelry, or scrap, and trades internationally in all these forms;
- Gold has a high actual value and can be found in relatively small sizes, facilitating its transport, purchase, and sale in several regions around the world;

65. Regulation 5(1)(a) DNFBP Regulations.

- Gold also preserves its value regardless of its form whether it comes in the form of bullions, golden articles, or is melted.

Diamond:

- Diamonds are easily portable and traded around the world due to the small size of diamond stones;
- They are unlikely to draw the attention of law enforcement as they are not detected by metal detectors and a very large value can be easily concealed due to their small size;

5.2.2. Enterprise Risk Assessment

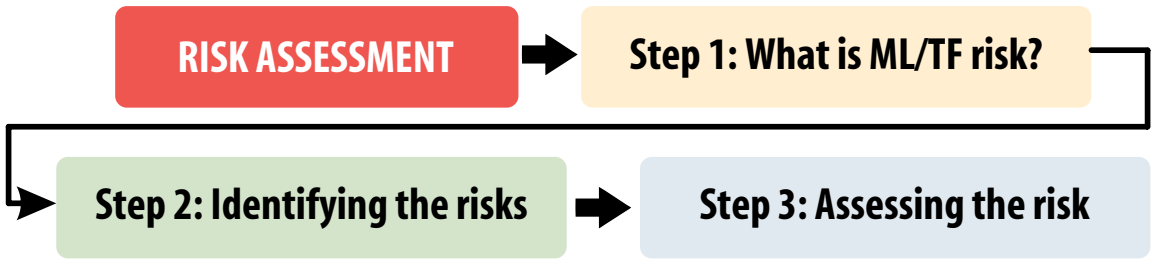
The key purpose of an ML/TF enterprise-wide risk assessment is to drive improvements in risk management by identifying the general and specific ML/TF risks the DMPS is facing, determining how these risks are mitigated by the DPMS's programme controls, and establishing the residual risk that remains for the DPMS. The DPMS's AML/CFT programme must be based on the DPMS's risk assessment.

The risk assessment should be approved by the DPMS's senior management. The risk assessment should therefore also include proposed mitigation measures needed, including AML/CFT controls and procedures identified by the risk assessment.

The ML/TF enterprise risk assessment is not a one-time exercise and should be updated on a regular basis, or when there are material or significant changes in specified services provided by the DPMS. The DNFBP Regulations is silent on the frequency of its update, but based on international practices, it should be reviewed and updated at least once every two years.

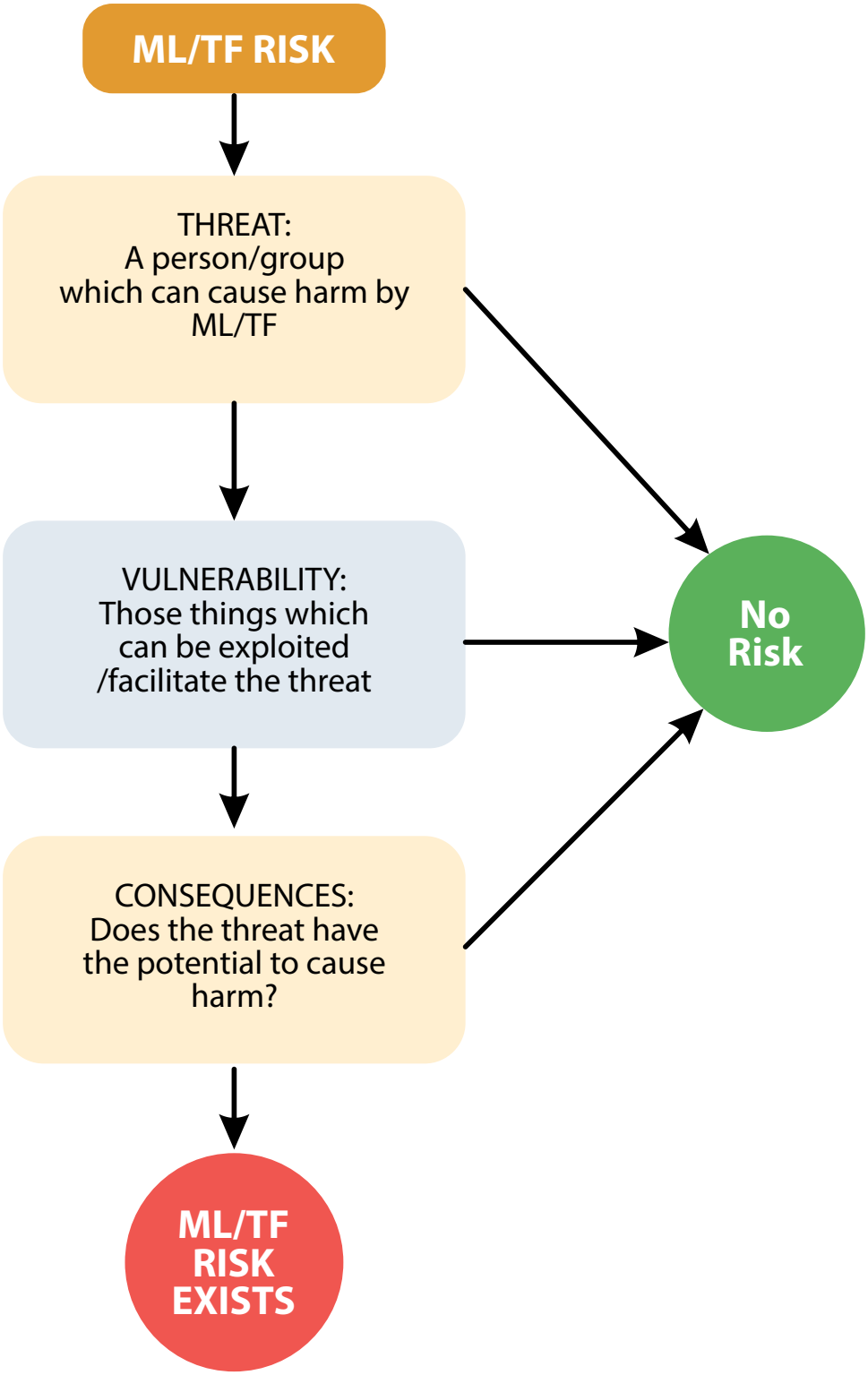
The enterprise risk assessment is separate from a customer risk assessment; the latter must be completed for every new customer before the new customer is accepted, and the risk rating reviewed and updated, if necessary, under ongoing CDD.

Conducting an enterprise risk assessment contains three steps as indicated below:



5.2.3. What is a Money Laundering/Terrorist Financing Risk?

The following diagram can help in determining whether there is an ML/TF risk:



5.2.4. Identifying the Risk

The four mandatory risk categories are customer risk, country and geography risk, products and services risk (including technology), and products and services delivery channel risk (including technology).

(i) Customer risk:

Retail customers of precious metals or precious stones, including jewelry will, in general, not have a business purpose for the purchase of precious metals or stones. A purchase is likely to be made purely for personal reasons.

Given most customers are retail, walk-in customers, the indicators pertain to unusual patterns in a sale transaction, e.g. avoiding the PKR 2 million threshold, or the value of the item is beyond the stated income of the customer or is not commensurate with the expected income derived from the occupation of the customer.

In the case of a DPMS buying or selling for another DPMS, there should be an identifiable business reason for the buying or selling of precious metals or stones.

(ii) Product/Service risk:

All precious metals and stones can potentially be used for ML/TF, but the utility and consequent level of risk are likely to vary depending on the value of the product. Below are some factors to consider when assessing product/service risk:

- Unless transactions involve very large quantities, lower-value products are likely to carry less risk than higher-value products;
- Gold can be high-risk. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself. Gold is available in a variety of forms, e.g. bars, coins, jewelry, or scrap, and trades internationally in all of these forms;
- The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of LEAs are at greater risk of being used in cross-border ML. For example, diamonds are small, lightweight, not detectable by metal detectors, therefore a very large value can be easily concealed;
- Accepting large cash payments increases the risk, especially in large amounts, which can be a warning sign, especially if cash is used anonymously or intentionally to hide an identity.

(i) Geographic risk:

Normally retail purchases are made in person, although the buyer may be a visitor from overseas, particularly wealthier customers who may find the prices less expensive than in their home countries. This in itself is not indicative of higher risk, but the use of large amounts of cash may. Geographic risk factors could be important for DPMSs that import or export precious metals and stones.

(ii) Channel of delivery:

Someone buying or paying on behalf of the customer may be indicative of higher risk. However, it is relatively common in jewelry purchases in Pakistan that a female will select an article, and a male will make payment later while directing delivery to the woman. If the person paying is unrelated to the customer then the risk is higher.

The DPMS may identify and assess the risk by using risk indicators under each of the four risk categories. The following table contains major risk indicators which are used globally including in FATF guidance documents.

Risk Indicators for Higher Risk	
Customer types (throat)	• Channels of delivery (vulnerability) Paying in cash equal or above the PKR 2 million threshold. • Payment by or delivery to third parties unrelated to buyer. • Structuring payments (separate payments below PKR 2 million(to avoid CTR threshold. • Value of item is beyond the stated occupation or income of customer e.g. source of wealth or funds.
Products / Services/ (vulnerability)	• Higher monetary value • Gold • Small size but high monetary Value • Investment or storage services • Large market and easy to resell

Channels of delivery (vulnerability)	• Use of cash • Payment by a third party • unrelated to the customer • Online order • Cross border payments
Geographic Location (threat and vulnerability)	• FATF listed countries on blacklist or grey list • Offshore tax havens/secrecy jurisdictions • High corruption countries • Countries with high terrorism

These risk categories can be weighted, or each of them can be given equal weighting, depending on the businesses' nature. Your risk assessment could include qualitative risk categories other than the four mentioned above, such as the institutions you deal with, e.g. lawyers, other DPMSs, banks, service providers, etc. While not explicitly stated in the law, the enterprise risk assessment should identify the risk categories in the context of the nature of your business activities.

5.2.5. Assessing the Risk

The following risk matrix will help in assessing the likelihood and consequences of the ML/TF event:

Money laundering and terrorism financing risk matrix				
Likelihood	Almost certain (High probability of ML/TF)	Medium	High	High
	Likely (Medium probability of ML/TF)	Low	Medium	High
	Unlikely (Low probability of ML/TF	Low	Medium	High
	Possible (Trivial probability of ML/TF)	Low	Medium	Medium
		Minor	Moderate	Significant
	Magnitude of Consequence			
Risk Rating		Low	Medium	High

The senior management of the DPMS is to approve the risk assessment, which is why it should include the proposed mitigation measures that are needed, which contain AML/CFT controls and procedures which have been identified by the risk assessment.

The enterprise risk assessment should be updated on a regular basis, or when there is information or substantial changes in specified services that the DPMS's provide. According to international practices, the risk assessment should be reviewed and upgraded at least once every two years.

5.2.6. Sources of Information for Enterprise Risk Assessment

The sources which may provide information for an enterprise risk assessment are:

(a) Internal Information: The DPMS's own information about the business – how many business lines, locations, main services, how many providing sales services, customers groups, technologies used, etc.

Information from within the DPMS may be collected via a questionnaire or a telephone meeting, or face to face meeting. Depending on how customer records are kept, it may take some time to extract the information needed. The DPMS is unlikely to obtain all the required information but should be sufficient for informed conclusions to be made.

(b) Pakistan's National Risk Assessment: This report contains information on the ML/TF threat environment for Pakistan including high-risk activities and sectors. The DPMS's risk assessment should take account of the findings of the latest National Risk Assessment to inform the enterprise risk assessment of the ML and TF threat environment, and include high-risk activities and sectors. The National Risk Assessment is not publicly available, so the DPMS will have to request a copy from FBR or FMU.

(c) Government agencies: FMU ML/TF reports (e.g. Strategic Analysis of High-Risk Professions), FBR, SRBs, SBP, MoFA, and other Pakistan government agencies.

(d) International organizations and NGOs:

- FATF and FATF-style regional bodies;
- Supra-national or international bodies such as the United Nations Security Council, International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units;
- Non-governmental organizations such as Transparency International, Basel AML Index, and Tax Justice Network.

5.2.7. Risk Assessment Template

Risk rating categories		***Low***	***Medium***	***High***
Customer - Types *[Add as many columns as customer types]*			***Risk Rating***	***Miligation Measures***
Products/Sercives *[Add as many rows as required]*				
Geographic Location *[Add as many rows as required]*				
Channels of Delivery *[Add as many rows as required]*				
Overall Risk Rating				

6. COMPLIANCE PROGRAM, POLICIES & PROCEDURES

6.1. LEGAL REQUIREMENTS

The law requires reporting entities to implement compliance management arrangements, including the appointment of a compliance officer at a management level and training programs, having regard to the ML/TF risks and the size of the business during the course of their activities.[66] Reporting entities are also required to implement policies and procedures to ensure their compliance with the law that impose TFS obligations upon reporting entities.[67]

As part of their risk assessment and mitigation measures, DNFBPs are required to do the following:

(a) Have policies, controls, and procedures, which are approved by senior management, to enable them to manage and mitigate risks that have been identified in its own risk assessment and any other risk assessment publicly available or provided by FBR;[68]
(b) Monitor the implementation of those controls and enhance them if necessary;[69] and
(c) Take enhanced measures to manage and mitigate the risks where higher risks are identified.[70]

In order to implement compliance programs, DNFBPs must implement the following internal policies, procedures and control:

(a) Compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the regulated person compliance with the law.[71] Such regulated person is to ensure that the compliance officer:

    i. Reports directly to the board of directors or chief executive officer or committee;
    ii. 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;

66. Section 7G AMLA.
67. Section 7H AMLA.
68. Regulation 4(2)(a) DNFBP Regulations.
69. Regulation 4(2)(b) DNFBP Regulations.
70. Regulation 4(2)(c) DNFBP Regulations.
71. Regulation 7(1)(a) DNFBP Regulations.

iii. Be responsible for the areas including, but not limited to:
- 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;
- Monitoring, reviewing and updating AML/CFT policies and procedures, of the regulated person;
- Providing assistance in compliance to other departments and branches of the regulated person;
- Timely submission of accurate data/ returns as required under the applicable laws;
- Monitoring and timely reporting of suspicious and currency transactions to FMU; and
- Such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations.

(b) Screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;[73]

(c) An ongoing employee training program;[74] and

(d) An independent audit function to test the system.[75] This includes an assessment of the adequacy and effectiveness of the policies, controls and procedures adopted by the regulated person to comply with the requirements of these regulations; and to make recommendations in relation to those policies, controls and procedures.[76]

In the case of a corporate group, in addition to the aforementioned obligations, 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; and
(c) Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

72. Regulation 7(3)(c) DNFBP Regulations.
73. Regulation 7(1)(b) DNFBP Regulations.
74. Regulation 7(1)(c) DNFBP Regulations.
75. Regulation 7(1)(d) DNFBP Regulations.
76. Regulation 7(2) DNFBP Regulations.

The DNFBP shall ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with Pakistan requirements where the minimum AML/CFT requirements are less strict than Pakistan, to the extent that host country laws. If the foreign country does not permit the proper implementation of AML/CFT measures consistent with that of Pakistan requirements, financial groups should to apply appropriate additional measures to manage the risks, and inform the SECP.

6.2. OPERATING PROCEDURES

6.2.1. Written Policies and Procedures

AML/CFT procedures should deal with the following:

a) Enterprise and Technology Risk Assessment;
b) Compliance Officer;
c) Staff Vetting and Training;
d) CDD;
e) Targeted Financial Sanctions;
f) Filing of STRs and CTRs with FMU;
g) Record Keeping; and
h) Independent Audit.

The adopted procedures should be:

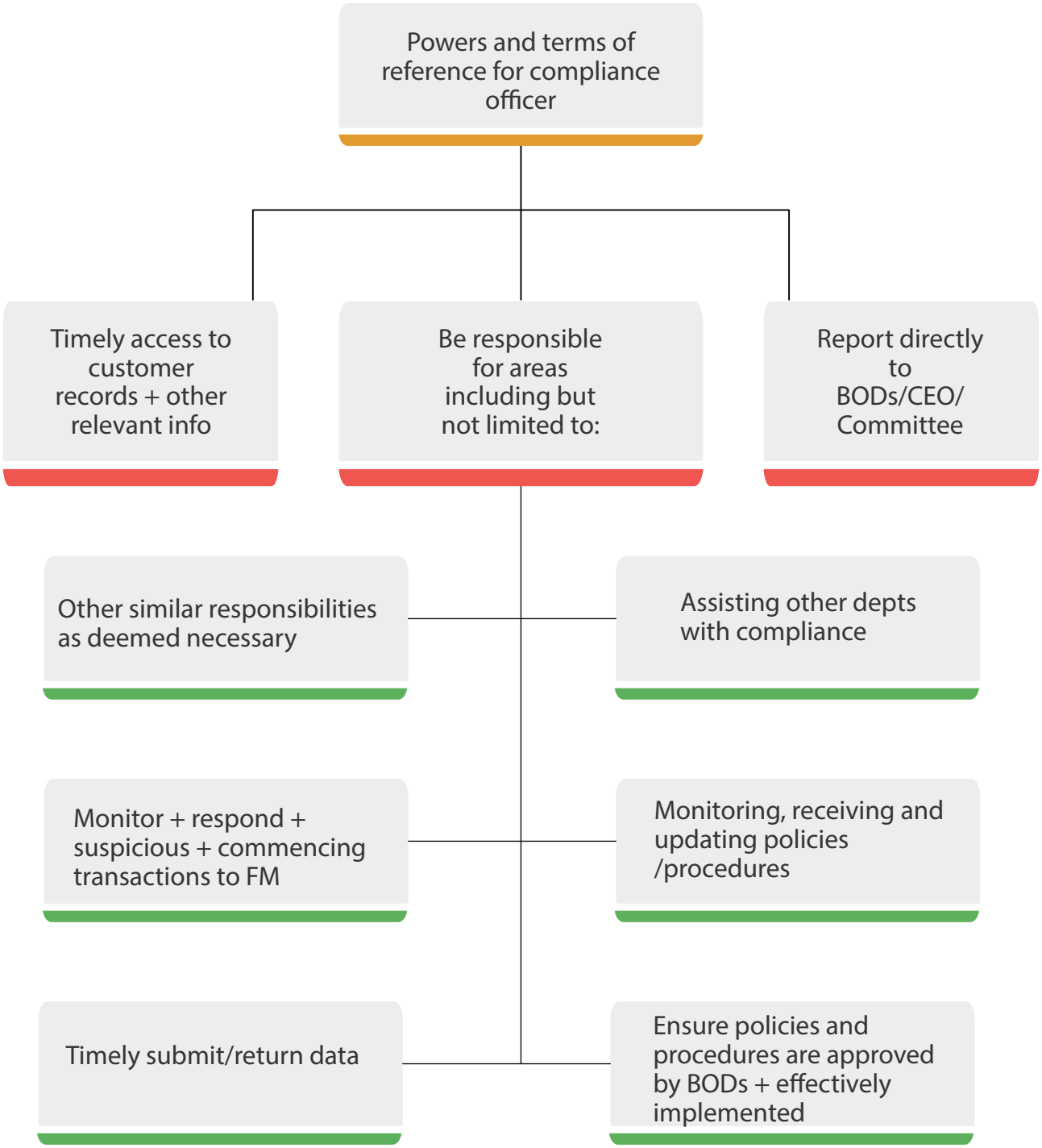
a) Clearly dated to allow for easier identification by staff of any subsequent changes;
b) Made available via the REA's intranet or email distribution; and
c) Any changes to the procedures should be communicated to all staff, and reflected in the AML/CFT training.

6.2.2. Role of Senior Management and Compliance Officer

The senior management must:

(a) Engage in decision-making on policies and procedures;
(b) Oversee risk-based compliance programs;
(c) Encourage compliance; and
(d) Ensure adherence to said procedures by employees.

The designated compliance officer is responsible for the following:



6.2.3. Group Compliance

If the REA has branches/subsidiaries, in Pakistan or abroad:

a) Group compliance should ensure the implementation of policies and procedures;
b) A head compliance officer should oversee other compliance officers; and
c) As a group, they must monitor and review, conduct an internal audit, introduce safeguards for confidentiality, and have procedures compliant with CDD and ML/TF management.

6.2.4. Staff Vetting and Training

6.2.4.1. Vetting and Employment

To ensure a high standard of employees, vetting should be:

a) Different for senior managers, compliance officers, and customer-facing roles;
b) Applied when job applicants are changing fields/roles;
c) Applied to temporary/interim employees or contractors;
d) Triggered by events (e.g. behavioral report or adverse media).

Background assessments may include:

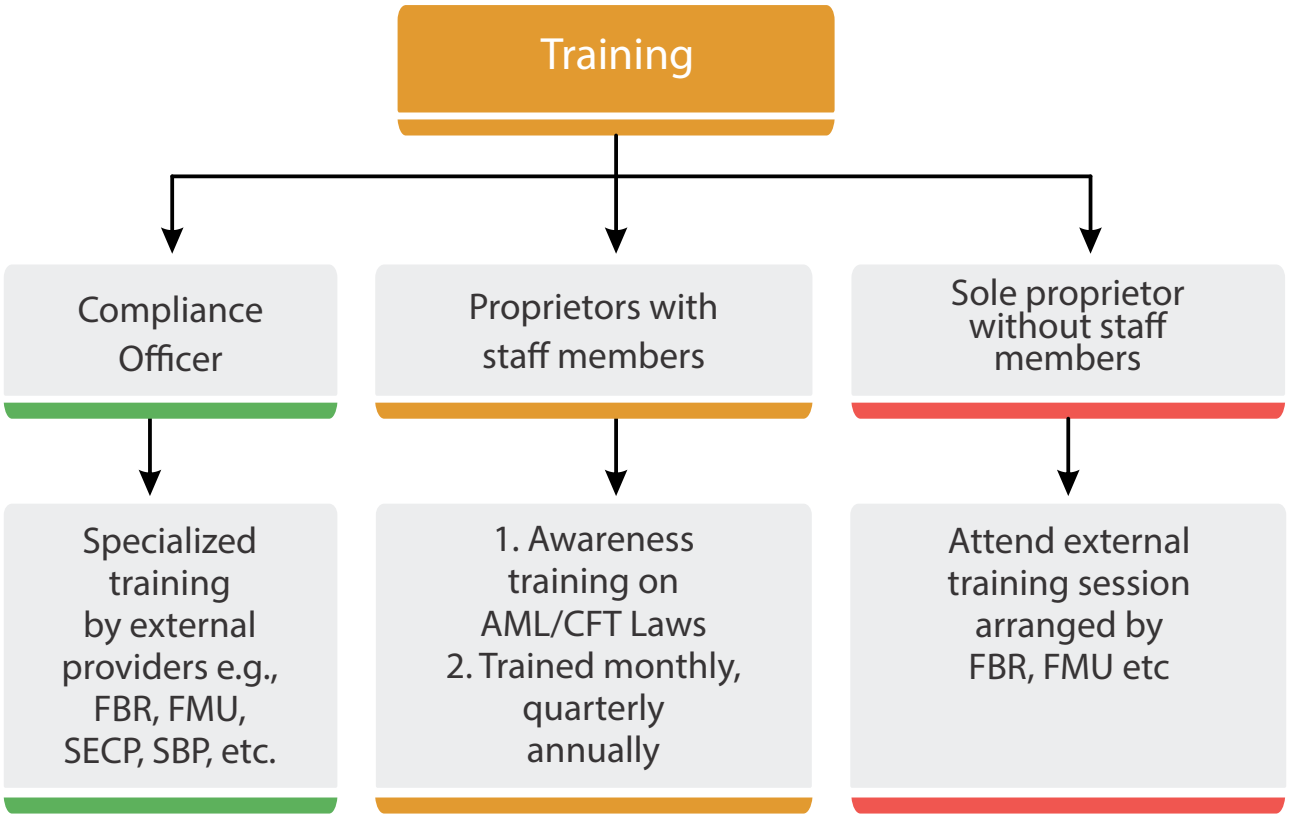
a) Written references from previous employers;
b) Character statements from people of good standing in the community (e.g. religious figure, medical practitioner, police officer);
c) Internet search;
d) For new graduates, a reference letter from a university lecturer, university society or from a person of good standing in the community may be sufficient.

All employees must comply with AML/CFT laws and REA procedures. In the event of frequent procedural violations, sales commissions should be deducted, or employment should be terminated.

6.2.4.2. Training

To maintain adequacy and efficacy of the system, staff members should be:

a) Educated on AML/CFT laws;
b) Trained regularly (e.g. monthly, quarterly, etc.) to deal with circumstances related to ML/TF.



The law is silent on the frequency of training. Ideally, it should be conducted upon commencement for new staff and a refresher training, ideally annually, or at least biennially. Training or awareness-raising will also need to be undertaken if there are new regulatory requirements or changes to key internal AML/CFT procedures and processes.

Records should be kept showing who has received training, the training received, and when the training took place. These records should be used so as to inform when additional training is needed, e.g. when the ML/TF risk of a specific business area changes, or when the role of a relevant employee changes.

6.2.5. Monitoring and Review

Even though the law does not explicitly provide for it, REAs are required to carry out checks through their compliance officer to understand:

a) If the AML/CFT procedures are being implemented; and
b) If there has been any breach.

Reviews should be regular, preferably on a monthly or quarterly basis, which will help point out gaps for rectification like amending procedures, staff counseling or punishment, and additional training.

Identifying gaps at an earlier stage helps to reduce the:

a) Problem;
b) Rectification work; and
c) Cost to rectify the problem.

6.2.6. Independent Audit Function

The law requires regular independent audits. Ideally, the audit should ideally be conducted annually at the very least and include:

a) An assessment of the adequacy and effectiveness of the policies, controls, and procedures adopted. The assessment should include a review of the DNFBPs AML/CFT procedures, such as:

    i. Risk Assessment and Risk Mitigation;
    ii. AML/CFT Programme;
    iii. Risk-Based Customer Due Diligence (CDD);
    iv. Targeted Financial Sanctions;
    v. Suspicious Transaction Report (STR);
    vi. Currency Transaction Report (CTR);
    vii. Record Keeping; and

b) Making recommendations in relation to those policies, controls, and procedures.

For a REA that is a single individual, undertaking an independent review may be challenging given the cost involved in engaging an external expert. You may want to consult the FBR in the first instance on what is acceptable. You could ask your accountant to undertake the review, if you are using the services of an accountant which may be more affordable than an AML/CFT expert.

7. ANNEXURES

7.1. ANNEXURE A – LIST OF ADDITIONAL RESOURCES

No.	Document	Link
1	AML/CFT Sanctions Rules, 2020 (SRO 950(I)/2020)	https://download1.fbr.gov.pk/Docs/20201015151053306 7AML-CFT-Sanction-Rules-2020-SRO-NO-950I-2020.pdf
2	Anti-Money Laundering Act, 2010 (Act No. VII of 2010)	https://www.fmu.gov.pk/docs/Anti-Money-Laundering-Act-2010-amended-upto-Sep.%202020.pdf
3	Anti-Terrorism Act, 1997	https://nacta.gov.pk/wp-content/uploads/2017/08/Anti-Terrorism-Act-1997.pdf
4	DNFBPs FBR Order No. 1 of 2021	https://download1.fbr.gov.pk/Docs/20211130101158217 79ConditionCircular01of2021-housing.pdf
5	DNFBPs (Real Estate Sector) FMU-Circular No. 07 of 2020	https://www.fmu.gov.pk/docs/Circular-for-Real-Estate-Sector-Red-Flags.pdf
6	FBR AML/CFT Guidelines for Real Estate Agents (REAs)	https://download1.fbr.gov.pk/Docs/2021821683014134AML-CFTRealEstateAgentsUpdatedJuly2021.pdf
7	FBR AML/CFT Regulations for DNFBPs, 2020 (SRO 924 (1)/2020)	https://download1.fbr.gov.pk/SROs/2020929179 76805SRO9242020.pdf
8	Guidelines for DNFBPs on Targeted Financial Sanctions (TFS) Under Nations Security Council Resolutions	https://download1.fbr.gov.pk/Docs/2021382031741 608pg1.pdf https://www.fbr.gov.pk/Targeted-financial-sanctions-regulations/152366/152886
9	Guidelines for the Reporting Entities on filing of Currency Transaction Reports	https://www.fmu.gov.pk/docs/2021/Guidelines-filing-Currency-Transaction-Reports.pdf
10	Guidelines for the Reporting Entities on filing of Suspicious Transaction Reports	https://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-filing-of-Suspicious-Transaction-Reports-for-the-Reporting-Entities.pdf

No.	Document	Link
11	Ministry of Interior/National Counter Terrorism Authority (NACTA) Proscribed Organizations under Schedule-1 and Proscribed individuals under Schedule 4 of the Anti-Terrorism Act, 1997	https://nacta.gov.pk/wp-content/uploads/2018/12/Proscribed-Organizations Eng-3.pdf https://nacta.gov.pk/proscribed-persons/
12	Red Flags Indicators for Real Estate Sector	https://www.fmu.gov.pk/docs/Red-Flag-Indicators-for-Real-Estate-Sector.pdf
13	Short Guidance on AML/CFT Obligations for Real Estate Agents (REAs) (English)	https://download1.fbr.gov.pk/Docs/20219150913325 70ShortGuidanceForREAs.pdf
14	Short Guidance on AML/CFT Obligations for Real Estate Agents (REAs) (Urdu)	https://download1.fbr.gov.pk/Docs/20219150927216 83ShortGuidanceforREAs-Urdu.pdf
15	United Nations Security Council (Freezing and Seizure) Order, 2019, and other SROs issued by the Ministry of Foreign Affairs	http://mofa.gov.pk/wp-content/uploads/2020/01/UNSC-Freezing-Seizure-Order-2019.pdf