ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

HANDBOOK FOR ACCOUNTANTS

DISCLAIMER

This Handbook is designed to assist accountants 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, an accountant should utilize the Handbook in light of his or her professional judgment and the facts and circumstances involved, and each particular client relationship. Each accountant 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 ACCOUNTANTS

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
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FBR	Federal Board of Revenue
FMU	Financial Monitoring Unit
ICAP	Institute of Chartered Accountants of Pakistan
ICAP Regulations	Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms
ICMAP	Institute of Cost and Management Accountants of Pakistan
ICMAP Regulations	Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms
IMF	International Monetary Fund
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
UNSC	United Nations Security Council

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 various financial transactions handled by accountants. 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 accountants, 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. Accountants (self-regulated and otherwise) must recognize the role that they must play in protecting themselves from involvement in ML/TF and in protecting Pakistan's reputation of integrity.

Accountants are likely to encounter ML activities in the course of their business activities. They act as gatekeepers to the financial system as they manage client money and assets, create, operate, and manage companies, and provide financial advice, due to which, in conducting their activities, they may interact with money launderers and those who wish to finance terrorism. Thus, accountants must be aware of relevant AML/CFT obligations to ensure that their activities are not exploited by criminals.

Accountants would not want to be a party to such activities. If accountants are not vigilant, the financial 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. Accountants 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 accountants in complying with the requirements of the AML/CFT laws, rules, and regulations to prevent Pakistan's accounting system and operations from being abused for ML/TF. The particular objectives of the Handbook are to:

- Outline the requirements of AMLA, DNFBP Regulations, ICAP Regulations, and ICMAP Regulations to be followed by accountants;
- Assist accountants in complying with the requirements of such laws and regulations;
- Emphasize the responsibilities of compliance officers and key personnel belonging to the accounting 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 accountants may face and is not the only source of guidance on ML/TF. Accountants are reminded that guidance produced by FATF, FMU, FBR, and ICAP/ICMAP 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 an accountant. For the purposes of this Handbook, you are an accountant if you are sole practitioner, partner, or employed professionals within professional firms (whether regulated by ICAP/ICMAP or not),[3] and carry out the following activities:

Accountancy services: when they carry out monetary transactions for their customers concerning the following activities:

- Managing, operating, buying and selling of real estate, legal persons and legal arrangements and preparing documents therefore;
- Managing of client money, securities or other assets;
- Managing bank, savings or securities accounts; or
- Organizing contributions for the creation, operation or management of companies.[4]

2. See Annexure A for a non-exhaustive list of resources.
3. Regulation 2(1)(a) DNFBP Regulations, Section 6A(1) read with Schedule IV AMLA.
4. Section 2(xii)(c) AMLA.

Trust and company formation services: when they carry out monetary transactions or services for a client concerning the following activities:

- Acting as a formation agent of legal persons;
- Acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as or arranging for another person to act as a trustee of a trust or performing the equivalent function for another form of legal arrangement; or
- Acting as or arranging for another person to act as a nominee shareholder for another person.[5]

However, note that "accountants" does not refer to internal professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.[6]

Activities such as audit of financial statements carried out according to the International Standards on Auditing (ISAs) as applicable in Pakistan, tax consultancy services, and book keeping services are not subject to the AML/CFT laws.

Below are some examples of the activities that could render you subject to the AML/CFT laws. However it is important to note that giving advice to a customer, in the context of accountant-customer relationship, is not considered providing instructions, and therefore is not considered to be a specified service.

(a) Acting as a formation agent for legal persons or legal arrangements

This service refers to forming a legal person (such as a company) or legal arrangement on behalf of a customer (for example, registering a company with the SECP). The service does not include instances where the reporting entity provides advice, including referring the customer to a third party, e.g. a lawyer, for more detailed

5. Section 2(xii)(d) AMLA.
6. Explanation to Regulation 2(1)(a) DNFBP Regulations.

advice. In the case of formation of a company, if a customer asks an accountant to register the company or registers the company based on the advice given by the practicing firm, the specified service would be undertaken by the accountant (or the customer, as the case may be) and the accountant would have to apply their AML/CFT compliance programme to that service.

The filing of statutory forms/annual returns is a regulatory requirement under the Companies Act 2017, therefore, it is not a specified service subject to AML / CFT laws.

Examples of this kind of captured service in practice include:

- Incorporation/registration of a company with the SECP on behalf of a customer; and
- Incorporation of an entity (partnership/firm/society/company, etc.) on behalf of a customer.

ML/TF risks associated with this activity:

When a reporting entity is engaged to register a company or partnership, the actual ownership of the company or partnership being formed may be concealed or obscured, for example, where shell companies, multiple layers of ownership, or other complex legal structures are used. Setting up a trust can also be a way to create a perception of distance between assets and their beneficial owners. Charitable organizations (such as incorporated societies and charitable trusts) are also used to finance terrorism.

(b) Acting as a nominee director, shareholder or trustee

Where the reporting entity is engaged to act as a nominee director or shareholder for a company, or as a trustee of a trust, this is a specified service subject to AML/CFT laws. However, where the firm has only assisted the company/partnership in the appointment of a director/partner by sharing the database of the individuals and the firm has no authority with regards to the selection process of the candidate, that service is not a specified service subject to AML/CFT laws.

Examples of this kind of captured service in practice include:

- The reporting entity or staff member acts as a nominee shareholder or director for a customer, i.e., the name or employee of the reporting entity is registered as the legal owner, but there may be a separate agreement with the customer governing its ultimate ownership;
- The reporting entity or staff member acts as a trustee of a trust;

- The reporting entity or staff member arranges for a person to act as a nominee shareholder for a company.

ML/TF risks associated with this activity:

If an accountant is acting as a nominee director, nominee shareholder for a company, or a trustee for a legal arrangement (such as a trust or charity), others may gain a false impression of legitimacy for the activities undertaken by the company or legal arrangements. This lack of visibility provides criminals with the opportunity to use their companies or other legal arrangements for ML or other financial crime without being detected. The possibility of detection is made less likely because they can do this while maintaining the impression of oversight by reputable Pakistan-based directors.

(c) Managing customer funds, accounts, securities, or other assets

If the reporting entity is engaged in managing payments to, or from its customers' accounts as a specified service; and, with the exception of payments for professional fees, any instance where the reporting entity receives or holds customer funds and controls the payment of those funds will be a specified service subject to AML/CFT laws. The key determining factor is whether the reporting entity has control over the flow of funds (if it has the control then the activity is specified service).

For example in a payroll situation, if the reporting entity is preparing the vouchers or uploading the payments in the system that are then actioned by the customer, in such a case the reporting entity is not controlling the funds, rather the customer is. However, if the reporting entity is authorizing salary payments from the customer's account directly into customer staff's personal accounts, then this is a specified service.

Examples of this kind of activity in practice include:

- The reporting entity has the authority to make payments on behalf of its customer's business directly from customer's bank accounts;
- The reporting entity makes investments on behalf of a customer in securities and/or other assets using funds from the customer's bank accounts which practicing firm has the authority to transfer;
- The reporting entity manages the sale and/or purchase of trust assets for the customer using funds from the customer's bank accounts which the reporting entity has the authority to transfer;
- The reporting entity disburses the funds generated from a company's winding up/liquidation to a creditor in line with the relevant administration requirements.

ML/TF risks associated with this activity:

Some people will try to avoid accessing banking services typically used in transactions to obscure the trail of funds, changing hands as a means to hide their criminal activities. One way to obscure this trail or to add an appearance of legitimacy is to use the professional services of accountants to interact with financial institutions.

(d) Providing a registered office, business address or accommodation

A reporting entity provides a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal persons or arrangement, is a specified service.

Examples of this kind of activity in practice include:

- A company wants to use the address of the reporting entity because it has no physical office, and the business operates from a residential address;
- A foreign company has opened a branch in Pakistan and registered with SECP, but business is not sufficient to have a physical presence. Representatives of the foreign company flies in and out to attend to business matters;
- The business has no physical presence in your city, but has an office in another city, and wants a local address for convenience.

ML/TF risks associated with this activity:

For a person who is intent on ML/TF or committing other crime, the use of an address that is not their physical location is appealing. It allows them to keep anonymity and distance from the transactions and activities they are undertaking, and if it is the address of a reporting entity, it adds a perception of legitimacy to their activities. It also makes it more difficult for law enforcement to track them down in person. It is also why it is important to obtain the physical address of the customer when providing specified services.

Support and guidance on AML/CFT

- If you are unsure as to whether they are a reporting entity, they should contact their SRB, FBR, ICAP/ICMAP or FMU and/or seek independent professional advice;
- Where employees of the reporting entity have compliance questions, their first reference point should be the reporting entity's AML/CFT policies and procedures. The AML/CFT procedures should be able to provide answers to basic questions that are likely to arise in the specific business context;

- Specific questions should be answered by the firm's designated compliance officer or senior management;
- Reporting entities can access support from a range of sources including your professional accountancy body/SRB (ICAP/ICMAP), FBR, FMU, MoFA, MoI, independent professional advice from legal counsel, AML/CFT consultants, and open source information from relevant international bodies concerned with AML/CFT.

1.3. SANCTIONS FOR NON-COMPLIANCE

The legal requirements described in this Handbook are requirements prescribed by the AMLA,[7] DNFBP Regulations[8] and ICAP and ICMAP Regulations[9] and the Sanctions Rules.[10]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

7. Sections 6A(2)(h) and 7I AMLA.
8. Regulation 16 DNFBP Regulations.
9. Regulation 32 ICAP and ICMAP Regulations.
10. Section 3 Sanctions Rules.

imprisonment for a term which may extend to five years, a fine which may extend to five hundred thousand rupees, or both.[11]

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.[12]

Sanctions may be imposed on a "person" which means a reporting entity, directors, senior management, or officers in similar positions of that reporting entity.[13] "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.[14]

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.

11. Section 33 AMLA.
12. Section 34 AMLA.
13. Rule 2(1)(d) Sanctions Rules.
14. 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.[15]

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.[16]

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.[17]

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.[18]

15. Section 7(1) AMLA, Regulation 14 DNFBP Regulations, Regulations 26 ICAP Regulations and ICMAP Regulations.
16. Section 7(3) and 2(xi) AMLA, SRO No.73 (I)/2015 dated 21.01.2015, Regulation 14 DNFBP Regulations, Regulations 26 ICAP Regulations and ICMAP Regulations.
17. Section 7(2) AMLA.
18. 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.[19] 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.[20]

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.[21]

If during the process of screening or monitoring of customers a positive or potential match is found then the reporting entity 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.[22]

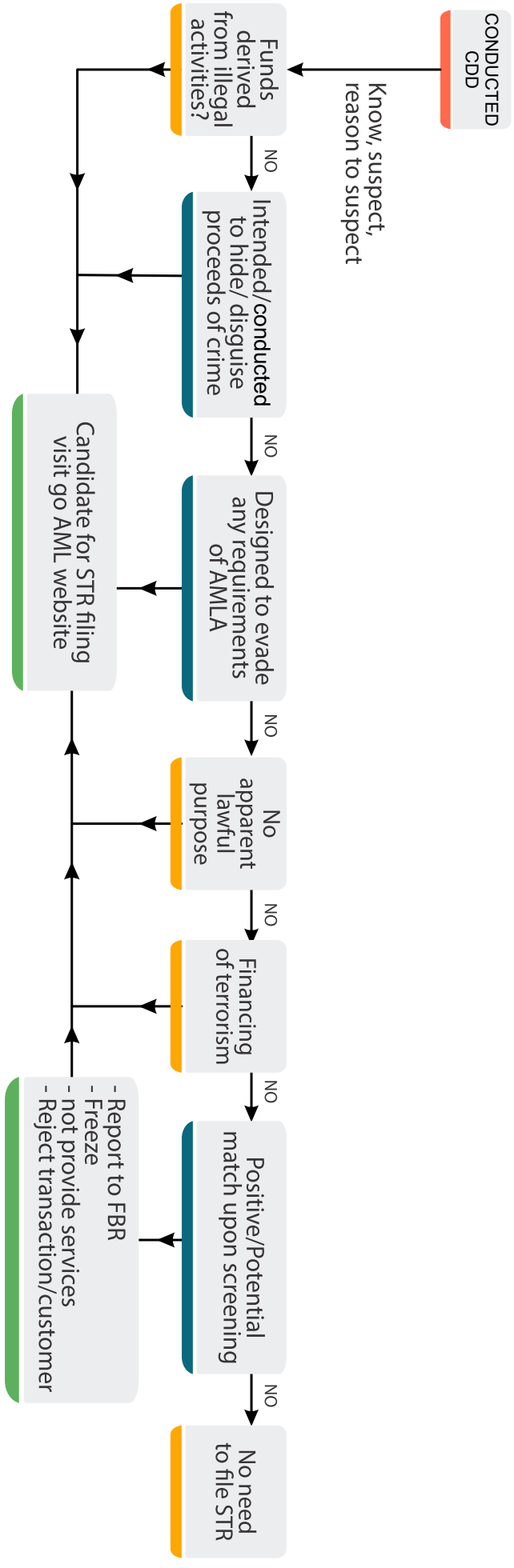
In all the cases mentioned above, the accountant shall report to the FBR and FMU by filing an STR and/or CTR.[23]

2.2. OPERATING PROCEDURES FOR SUSPICIOUS TRANSACTION REPORTS

2.2.1. Should you file a Suspicious Transaction Report?

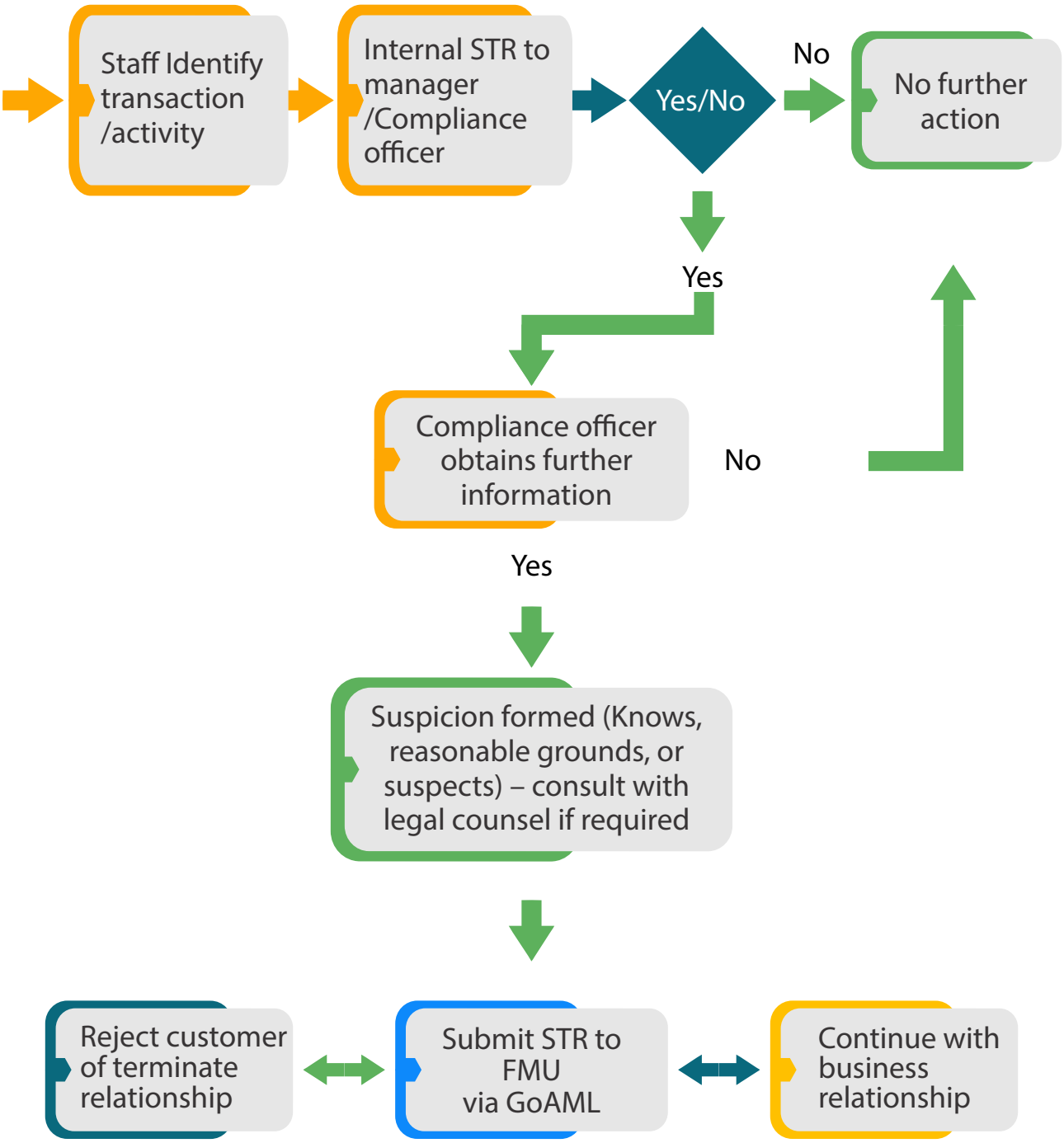
The following diagram is a decision-making framework for whether you should file an STR.

19. Section 7(5) AMLA.
20. Section 7(6) AMLA.
21. Section 7H AMLA.
22. Regulation 13(1)(b) DNFBP Regulations.
23. 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 REAs 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 counterparties, 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 s '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);
    - Statement of accounts (if applicable);
    - Copies of transaction vouchers;
    - Copy of SWIFT messages;
    - Account details annexure (if applicable);[24]
    - 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.

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

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?

All cash-based transactions above PKR 2 million or equivalent in terms of foreign currency are required to be reported to FMU. Aggregation of cash transactions during the day for the purpose of reporting a CTR is not required. However, if there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade the reporting of CTR, the same may be reported in the form of an STR.

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[25] and DNFBPs[26] 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:

25. Defined in Section 2(xiv) AMLA.
26. 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 two 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,[27] as well as continuously monitor the business relationship. A third party can be relied upon by the reporting party to carry out CDD.[28]

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.[29]

A reporting entity entering into a relationship with a customer who gives a fictitious name or is anonymous is prohibited.[30]

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;[31]
(b) Delayed verification, subject to certain conditions;[32]
(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.[33]

27. Section 7A AMLA, Regulation 24 ICAP and ICMAP Regulations.
28. Section 7B AMLA.
29. Section 7D AMLA.
30. Section 7E AMLA.
31. Regulation 8(1) to 8(12) DNFBP Regulations.
32. Regulation 8(13) and 8(14) DNFBP Regulations.
33. Regulation 8(15) and 8(16) DNFBP Regulations.

Furthermore, REAs are to apply enhanced due diligence where the risk is greater, which is called upon by the FATF for certain countries and PEPs, including their family members and close associates.[34] If the risks are lower, the REA can apply due diligence which is simple, but not where ML/TF is suspected.[35] Countermeasures must be used by the REA in countries where the risk is high,[36] while third parties can be relied upon under certain conditions.[37]

3.2. Operating Procedures

3.2.1. Whom is Customer Due Diligence conducted upon?

CDD is conducted upon:

(a) Your customer

Any person engaging a reporting entity for the purposes of requesting, acquiring, or using accountant or any services or carrying out any transaction or business with the reporting entity but only for specified services as explained earlier.[38]

(b) Any beneficial owner of your customer

- A natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or
- A natural person who exercises ultimate effective control over a legal person or legal arrangement.[39]

(c) Any person acting on behalf of your customer

There are instances where a person is acting on behalf of a customer but is not necessarily a beneficial owner of that customer. For example:

- A person exercising a power of attorney for your customer;
- A legal guardian acting on behalf of a minor who is your customer;
- An employee who has the authority to act on behalf of a company that is your customer.

34. Regulation 9(1) to 9(3) DNFBP Regulations.
35. Regulation 10 DNFBP Regulations.
36. Regulation 11 DNFBP Regulations.
37. Regulation 12 DNFBP Regulations.
38. Regulation 2(f) DNFBP Regulation, Regulation 3(c) ICAP and ICMAP Regulations.
39. Section 2(iv) AMLA.

3.2.2. When should Customer Due Diligence be conducted?

(a) New customer

Before commencing a business relationship[40]

- The CDD process should commence after both parties have started discussion about potential services, but should be completed before the reporting entity has agreed to provide such services, i.e., accepted the customer or new engagement;
- Identification of a new customer must be completed before accepting the new customer;
- Delayed verification is accepted in certain, very limited circumstances.

(b) Existing customer

Once a significant change in the nature of business relationship or the ownership and control structure of the customer's business is noticed

- These will not be common, but in servicing an existing customer, the reporting entity may acquire knowledge that there is a new director requiring CDD, or a new beneficial owner, or a new company representative requiring CDD;
- The above could be identified when an existing customer seeks the services of the reporting entity for a new engagement (including migrating from a non–specified service, auditing to a specified service, managing bank account), or monitoring the transactions of an existing customer;
- For other existing customers where there are no changes, there is no fixed deadline for updating CDD. Updating is based on your reporting entity's assessment of the risk of existing customers. This review could be done annually or biennially, depending on your reporting entity's resources and risk profile of your existing customers.

Suspicion of money laundering or terrorist financing

- Since, there are no occasional customers or transactions, this applies to existing customers;
- These include existing customers before the AML/CFT requirements took effect;

40. As per Section 2(v) AMLA, "business relationship" means a professional or commercial relationship between a reporting entity and a customer to conduct transaction, activity or to provide service or product.

- This could be triggered from scrutinizing transactions showing unusual transactions, or the income or transactions are no longer consistent with the reporting entity's understanding of the customer's business.

Doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification

- It may be more applicable to existing customers, i.e., persons that were already customers prior to the AMLA or AML/CFT laws came into effect so they were not subjected to the same level of due diligence;
- It may also be applicable to the individual that you have been dealing with for a company establishes a new company, and the customer is the new company (not the old company), even though it is the same individual;
- The trigger could be when they return for another engagement and the reporting entity needs to collect and verify information on beneficial ownership which were not previously obtained.

3.2.3. Components of Customer Due Diligence

The following are key components of the CDD process:

(i) Identify legal identity and address

- The reporting entity must identify the legal identity of the customer which can be an individual, legal persons (companies or non-profit organizations) or legal arrangements (e.g. trusts).
- The reporting entity must also obtain the:
    - Date of birth and address of the natural person;
    - Date of incorporation of the legal person;
    - Date of trust formation.
- The address for all three categories should be a physical address.

(ii) Verify legal identity and address

The reporting entity must verify the customer identity, including name and date of birth/formation and address using reliable and independent source documents, data or information.[41]

41. Refer to the information on acceptable verification documents below in Section 3.2.3.1. of the Handbook.

(iii) Identify and verify beneficial ownership

- For a customer who is an individual, unless there are indication to the contrary, the person is considered to be both the legal and beneficial owner;
- For a non-complex company structure, the natural person director(s) may also, prima facie, be the beneficial owner(s). Therefore, in these instances your customer's legal identity or the first layer of ownership is the same as the beneficial owner(s), but not in all cases;
- The challenges are with complex ownership of companies or beneficial owners in a discretionary trust. Multiple layers of legal ownership or control will need to be identified before finding the beneficial owner (i.e., individual), and then reasonable measures be taken to verify such beneficial owner.[42]

(iv) Identify and verify any person acting on behalf of the customer

- The reporting entity must identify and verify the identity of the authorised, individual representative. There is no requirement to identify and verify the beneficial owner in this situation. Examples of the person acting on behalf of a customer include:
    - An employee who has the authority to act on behalf of a company that is the customer;
    - A trustee;
    - A person exercising a power of attorney for the customer;
    - A legal guardian acting on behalf of a minor who is a customer.
- The requirements are the same as for an individual customer, except the individual is authorised to act on behalf of the customer. If another legal person is the authorised representative of the customer, then an individual(s) of that company must be identified and verified. In other words, the reporting entity must always identify and verify an individual or individuals.
- The reporting entity also needs to obtain evidence such as documentary evidence that the customer has appointed the individual(s) to act on its behalf and the specimen signature of the person appointed.

(v) Information on the purpose and the intended nature of the relationship

- The reporting entity must obtain information on the purpose and intended nature of the business relationship;
- In most instances, this will be self-evident when the customer approaches the reporting entity to seek accountancy services, and whether one-off or ongoing. There are additional requirements in that the information must be

42. Refer to the explanation below in Section 3.2.3.2. of the Handbook.

documented, and if the customer is rated high-risk, as more information will need to be collected;
- Unlike for identity, there is no requirement to verify the information.

(vi) Establish or obtain information on the source of wealth or funds

- The reporting entity must obtain information on the source of wealth or funds under EDD for higher risk customers. For PEPs, including their beneficial owners, family members and close associates, the reporting entity must take reasonable measures to establish the source of wealth and funds;[43]
- For accountants, many of the professional services provided by accountants put them in a relatively good position to acquire this knowledge.

(vii) Ongoing CDD

The reporting entity must conduct ongoing due diligence on any continuing business relationship and scrutiny of transactions (if any) undertaken throughout the course of that relationship to ensure that the services provided under the business relationship are consistent with the firm's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.[44]

3.2.3.1. Verification of Customer Documents, Data or Information

Below is a list of acceptable reliable and independent documents, data or sources for verification of customers, beneficial owners and persons acting on behalf of the customer.[45]

43. Refer to the explanation below in Section 3.2.4. of the Handbook.
44. Refer to the explanation above in Section 3.2.2. of the Handbook.
45. Regulation 8(11) DNFBP Regulations and Regulation 15 ICAP and ICMAP Regulations.

Table on acceptable verification documents, data or information	
Customer Category	**Identity documents/data/information**
1) Individuals (as customers, authorised representatives and beneficial owners)	(I) Computerized National Identity Card (CNIC) issued by NADRA; or (ii) 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 (iii) Pakistan Origin Card (POC) issued by NADRA and / or Passport for Pakistanis who have given up Pakistan nationality; or (iv) Form B or Juvenile card issued by NADRA to children under the age of 18 years; or (v) 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.
2) Sole Proprietors	(i) Identity document as per Individuals above of the proprietor. (ii) Registration certificate for registered concerns. (iii) Sales tax registration or NTN, wherever applicable. (iv) Certificate or proof of membership of trade bodies etc., wherever applicable. (v) Declaration of sole proprietorship on business letter head.
3) Partnership	Identity document as per Individuals above of the partners. (i) Original or attested copy of 'Partnership Deed' duly signed by all partners of the firm. (ii) Original or attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Client Acceptance Form. (iii) Authority letter from all partners, in original, authorizing the person(s) to operate firm's business relationship.

4) Legal person e.g. Limited companies /corporations	(i) Resolution of board of directors for establishing of business relationship with the reporting firm; (ii) memorandum of association (iii) articles of association, wherever applicable; (iv) certificate of incorporation; (v) Securities and Exchange Commission of Pakistan (SECP) registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017), as applicable; and (vi) list of directors required to be filed under the Companies Act, 2017 (XIX of 2017), as applicable; (vii) identity documents (as per Section 1 of this Table for individuals) of all the directors, beneficial owners and persons authorized to operate the business relationship. (viii) any other documents as deemed necessary including its annual accounts and financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer; (ix) Register of Ultimate Beneficial Ownership Information by the Companies, SECP Circulars No.16 and No.20 of 2018, Section 123A of Companies Act

5) Legal arrangements	(i) the instrument creating the legal arrangement (ii) registration documents and certificates; (iii) the legal arrangement's by-laws, rules and regulations; (iv) documentation authorizing any persons to open and operate the business relationship; (v) identity document as per as per Section 1 of this Table for individuals) above of the authorized persons, beneficial owners and of the members of governing body, board of trustees or executive committee, if it is ultimate governing body, of the legal arrangement; and (vi) any other documents as deemed necessary including its annual accounts and financial statements or disclosures in any form which may help to ascertain the subject of the trust, the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer; (vii) Also, if not covered by the above, the identity document of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries.
6) NGOs/NPOs/ Charities	i) Registration documents / certificate (ii) By - laws / Rules & Regulations (iii) Resolution of the Governing Body / Board of Trustees / Executive Committee, if it is ultimate governing body, for opening of business relationship (iv) Identity document of the authorized person(s) and of the members of Governing Body / Board of Trustees / Executive Committee, if it is ultimate governing body. (v) Any other documents as deemed necessary including its annual accounts / financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.
7) Government institutions and entities	(i) CNICs of the authorized persons; and (ii) letter of authorization from the concerned authority - for the individual authorised for action behalf of the institution

- **Additional guidance:**

  - **Original documents:**

    - For the purposes of verification, original documents need to be sighted, photocopied and attested by the reporting entity (i.e., the person verifying should mark "original sighted" on the copy);

  - **Certified true copy of document:**

    - Where the client is unable to produce original documents, the reporting entity may consider accepting documents that are certified to be true copies by an independent and qualified person (e.g., a notary public or an external law firm);
    - The original of the certified true copy must be provided and not just a photocopy of the certified true copy.

  - **Electronic verification:**

    - Alternatively, if feasible, electronic verification may be undertaken;
    - A number of subscription services give access to identity-related information. Many of them can be accessed online and are often used to replace or supplement paper-based verification checks. NADRA is a good source of verification of individuals and SECP for companies and some NPOs.
    - If on boarding is not face to 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.

3.2.3.2. Identifying and Verifying Beneficial Ownership

Legal ownership is separate and distinct from beneficial ownership.[46] 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.[47]

46. Section 2(iv) AMLA.
47. Regulations 2(1)(o) DNFBP Regulations.

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, unless there are reasons to doubt, the reporting entity may assume the individual customer is also the beneficial owner. However, the reporting entity 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: Identifying the beneficial owner through controlling legal ownership

This is normally the first test used to identify the beneficial owner as provided under Section 13(a) of the SRB AML / CFT Regulations for Reporting Firms and Section 8(9)(a) of the FBR AML / CFT Regulations for DNFBPs.

This test is still 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.

1. 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 25% is the threshold, there can only be a maximum of 4 beneficial owners as provided in Section I 23A 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. It is also important to highlight that this approach includes the notion of indirect ownership through a chain of companies. It is also important to note that 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. These concepts will be explained in the examples following this table.

TEST 2: Identifying the beneficial owner through control by other means

This is normally the second test used to identify beneficial owner as provided under Section 13 (b) of the SRB AML / CFT Regulations for Reporting Firms and Section 8 (9) (b) of the AML / CFT Regulations for DNFBPs.

This test is used if there is doubt whether the person with the controlling ownership interest is the beneficial owner or where no natural persons 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 own the company in the top layer

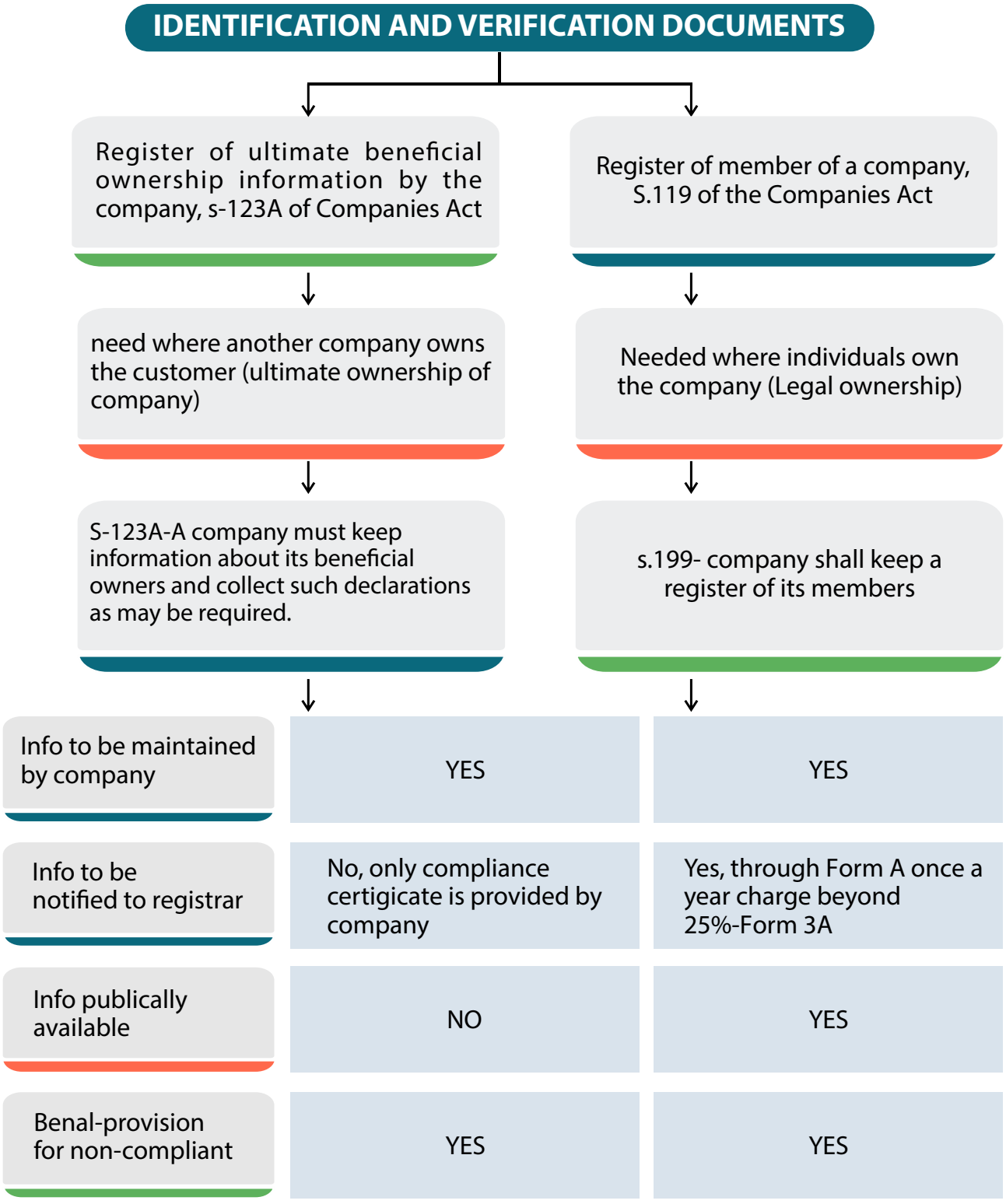
2. Majority interest approach: Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity.	- For example, to appoint or remove the majority of the board of directors, or its chair, or CEO of the company. While the above can be achieved through ownership, it could also be achieved without either direct or indirect ownership e.g. lender provides funds directly to company or individual shareholder. It is also important to highlight that this approach includes the notion of indirect control which may extend beyond legal (direct) ownership or could be through a chain of corporate vehicles and through nominees.
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 associations, 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: Identifying the beneficial owner through control by other senior managing officials

In the event the beneficial owner cannot be identified or verified as above Tests 1 and 2, Section 13 (b) of the SRB AML CFT Regulations for Reporting Firms and Section 8 (9) (c) of the FBR AML/CFT Regulations for DNFBPs provide for the use of the senior management approach as the alternative test of beneficial ownership.

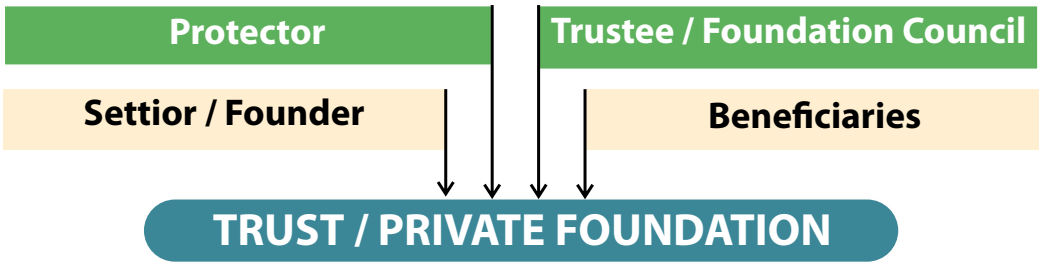
5. Senior management approach (alternative test): The natural Person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position	This is only permitted when the reporting firm cannot identify or ven the beneficial owner in limited circumstances, 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 (CEO), chief financial officer (CFO), managing or executive director, or president.

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.



Reporting entities are required to identify and take reasonable measures to verify the identity of beneficial owners as follows:[48]

(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.

Unlike for identifying the beneficial owners of legal persons, the identification of a trust's beneficial ownership is not based on the cascading tests. The reporting entity should identify all parties of the trust as they are all beneficial owners, prima facie, regardless of whether or not any of them exercises control over the trust. The following table shows how to identify beneficial ownership of a trust.

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	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 (trust) customer of the reporting firm.

48. Regulation 8(10) DNFBP Regulations and Regulation 14 ICAP and ICMAP Regulations.

2, Trustee (or equivalent) may be professional (e.g. a lawyer. accountant or trust company) if they are paid to act as a trustee in the course of their business, or non - professional (e.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 reporting firm. If the trustee is a corporate trustee, the individual authorised to represent the corporate trustee e.g. director needs to be identified and verified.
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 reporting firm. If the beneficiary is a corporate beneficiary, then all CDD requirements of a legal person would need to be undertaken. If the beneficial is another trust - then all the CDD requirements of a trust would need to be undertaken.

3.2.4. 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: [49]

(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.

49. Regulation 2(1)(m) DNFBP Regulations and Regulation 3(1)(i) ICAP and ICMAP Regulations.

EDD must be applied to:[50]

(a) All PEPs;

(b) Family members;[51]

(i) Spouse of the PEP;

(ii) Lineal descendants and ascendants and siblings of the PEP;

(c) Their close associates:[52]

(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.

3.2.4.1. What should Accountants do?

Accountants 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.

3.2.4.2. When should Accountants 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

50. Regulation 9(1) DNFBP Regulations and Regulations 3(1)(e) and 21 ICAP and ICMAP Regulations.
51. Regulation 2(1)(i) DNFBP Regulations and Regulation 3(1)(f) ICAP and ICMAP Regulations.
52. Regulation 2(1)(e) DNFBP Regulations and Regulation 3(1)(d) ICAP and ICMAP Regulations.

The following circumstances do not require the application of EDD measures, even if the individual is a PEP (and family members and close associates) because in the following situations, the PEP is not the customer nor the beneficial owner:

Authorised representative of a legal person	Non beneficial owner of a company
• For example. authorised representative of a government entity **Note:** While enhanced due diligence is not required, the reporting firm will still need to identify and verify the identity of the authorised representative. and that the individual is so authorised by hisler organisation.	• The PEP is a director on a board of directors, but there are 9 other directors, and the PEP has only one 1% ownership. • This PEP does not meet the controlling ownership test or the control by other means test. **Note:** Careful consideration needs to be given to the control test for beneficial ownership. The PEP is still a prominent person. and despite miniscule ownership and limited voting rights, it may still influence other directors or senior managament, and thereby control the company.

However, there is nothing precluding a reporting entity from applying EDD to a PEP in the above circumstances, even if is not rule mandated in the AML/CFT laws.

It is also important to note that PEP is one reason why EDD may apply, but not the only factor. EDD may apply in the absence of a PEP, or for reasons additional to the presence of a PEP, e.g., geographical risk.

3.2.4.3. How can Politically Exposed Persons be identified?

PEPs can be identified through the following method:

(a) Reporting entites 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 reporting entity should undertake an independent check. The reporting entity's procedures may include:
    (i) An internet search of the customer's or beneficial owner's background;
    (ii) Databases and reports from commercial service providers

(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 reporting entities.
(d) Reporting entities 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.

3.2.4.4. 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.[53] 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 reporting entity and the customer. Note that this requirement is only for reporting entities to obtain information. There is no requirement for reporting entities 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 reporting entities 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.[54] 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 reporting entity.

If the reporting entity has doubts that the stated source of wealth or funds may be incorrect, it should request documents to confirm of source of wealth or funds, for example, a financial statement or tax return. Unlike for ID documents, these do not need to be originals or certified true copies, unless the reporting entity has doubts regarding the veracity of the documents provided.

53. Regulation 9(2)(c) DNFBP Regulations, Regulations 21(2)(c) ICAP and ICMAP Regulations.
54. Regulation 9(3)(b)(ii) DNFBP Regulations and Regulation 21(3)(b) ICAP and ICMAP Regulations.

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.)

3.2.5. Customer Risk Assessment

Accountants are required to conduct both enterprise risk assessment and individual customer risk assessment, particularly of new customers.[55] The enterprise risk assessment gives a macro assessment of risk in the reporting entity, 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		
Politically Exposed Persons (PEP), or a family member or known close associate of a PEP.	Discretionary trust (e.g. family)	Companies with trusts. Complex ownership structures.
Non-Government Organization (NCO), Not for Profit Organisation (NPO) or charity.	Companies that have nominee shareholders or shares in bearer form.	Cash intensive businesses.
Customers dealing in high value items etc. High value is Rupees 2 million and over	The business relationship will be conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Reporting firm and the client)	Legal persons or arrangements that are personal asset-holding vehicles.

55. Regulation 4 DNFBP Regulations and ICAP and ICMAP Regulations.

Customers belonging to high risk sectors as identified in the NRA except those that are publicly listed companies or regulated by the State Bank of Pakistan	Customers conducting frequent online transactions from locations having tax amnesty to avoid taxes.	Non-resident customers from countries identified by the FATE (refer geographic risk section)
Higher risk products/services		
Accepting large cash payments from the customer.	Managing accounts that would involve large and regular cash deposits.	Managing accounts or transactions for the customer that would involve receipt of funds from unknown or un-associated third parties for services and / or transactions provided by the customer.
Products/services that involve the provision of nominee director, nominee shareholders or shadow directors, or the formation of companies in a third country.	Assisting a customer to form a company that issues bearer shares.	The product or service that favours anonymity e.g. opening a bank account for the customer under the name of Reporting firm, or undertaking wire transfers on behalf of the customer.
Products/services identified as high in NRAs. that client.	When client receives donations and is a body corporate, partnership, association, or any other legal arrangement including non-governmental organizations, and Not for profit organizations.	When the Reporting firm discovers that a client has provided false identification, documentation, or information, and the Reporting firm proposes to continue to deal with
Higher risk delivery channels		
Services or products provided exclusively via telephone. email, etc, where non face-to-face approach is used?		
Higher risk geographic locations		
The jurisdictions which have been identified for inadequate AML/ CFT measures by FATF or called for by FATF for taking counter-measures	Countries subject to sanctions, embargos	Countries identified by credible sources as having significant levels of corruption, or other criminal activity
Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities	Locations identified as high risk in NRA (including in Pakistan)	

3.2.5.1 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.

3.2.5.2 Simplified Due Diligence

Simplified DD may be applied to both the customer or beneficial owner, but only where lower risks have been identified through:[56]

- Adequate analysis through its own risk assessment;
- Any other risk assessments publicly available or provided by FBR or ICAP/ICMAP; 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.

If a risk assessment confirms low risk, simplified due diligence may be applied to:

1. Publicly listed companies (in Pakistan, a FATF member country or a country with equivalent transparency standards on such companies);
2. Financial institutions regulated by the State Bank of Pakistan.

For these two categories, the requirement to verify the beneficial owner may be waived depending on the risk assessment e.g. no prosecutions for criminal offences including money laundering, either in Pakistan or overseas.

56. Regulation 10 DNFBP Regulations and Regulation 23 ICAP and ICMAP Regulations.

3.2.5.3. 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.

3.2.5.4. 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.

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.

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;
- Senior management approval before accepting customer;
- Enhanced ongoing monitoring.

3.2.5.5 Customer Risk Assessment Template

Explanatory Notes:

- This is an example template for customer risk assessment for voluntary use. The reporting entity may wish to amend this template to suit its own circumstances;
- The factors contained therein should be considered by the reporting entity in carrying out its risk assessment for new customers. The list is non-exhaustive and the reporting entity 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 reporting entity 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 reporting entity is required to conduct EDD which involves approval by senior management of the reporting entity 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 reporting entity can then decide whether to accepts the new customer of 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
Muustiy of Iterior/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 REA must also submit a Suspicious Transaction (STR) 7 days of identifying the match and other authorities.*		

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

The customer or beneficial owners 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 from the customer?	YES	NO
Managing accounts that would involve large and regular cash deposits?	YES	NO
Managing accounts or transactions for the customer that could involve receipt of funds from unknown or un-associated third parties for services and / or transactions provided by the customers?	YES	NO
Providing services that involve the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country?	YES	NO
Assisting a customer to form a company that issues bearer shares?	YES	NO
The product or service that favours anonymity e.g. opening a bank account for the customer under the name of the Reporting firm, or undertaking wire transfers or behalf of the customer?	YES	NO

SECTION 1.5: DELIVERY CHANNEL 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? Note: This only applies where there is no physical or live video sighting of the customer.	YES	NO

SECTION 1.6: REPUTATIONAL RISK SCREENING
(refer point # 4 of the explanatory note)

	Response	
Are there adverse news or information arising from further screening of details of customer. beneficial owner 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.'	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: _____

3.2.6. Prohibited Customers and Risk Screening

Reporting entities 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.[57] 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 TFS.

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 reporting entity cannot accept the new customer as the legal person no longer exists. The reporting entity can check online at the SECP website: https://eservices.secp.gov.pk/eServices/NameSearch.jsp.

While not mandated in the AML/CFT legislations, the reporting entity 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 reporting entity does not have a subscription to a commercial risk screening provider. So, if the reporting entity does not have such a subscription, this is on a risk basis only which includes higher risk customers such as PEPs.

57. Regulation 8(1) DNFBP Regulations and Regulation 25 ICAP and ICMAP Regulations.

3.2.7. 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 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:[58]

MANAGING DELAYED CDD VERIFICATION

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

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

Your reporting firm's CDD procedures should mention the circumstances under which the completion of CDD verification after the establishment of business relationship is permitted. however, these noted instances should be rare / limited.

If verification is delayed. measures should be in place to minimise the risk. These could include not completing the company formation — only starting the process: a limit of funds transfers if managing an account: etc.

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

58. Regulation 8(13) to (14) DNFBP Regulations and Regulations 17 and 18 ICAP and ICMAP Regulations.

3.2.8. Unable to complete Customer Due Diligence

Where an accountant is unable to complete CDD, the accountant shall:[59]

(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 accountant cannot complete the CDD process, even when verification is delayed after the start of the business relationship, the accountant 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 accountant is not satisfied with the information and verification commensurate with the higher risk profile of the customer; and
(c) Where too many questions may be tipping off the customer of suspicion by the accountant.

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.

3.2.9. Customer Due Diligence and Tipping Off

If the accountant forms a suspicion of ML/TF and reasonably believes that performing the CDD process will tip-off the customer, the accountant shall not pursue the CDD process and shall file an STR.[60]

3.2.10. 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 accountants must conduct ongoing due diligence of the business relationship.[61] 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 consists of two major components:

59. Section 7D AMLA.
60. Section 7D(2) AMLA.
61. Regulation 8(6) DNFBP Regulations and Regulation 19 ICAP and ICMAP Regulations.

- Scrutinizing transactions:
    - Consistent with customer business profile;
    - Risk profile;
    - Source of wealth and funds, where necessary.
- CDD information and records:
    - Customer information and verification documents, data or information is kept up-t-date;
    - Greater focus on higher risk customers.

The extent to which a reporting entity has to undertake both will depend on the specified services provided. If you are providing services that manages the funds, assets or properties of your customers, e.g., bank account, then scrutinizing transactions will be an integral component of your ongoing CDD processes. The other component on CDD information and records will apply to all your customers, but risk-based, namely, more regular checks for customers rated higher risk than medium or lower risk.

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.

Broadly, there are two types of reviews which are discussed in detail as follows.

(i) Event-driven reviews

The events triggering a CDD information update may include:

- A change in the customer's identity;
- A change in beneficial ownership of the customer;
- A change in the service provided to the customer;
- Information that is inconsistent with the business' knowledge of the customer; or
- A suspicion of ML/TF.

An event driven review may also be triggered by:

- The start of a new engagement;
- Planning for recurring engagements;
- A previously stalled engagement restarting;
- A significant change to key office holders;
- The participation of a PEP;
- A significant change in the customer's business activity (this would include new operations in new countries); and

- There is knowledge, suspicion or cause for concern (for example, where in doubt about the veracity of information provided). If an STR has been made, care should be taken to avoid making any disclosures which could constitute tipping off.

(ii) Periodic reviews

Routine periodic reviews (e.g., annually) to update CDD are also needed. The frequency of updating should be risk-based, making use of the reporting entity's risk assessment, and reflecting the business' knowledge of the customer and any changes in its circumstances or the services it requires.

The CDD procedures necessary for either event-driven or periodic reviews may not be the same as when first establishing a new business relationship. Given how much existing information could already be held, ongoing CDD may require the collection of less new information than was necessary at the customer on boarding stage.

3.2.11. Existing Customers

The reporting entity shall apply CDD requirements to existing customers[62] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.[63]

It is important for accountants, 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.

A centralized system should include a list of existing customers prior to the date of effect of AML/CFT requirements. The reason is existing customer falls into two categories. First, those who are active. Second, those who are dormant. For the second category, a senior management decision should be made on whether all should be considered existing, or have a cut-off date for dormant accounts, e.g. if dormant for a few years, then they would be treated as new customers from an AML/CFT perspective and CDD is undertaken if there is a new engagement. Having two lists of customers will avoid confusion whether a customer is existing or new.

62. Existing customers refer to customers of the reporting entity prior to 29th September 2020, i.e. when the DNFBP Regulations came into force.
63. Regulation 8(16) DNFBP Regulations and Regulation 20 ICAP and ICMAP Regulations.

TABLE ON EXISTING AND NEW CUSTOMERS

Exiting customers (prior to AML/CFT requirements)		New customers (After AML/CFT requirements Coming into force and effect)
Dormant	**Active**	Subject to the full CDD requirements
No ongoing business relationship or services	Ongoing services	
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 triggered 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.	

3.2.12. Third-party conducting Customer Due Diligence

A third party can also conduct CDD on behalf of the accountant.[64] The conditions placed upon the reporting entity when relying on third parties are as follows:

(a) Reporting entities 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 reporting entity should be satisfied that the third party is under the supervision of an AML/CFT regulatory authority;
(e) The reporting entity 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.

If the third party is in the same corporate group as the reporting entity, the reporting entity 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.

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 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: DETAIL ON THE BUSINESS	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

PART 4: SOURCE OF FUNDS OR WEALTH	
What is the main source of income or wealth of the business?	
Income last financial year?	
Assets held by 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	
Name:	**Verification Details** (Original, certified true copy or electronic verification) CNICs/ Smart National Identity Card (SNIC) issued by NADRA or Equivalent for non-residents (refer Part 1 above)
Address:	Incorporation certificate with physical address: or 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 REA 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
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 am 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):	CNICs/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	VERIFCATION 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.	**Note for staff:** Documents required from customer! [these documents may be obtained from the network firm. if available] **Details of company:** 1. SECP registered declaration for commencement of business as required under the Companies Act. 2017 (XIX of 2017). as applicable: 2. List of directors, members and shareholders required to be filed under the Companies Act. 2017 (XIX of 2017). as applicable 3. Register of Beneficial Ownership maintained by the Company. as required under SECP Circulars No.16 and No.20 of 2018. Section 123A of Companies Act 4. 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

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.

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

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 of18 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.

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:	
Name:	**Verification Details** (Original, certified true copy or electronic verification)
	CNICs/ Smart National Identity Card (SNIC) issued by NADRA or Equivalent for non-residents (refer Part 2 above)
Address:	Incorporation certificate with physical address: or 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
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. 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 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/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
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?

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 accountants 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.[65]

Records can be maintained in paper form (in the form of books) or stored in a computer or any electronic device (or on microfilm).[66] As per the law, every reporting entity is to maintain:

(a) A record of all transactions for at least five years after their completion.[67]
(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.[68]
(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.[69]

Furthermore, although not expressly mentioned, as a rule of thumb, reporting entities 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.[70]

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.

64. Section 7B AMLA, Regulation 12 DNFBP Regulations and Regulation 24 ICAP and ICMAP Regulations.
65. Regulation 6(5) DNFBP Regulations.
66. Section 2(xxxii) AMLA and Regulation 6(2) DNFBP Regulations.
67. Section 7C AMLA, Regulation 6(3) DNFBP Regulations and Regulations 29 to 31 ICAP and ICMAP Regulations.
68. Ibid.
69. Section 7(4) AMLA.
70. Regulation 6(4) DNFBP Regulations.

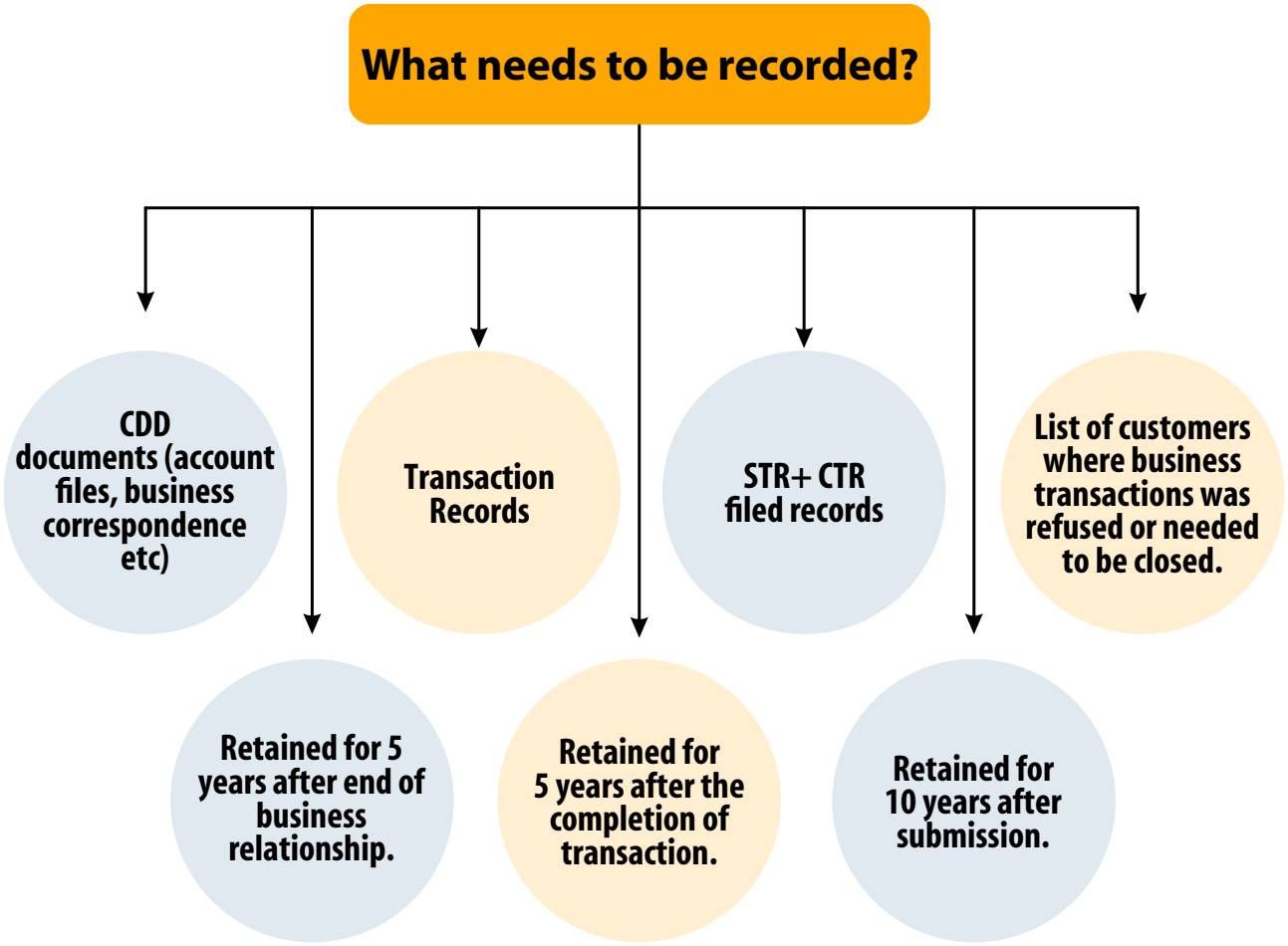
Accountants subject to the DNFBP Regu.ations must keep a list of all such customers where the business transaction was refused or needed to be closed either on account of the failure of the customer to provide:

(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.[71]

4.2. OPERATING PROCEDURES

4.2.1 Record-keeping Requirements

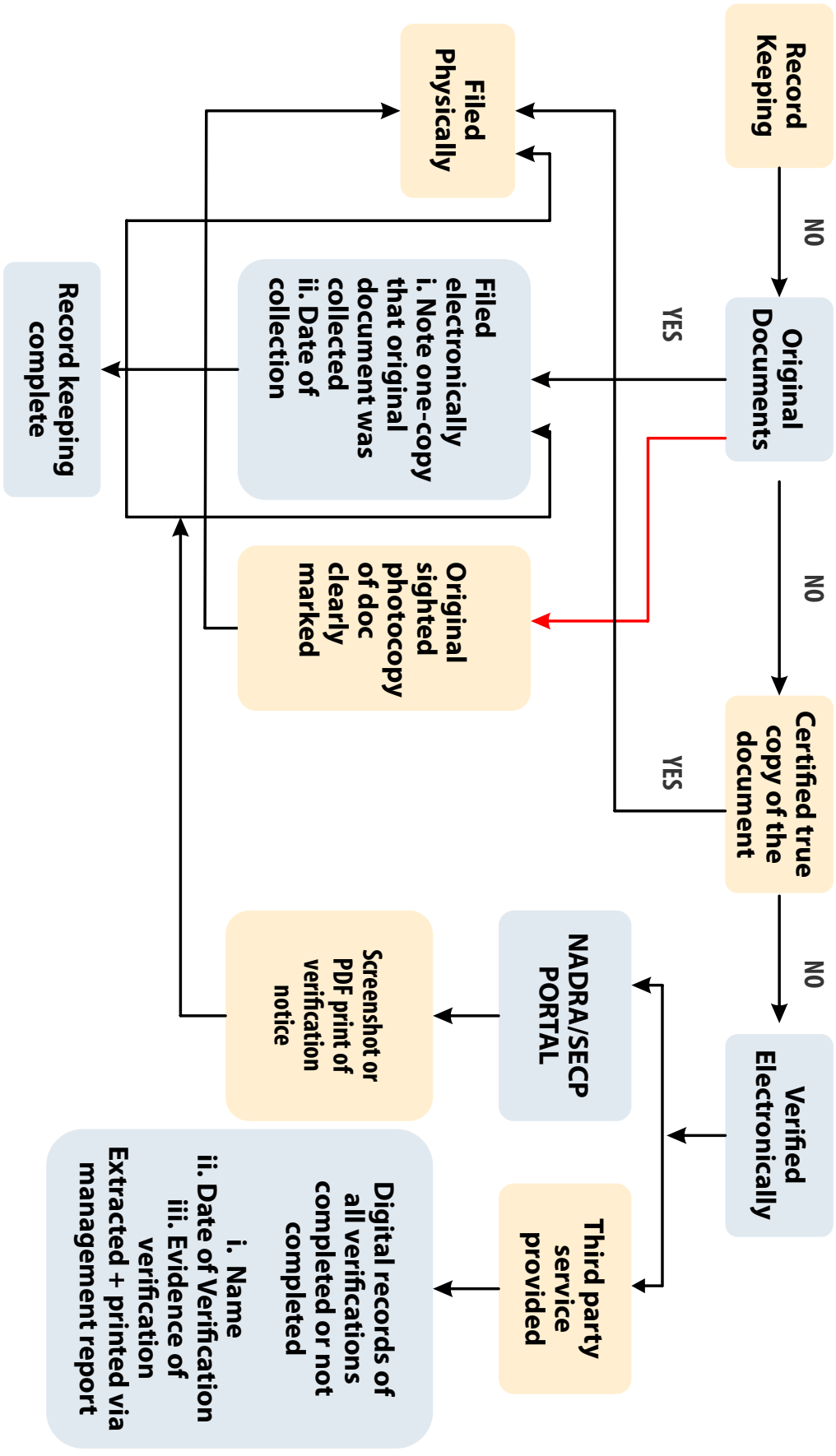
The type of documents that need to be kept as part of the REAs' record and the respective durations are as follows:



71. 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.[72] 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 or ICAP/ICMAP.[73]

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.[74]

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.[75]

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.[76] Moreover, prior to the launch or use of product, practice or technology, DNFBPs shall undertake the risk[77] assessment and take appropriate measures to manage and mitigate the risks.

72. Section 7F AMLA, Regulation 4(1) DNFBP Regulations and Regulation 4 ICAP and ICMAP Regulations.
73. Regulation 4(1) DNFBP Regulations and Regulation 4 ICAP and ICMAP Regulations.
74. Regulation 4(2) DNFBP Regulations and Regulation 5 ICAP and ICMAP Regulations.
75. Regulation 4(3) DNFBP Regulations and Regulation 6 ICAP and ICMAP Regulations.
76. Regulation 5(1)(a) DNFBP Regulations and Regulation 7(a) ICAP and ICMAP Regulations.
77. Regulation 5(1)(b) DNFBP Regulations and Regulation 7(b) ICAP and ICMAP Regulations.

5.2. OPERATING PROCEDURES

5.2.1. Enterprise Risk Assessment

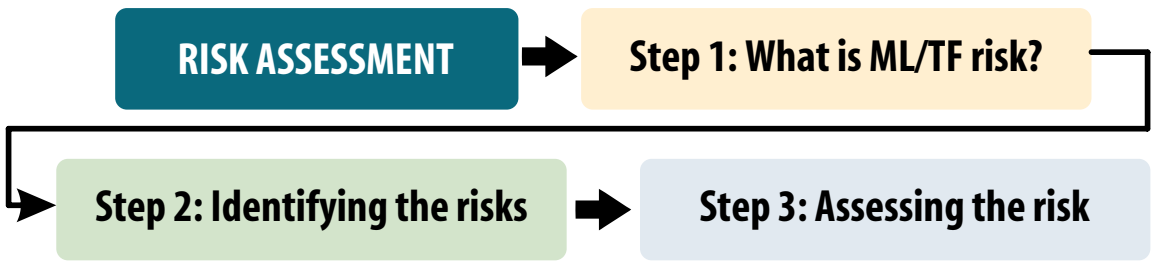
The key purpose of an ML/TF enterprise-wide risk assessment is to drive improvements in risk management by identifying the general and specific ML/TF risks the accountant is facing, determining how these risks are mitigated by the accountant's programme controls, and establishing the residual risk that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

The risk assessment should be approved by the accountant's senior managing official[78] or senior management,[79] as the case may be. 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 reporting entity. The DNFBP Regulations and ICAP and ICMAP Regulations are 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.

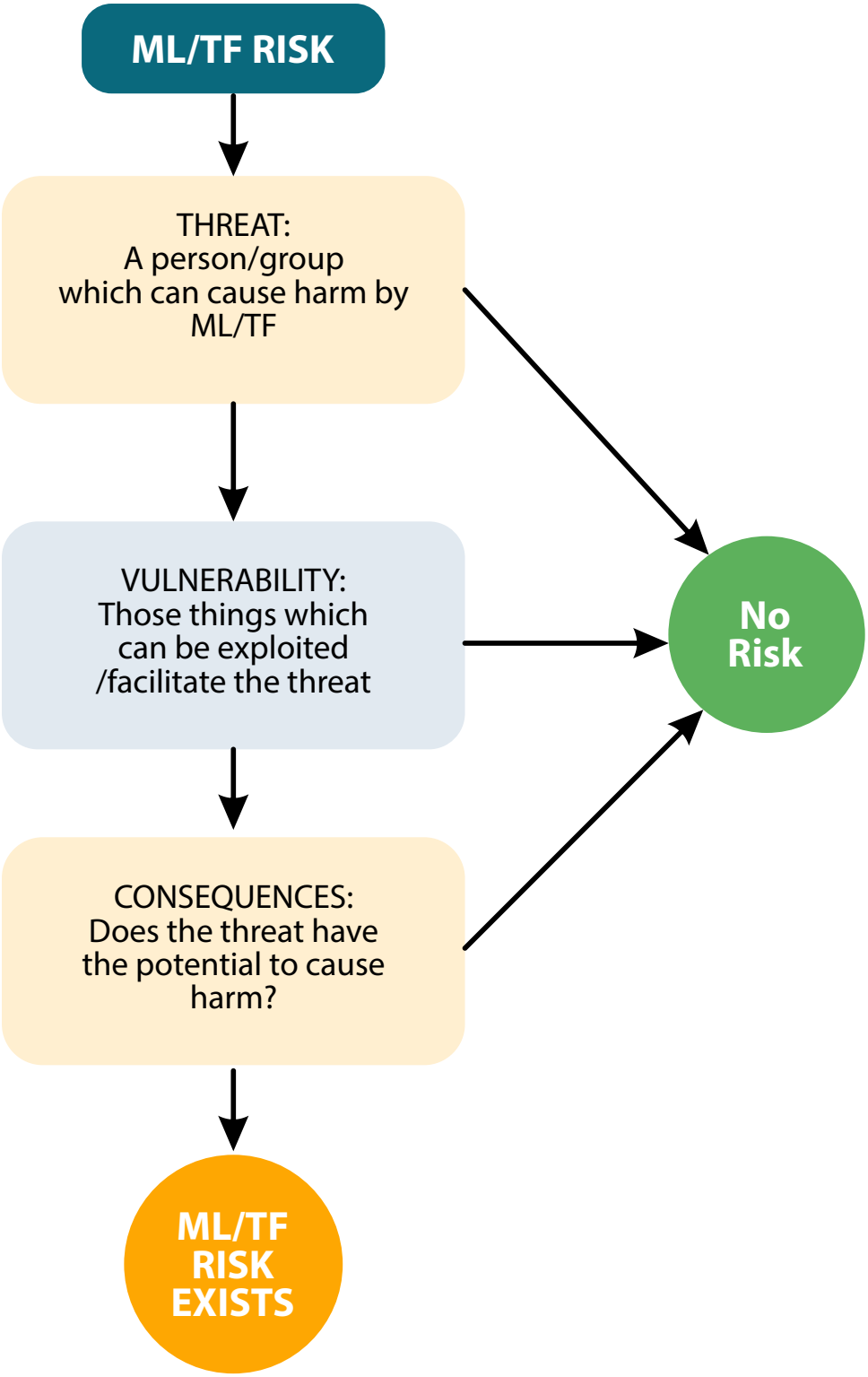
Conducting an enterprise risk assessment contains three steps as indicated below:



78. Regulation 2(1)(p) DNFBP Regulations.
79. Regulation 3(1)(l) ICAP and ICMAP Regulations.

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

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



5.2.3. 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).

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 reporting entities, 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.

The following are some risk indicators for each of the four categories that can help DNFBPs in identifying risks.

(i) Customer Risk

This risk category is considered as a threat to the firm's business. The following question should be considered – does the customer or its beneficial owners have characteristics known to be frequently used by money launderers or terrorist financiers? Customer risk may be summarized as follows:

- Type of customer. For example, an individual who has been entrusted with a prominent public function (or immediate family member or close associate of such an individual) may present a higher risk e.g. politically exposed persons (PEPs), inactive company, links to offshore tax havens and personal asset holding arrangements;
- Transparency of customer. For example, persons that are subject to public disclosure rules, e.g., on exchanges or regulated markets (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g., SBP may indicate lower risk;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk, e.g., those with nominee directors or nominee shareholders or which have issued bearer shares;
- Type and complexity of ownership. For example, the use of overly complex or opaque structures with different layers of entities situated in two or more countries and cross border transactions involving counterparts in different parts of the world, the unexplained use of corporate structures and express

trusts by customers, and the use of nominee and bearer shares may indicate higher risk;

- In the case of an express trust, the nature of the relationship between the settlor(s) and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power. For example, a trust that has company or another trust as a beneficiary may indicate higher risk. While a trust that is established for the benefit of the close family of the settlor may indicate a lower risk;
- Sector risk. Reporting entities should consider the sectors in which their customer has significant operations, and take this into account when determining a customer's risk profile. When considering what constitutes a high risk sector, firms should take into account the findings of the most recent National Risk Assessment (please contact the FMU for a copy). For example, a customer engaged in higher risk trading activities or engaged in a business which involves significant amounts of cash may indicate higher risk;
- Value and frequency of cash or other "bearer" transactions. For example, travelers' cheques and electronic money purses; higher value and/or frequency may indicate higher risk;
- Reputation of customer. For example, a well-known, reputable person, with a long history in its industry, and with abundant independent and reliable information about it and its beneficial owners and controllers may indicate lower risk;
- Behaviour of customer. For example, where there is no commercial rationale for the service that is being sought, or where undue levels of secrecy are requested by a customer, or where a customer is reluctant or unwilling to provide adequate explanations or documents, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered, this may indicate higher risk;
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent customer contact that result in a high level of understanding of the customer relationship may indicate lower risk;
- Value of customer assets. For example, higher value may indicate higher risk;
- Delegation of authority by the applicant or customer. For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk;
- Involvement of persons other than beneficial owners and controllers in the operation of a business relationship may indicate higher risk.

(ii) Geographic Risk

This risk category may be considered both a threat and vulnerability. A reporting entity should consider the following question – are our customers established in countries or regions (including within Pakistan) that are known to be used by money

launderers or terrorist financiers? Though it should be borne in mind that lower risk and legitimate commercial enterprises may be located in high risk countries. Other major factors include the following:

- Ineffective AML/CFT measures;
- Ineffective rule of law and economic stability;
- High levels of organised crime;
- Relevance of bribery and corruption;
- Association with terrorism and TF.

Information on the above should be based on credible sources. Credible sources refer to information that is produced by well-known bodies, are generally regarded as reputable, and that make such information publicly and widely available. These include FATF, FATF-style regional bodies, e.g., APG, FMU, FBR, SRBs (ICAP and ICMAP), SBP, MoFA and other Pakistan government agencies such as NACTA, the reporting entity's experience or the experience of other group entities (where the reporting entity's is part of a network) which may have indicated weaknesses in other jurisdictions, supra-national or international bodies such as the UNSC, IMF, the World Bank and the Egmont Group of Financial Intelligence Units, non-governmental organizations such as Basel AML Index, Tax Justice Network, and the Institute of Economics and Peace.

(iii) Product and services risk (including technology risk)

The products and services your reporting entity offer are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF. A reporting entity should consider the following question – do any of our services have attributes known to be used by money launderers or terrorist financiers?

The specified services have already been identified already as higher risk, and therefore subject to the AML/CFT laws. Within those specified services, there are other factors that will further increase the risk. Some of the main ones are as follows:

- Does your reporting entity accept large cash payments or virtual currency?
- Does the product/service allow for anonymity (i.e., you do not physically see or meet the actual customer)?
- Does the product/service disguise or conceal the beneficial owner of your customer?
- Does the product/service disguise or conceal the source of wealth or funds of your customer?
- Does the product/service allow payments to, or from third parties?
- Does the product/service commonly involve receipt or payment in cash?
- Has the product/service been identified in the NRA, FIU guidance material or

SRAs as presenting a higher ML/TF risk?
- Does the product/service allow for the movement of funds across borders?
- Does it hold boxes, parcels or sealed envelopes in safe custody for customers?
- Does it place funds in customer, nominee or other accounts, where funds are mingled with others' funds?

(iv) Delivery Channel Risk

How your firm delivers products and services are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF. The firm should consider the following question – does the fact that I am dealing with the customer non face to face pose a greater ML/TF risk? The higher risk factors could include the following:

- Indirect relationship with the customer (dealing through intermediaries or other third parties);
- Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
- Does your business have indirect relationships with customers (via intermediaries, pooled accounts, etc.)?
- Do you provide your products/services via agents or intermediaries?
- Do you provide your products/services to overseas jurisdictions?

5.2.4. 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 reporting entity 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 accountants provide. According to international practices, the risk assessment should be reviewed and upgraded at least once every two years.

5.2.5. Sources of Information for Enterprise Risk Assessment

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

(a) Internal Information: The REA'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 REA 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 REA 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 REA'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 REA 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.

5.2.6. Risk Assessment Template

Enterprise Risk Assessment Template with Mitigation Measures					
Risk rating categories			*Low*	*Medium*	*High*
Customer - types of customers we deal with (sellers and buyers in real property)	Are any of my business customers a higher or lower threat for ML/TF?	Likelihood rating of ML/TF (refer to risk matrix)	Consequence rating of ML/TF - minor, moderate, significant, severe (refer to risk matrix)	ML/TF Risk level High, Medium, or Low (refer to risk matrix)	Risk Mitigation Measures
Geographic locations/countries or region we deal with	Is it considered higher risk? Why?	Likelihood rating of ML/TF	Consequence rating of ML/TF	Risk level High, Medium, or Low	Risk Mitigation Measures
Services/Products Risk - types of products and services we offer	Are my services/ product at higher risk of abuse?	Likelihood rating of ML/TF	Consequence rating of ML/TF	Risk level High, Medium, or Low	Risk Mitigation Measures
Delivery Channels - how we deliver our services	Are my delivery channels more vulnerable to potential abuse?	Likelihood rating of ML/TF	Consequence rating of ML/TF	Risk level High, Medium, or Low	Risk Mitigation Measures
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.[80] Reporting entities are also required to implement policies and procedures to ensure their compliance with the law that impose TFS obligations upon reporting entities.[81]

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;[82]
(b) Monitor the implementation of those controls and enhance them if necessary;[83] and
(c) Take enhanced measures to manage and mitigate the risks where higher risks are identified.[84]

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.[85] 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;

80. Section 7G AMLA.
81. Section 7H AMLA.
82. Regulation 4(2)(a) DNFBP Regulations and Regulation 5(a) ICAP and ICMAP Regulations.
83. Regulation 4(2)(b) DNFBP Regulations and Regulation 5(b) ICAP and ICMAP Regulations.
84. Regulation 4(2)(c) DNFBP Regulations and Regulation 5(c) ICAP and ICMAP Regulations.
85. Regulation 7(1)(a) DNFBP Regulations and Regulation 27(1)(a) ICAP and ICMAP 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.[86]

(b) Screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;[87]

(c) An ongoing employee training program;[88] and

(d) An independent audit function to test the system.[89] 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.[90]

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.

86. Regulation 7(3)(c) DNFBP Regulations.
87. Regulation 7(1)(b) DNFBP Regulations and Regulation 27(1)(b) ICAP and ICMAP Regulations.
88. Regulation 7(1)(c) DNFBP Regulations and Regulation 27(1)(c) ICAP and ICMAP Regulations.
89. Regulation 7(1)(d) DNFBP Regulations and Regulation 27(1)(d) ICAP and ICMAP Regulations.
90. 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.[91]

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) TFS;
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 reporting entity'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

Senior Management

The senior management must:
(a) Engage in decision-making on policies and procedures;
(b) Oversee risk-based compliance programs;
(c) Encourage a culture of compliance;
(d) Ensure adherence to the firm's policies, procedures and processes designed to

91. Regulation 5 DNFBP Regulations and Regulation 28 ICAP and ICMAP Regulations.

limit and control risks; and

(e) Ensure sufficient resources are devoted to the implementation of the reporting entity's AML/CFT compliance programme (this includes the building of expertise through training, recruitment, taking professional advice and 'learning by doing'; it also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making).

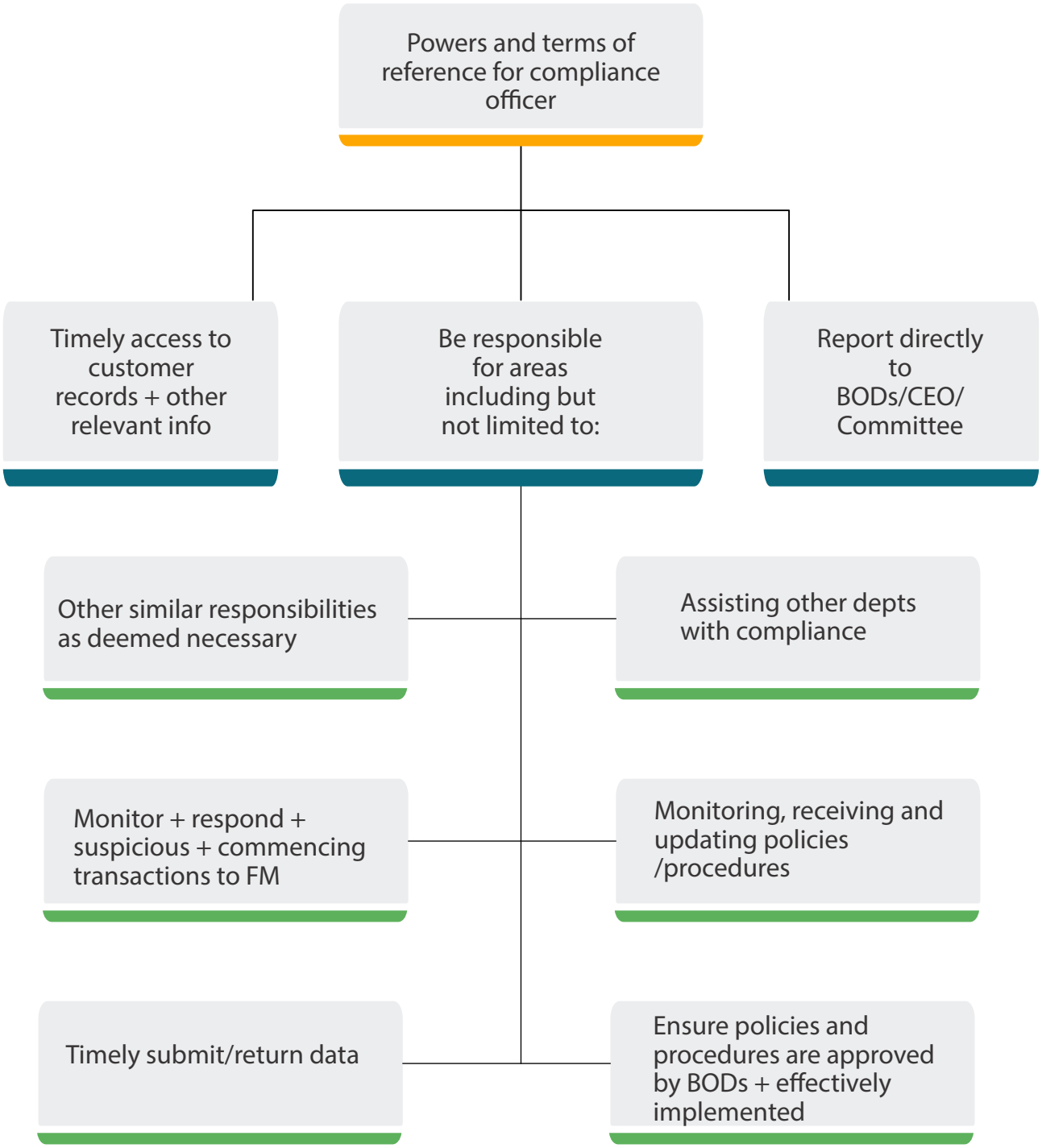
Compliance Officer

Depending on the size of reporting entity, the compliance officer could be:

- A senior partner;
- Someone from a senior level who has direct access to senior management of the firm; or
- In the case of a sole proprietorship, the sole proprietor can be the compliance officer.

The compliance officer can carry out other duties not related to AML/CFT compliance. It does not have to be a standalone position, but it must be a staff member of the reporting entity, irrespective of the employment conditions, e.g., permanent or contractual.

Such 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:

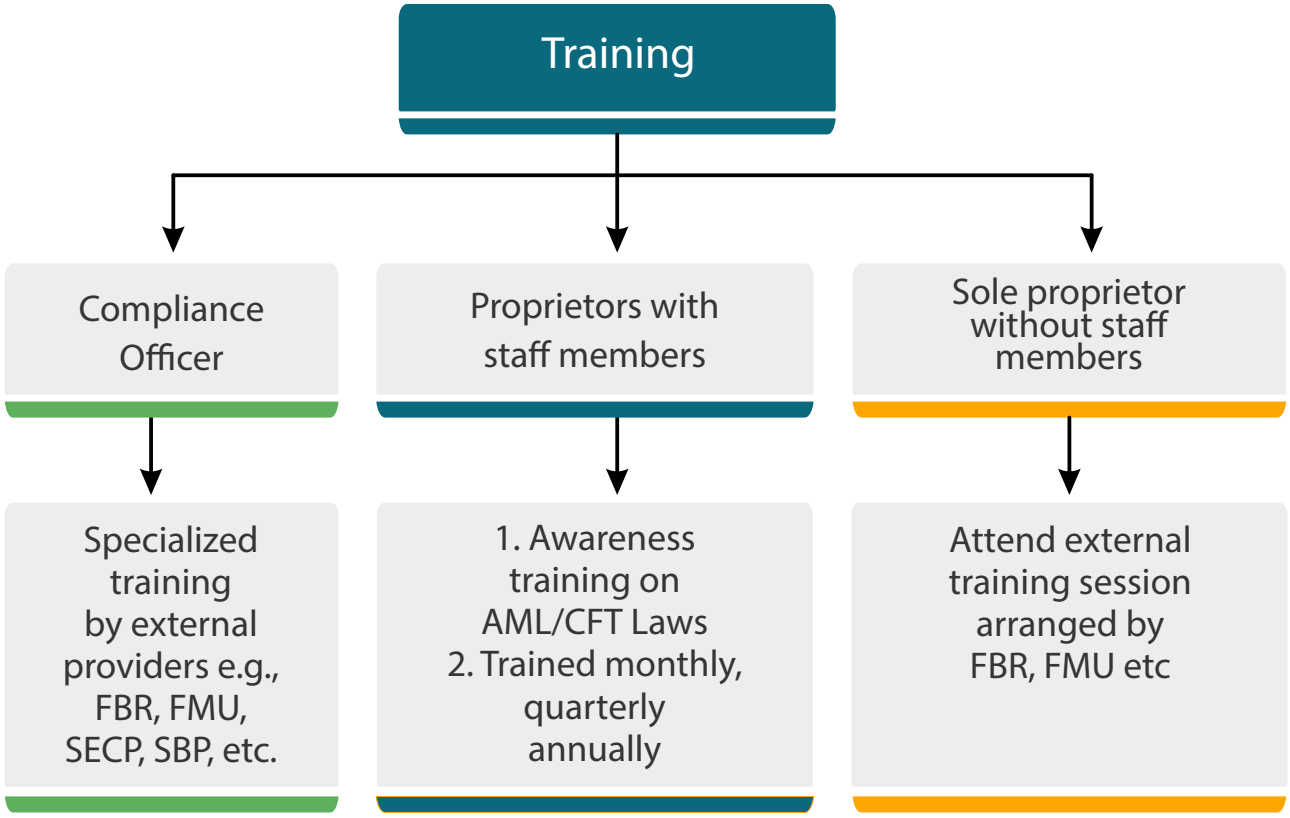
a) Written references from previous employers;
b) Character statements from people of good standing in the community (e.g. religious figure, medical practitioner, police officer);
c) Internet search;
d) For new graduates, a reference letter from a university lecturer, university society or from a person 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 Guidelines for Accountants issued by FBR (December 2020)	https://download1.fbr.gov.pk/Docs/20218216826 3117AMLCFTGuidelines_Accountantsupdated July,2020.pdf
2	AML/CFT Sanctions Rules, 2020 (SRO 950(I)/2020)	https://download1.fbr.gov.pk/Docs/2020101515 10533067AML-CFT-Sanction-Rules-2020-SRO-NO-950I-2020.pdf
3	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
4	Anti-Terrorism Act, 1997	https://nacta.gov.pk/wp-content/uploads/2017/08/Anti-Terrorism-Act-1997.pdf
5	DNFBPs FBR Order No. 1 of 2021	https://download1.fbr.gov.pk/Docs/20211130101 15821779ConditionCircular01of2021-housing.pdf
6	FBR AML/CFT Regulations for DNFBPs, 2020 (SRO 924 (1)/2020)	https://download1.fbr.gov.pk/SROs/2020929179 76805SRO9242020.pdf
7	FMU Circular No. 4 of 2020- Red Flags Indicators for Accountants	https://www.fmu.gov.pk/docs/Circular-for-Accountants-Red-flags.pdf https://www.fmu.gov.pk/docs/Red-Flag-Indicators-for-Accountants-final.pdf
8	Guidelines for DNFBPs on Targeted Financial Sanctions (TFS) Under Nations Security Council Resolutions	https://download1.fbr.gov.pk/Docs/20213820317 41608pg1.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://icap.org.pk/files/per/aml/AMCFTGuidelinesforAccountants.pdf

No.	Document	Link
11	ICAP AML/CFT Guidelines for Accountants	https://icap.org.pk/files/per/aml/AMCFTGuidelinesforAccountants.pdf
12	ICAP AML/CFT Regulations for Chartered Accountants Reporting Firms	https://icap.org.pk/files/per/aml/ICAPAMLCFTRegulations.pdf
13	ICAP FAQs	https://icap.org.pk/files/per/aml/FAQs.pdf
14	ICMAP AML/CFT Guidelines for Accountants	https://www.icmainternational.com/downloads/AML/AMLCFTGuidelinesforAccountants2020.pdf
15	ICMAP AML/CFT Regulations for Cost and Management Accountants Reporting Firms	https://www.icmainternational.com/News_Pdf/AML_CFT_Regulations_ICMAPakistan.pdf
16	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-OrganizationsEng-3.pdf https://nacta.gov.pk/proscribed-persons/
17	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