



ANTI – MONEY
LAUNDERING AND COUNTER
FINANCING OF TERRORISM

Guidelines for Accountants



Table of Contents

GLOSSARY OF ACRONYMS / TERMS	5
1. INTRODUCTION	6
1.1 Purpose	6
1.2 Scope and terminology	6
1.3 Structure	7
2. BACKGROUND	9
2.1 Why are accountants required to comply with AML / CFT?	9
2.2 Financial Action Task Force (FATF)	9
2.3 FATF 40 Recommendations	9
2.4 Asia/Pacific Group on Money Laundering (APG)	10
2.5 The FATF grey list	10
2.6 Money laundering	10
2.7 Terrorism financing	11
2.8 Differences between money laundering and terrorism financing	11
3. PAKISTAN’S AML / CFT REGULATORY REGIME	11
3.1 AML / CFT regulatory regime in Pakistan	11
3.2 Government authorities responsible for accountants	13
4. SPECIFIED SERVICES SUBJECT TO AML / CFT	15
4.1 Specified services subject to AML / CFT	15
4.2 Auditing, other assurance services, internal accounting and book keeping services	16
4.3 Common examples of ‘specified services’	16
4.4 Support and guidance on AML / CFT	18
5. RISK ASSESSMENT AND RISK MITIGATION	20
5.1 Statutory requirements under AML / CFT legislations	20
5.2 Sanctions for non-compliance	20
5.3 ML / TF enterprise wide risk assessment	20
5.4 Difference between an inherent and residual enterprise risk assessment	21
5.5 How to conduct the enterprise risk assessment on ML / TF	21
5.6 Quantitative and qualitative information for enterprise risk assessment	26
5.7 Example of an enterprise risk assessment template	27
6. AML / CFT Programme, Policies and Procedures	31
6.1 Statutory requirements under AML / CFT legislations	31
6.2 Sanctions for non-compliance	32
6.3 Role of senior management	32
6.4 Compliance officer	32
6.5 Written policies and procedures	33
6.6 Group compliance	34
6.7 Staff vetting and employment	34
6.8 AML / CFT training	35
6.9 Monitoring and review of AML / CFT programme	36
6.10 Independent audit function	36

7. Risk Based Customer Due Diligence (CDD)	37
7.1 Statutory requirements under AML / CFT legislations	37
7.2 Sanctions for non-compliance.....	38
7.3 Who to conduct CDD on	38
7.4 Timing of CDD.....	39
7.5 CDD components	40
7.6 Customer verification documents, data or information	42
7.7 Identifying and verifying beneficial ownership	44
7.8 Politically Exposed Person (PEP)	55
7.9 Source of wealth or funds.....	58
7.10 Enterprise risk assessment and customer risk assessment	60
7.11 Customer risk assessment and risk based CDD	60
7.12 Three categories of CDD	62
7.13 Simplified CDD.....	62
7.14 Standard CDD	63
7.15 Enhanced CDD	63
7.16 Examples of standard and enhanced CDD	63
7.17 Prohibited customers and risk screening.....	67
7.18 Delayed verification	67
7.19 Unable to complete CDD	68
7.20 CDD and tipping off.....	69
7.21 Ongoing monitoring of new customers	69
7.22 Existing customers.....	70
7.23 Reliance on third party to conduct CDD	71
8. Targeted Financial Sanctions	72
8.1 Statutory requirements under AML / CFT legislations	72
8.2 Sanctions for non-compliance.....	73
8.3 United Nations Security Council and Pakistan Sanctions.....	73
8.4 Ministry of Foreign Affairs Updates	74
8.5 Screening new and existing customers and their transactions	75
9. Suspicious Transaction Report (STR)	78
9.1 Statutory requirements under AML / CFT legislations	78
9.2 Sanctions for non-compliance.....	78
9.3 Reporting of STRs.....	79
9.4 Scope of STR reporting	80
9.5 AML / CFT red flag indicators for accountants	80
9.6 Internal reporting procedures.....	80
9.7 Reporting to FMU via goAML.....	81
9.8 Content of STR	82
9.9 Types of STRs	83
9.10 Timeline for STR reporting	83
9.11 No tipping off to customer.....	83

9.12	Protection for reporting in good faith	83
10.	Currency Transaction Report (CTR).....	84
10.1	Statutory requirements under AML / CFT legislations	84
10.2	Sanctions for non-compliance	84
10.3	Currency threshold for CTR.....	85
10.4	Reporting to FMU via goAML.....	85
10.5	Two Types of CTRs and Contents of CTR	85
10.6	Timeline for CTR reporting	85
10.7	No tipping off to customer.....	86
11.	Record Keeping	87
11.1	Statutory requirements under AML / CFT legislations	87
11.2	Sanctions for non-compliance.....	87
11.3	Table on record keeping requirements	88
Annex 1	– Customer Risk Assessment Template.....	89
Annex 2	- Customer Due Diligence Form – Template (Company)	94
Annex 3	- Customer Due Diligence Form – Template (Individual / Sole Proprietor).....	98
Annex 4	- Customer Due Diligence Form – Template (Trust).....	101
Appendix A	– Useful web links to publications / documents / information	104

Notice to the reader

All reasonable care has been taken in the preparation of these Guidelines, but it necessarily contains information in summary form and is therefore intended for general guidance only. The publication does not amend or override, and it is not intended to be a substitute for reading the Laws, Regulations and guidance issued in Pakistan as well as by the United Nations, including but not limited to the following: the Anti-Money Laundering Act 2010, the SRB AML / CFT Regulations for Reporting Firms, FBR AML / CFT Regulations for DNFbps, AML / CFT Sanctions Rules, The Anti-Terrorism Act 1997, the United Nations (Security Council) Act 1948 , the Anti-Money Laundering Regulations 2015, the United Nations (Security Council) Act 1948 Statutory Regulatory Orders, and the Financial Monitoring Unit (FMU) guidance documents on reporting. A person should utilize his/her professional judgment and the facts and circumstances involved in each particular case. The information presented in the Guidelines should not be construed as legal, auditing, or any other professional advice or service. The Institute (refers to both the ICAP and ICMA PAKISTAN) and/or its staff do not accept any liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly, whether in contract, or otherwise from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.

GLOSSARY OF ACRONYMS / TERMS

AMLA	Anti-Money Laundering Act 2010
AML	Anti-Money Laundering
AML / CFT legislations	AMLA SRB AML / CFT Regulations for Reporting Firms FBR AML / CFT Regulations for DNFBPs UNSC Act ATA AML / CFT Sanctions Rules Counter Measures for High Risk Jurisdiction Rules
AML Regulations 2015	Anti-Money Laundering Regulations 2015
ATA	Anti-Terrorism Act 1997
AML / CFT Sanction Rules	AML / CFT Sanction Rules 2020 SRO NO 950(I)/2020
FBR AML / CFT Regulations for DNFBPs	Federal Board of Revenue Anti Money Laundering and Countering Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions
ATA	Anti-Terrorism Act 1997
APG	Asia/Pacific Group on Money Laundering
BO	Beneficial Ownership
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
Counter Measures for High Risk Jurisdiction Rules	Counter Measures for High Risk Jurisdiction Rules, 2020
CTR	Currency Transaction Report
DNFBP	Designated Non-Financial Business or Profession
ECDD or EDD	Enhanced Customer Due Diligence
FBR	Federal Board of Revenue
FATF	Financial Action Task Force
FMU	Financial Monitoring Unit
Guidelines	Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT) - Guidelines for Accountants
ICAP	Institute of Chartered Accountants of Pakistan
ICMA PAKISTAN	Institute of Cost and Management Accountants of Pakistan
ML	Money Laundering
PF	Financing of Proliferation
NACTA	National Counter Terrorism Authority
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
Reporting firm	Accountants supervised by the two SRBs and FBR
SBP	State Bank of Pakistan
SECP	Securities and Exchange Commission of Pakistan
SRB	Self-Regulatory Body i.e. ICAP and ICMA PAKISTAN
SRB AML / CFT Regulations for Reporting Firms	Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms
SRO	Statutory Regulatory Order
STR	Suspicious Transaction Report
TF	Terrorism Financing
UN	United Nations
UNSC Act	United Nations (Security Council) Act, 1948
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution

1. INTRODUCTION

1.1 Purpose

1. The purpose of these *Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT) - Guidelines for Accountants* (“**The Guidelines**”) is to provide guidance for accountants providing specified services subject to AML / CFT legislations in Pakistan.
2. The Guidelines have been prepared jointly by Pakistan’s three designated AML / CFT supervisors of accountants in Pakistan, namely The Institute of Chartered Accountants of Pakistan (ICAP), The Institute of Cost and Management Accountants of Pakistan (ICMA PAKISTAN) and the Federal Board of Revenue (FBR).
3. Accountants are only subject to AML / CFT measures if they provide the specified activities or services as defined in the Anti Money Laundering Act (AMLA) Sections 2 (xii) (c) (d). All accountants, therefore, should review Section 4 in the Guidelines to determine whether they provide the specified services, and if so, what are the AML / CFT requirements, and how to implement the requirements. These are further explained in Sections 5 to 12 of the Guidelines.

1.2 Scope and terminology

4. The Guidelines are focused on AML / CFT measures such as risk assessment, AML / CFT programme, CDD, beneficial ownership, politically exposed persons, targeted financial sanctions, Suspicious Transaction Report (STR), Currency Transaction Report (CTR) and record keeping. Those measures are further explained in the Guidelines.
5. The Guidelines do not add new regulatory requirements upon accountants.
6. The Guidelines do not address the broader criminal conduct associated with those who engaged in, or aid or abet those engaged in money laundering (ML) or terrorism financing (TF). Those criminal offences under the AMLA and other laws apply to all persons’ subject to Pakistan’s laws.
7. In addition to the AMLA, the three main regulations referred to in the Guidelines are:
 - The Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms (SRB AML / CFT Regulations for Reporting Firms)
 - The Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms (SRB AML / CFT Regulations for Reporting Firms)
 - The Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions (FBR AML / CFT Regulations for DNFBPs)
 - AML / CFT Sanction Rules 2020 SRO NO 950(I)/2020 (AML / CFT Sanction Rules)
8. Both the ICAP and ICMA PAKISTAN, as Self-Regulatory Bodies (SRBs), have been designated by Federal Government pursuant to AMLA (Section 6A) as AML / CFT regulatory authorities. To avoid repetition and any perceived favouritism, and purely for the purposes of the Guidelines, the two professional bodies will be referred to as “*SRBs*” and their AML / CFT regulations collectively referred to as the “*SRB AML / CFT Regulations for Reporting Firms*”. Except for the name of the SRB, the two regulations are identical.
9. The FBR AML / CFT Regulations for DNFBPs are very similar to the SRB AML / CFT Regulations for Reporting Firms. However, they are not identical in terms of numbering and there are sector specific requirements covering other DNFBPs that are not applicable to accountants (accountants licensed by ICAP

and ICMA PAKISTAN). For these reasons, they are referred separately in the Guidelines.

10. For ease of reference, unless specifically referred, all applicable AML / CFT laws and regulations will be referred to in the Guidelines as AML / CFT legislations.
11. The Guidelines use the term “Customer” as the term is more broadly used in AML / CFT i.e. customer due diligence and not client due diligence. The term customer should be regarded as synonymous with the term “client” which is more commonly used by the accountancy profession.
12. In the Guidelines where the terms “must”, “required”, “requirements” or “shall” are used, this means that the information is referring directly to an obligation that is specified in AML / CFT legislations. Where the term “should” is used, it is making a recommendation (which is reader / users choice to accept or not). In most cases, the Guidelines are limited to mandatory regulatory requirements.
13. For the purposes of the Guidelines, the term “reporting firm” applies to all accountants supervised by the two SRBs and the FBR. In the FBR AML / CFT Regulations for DNFBPs, they are referred to as DNFBPs or regulated person.
14. The term “reporting firm” or “reporting firms” are used interchangeably in the Guidelines and refer to both the singular and plural.

1.3 Structure

15. The Guidelines have been organized into the following sections:
 1. **Introduction** – Explains the purpose, scope and content of the Guidelines;
 2. **Background** – Offers Information on the global and regional context of international AML / CFT standards, the Financial Action Task Force (FATF) 40 Recommendations, Asia/Pacific Group on Money Laundering (APG), and explains ML and TF.
 3. **AML / CFT and Pakistan’s Regulatory Regime** – Lists Pakistan’s AML / CFT related laws, outlines the requirements for AML / CFT legislations applicable to accountants;
 4. **Specified Services Subject to AML / CFT** – Describes the AML / CFT requirements applicable to accountants engaged in specified activities / services;
 5. **Risk Assessment and Risk Based Approach** – Explains the rationale and purpose of risk based approach for AML / CFT system and procedures, lists responsibilities in relation to the risk based approach, summarizes the categories of ML /TF risks and outlines the risk assessment methodology for accountants;
 6. **AML / CFT Programme** – Explains the key components of an AML / CFT programme including written policies and procedures, compliance officer, staff on boarding, training, monitoring and internal audit - which provide the foundation for effective implementation of enterprise risk assessment, customer due diligence, targeted financial sanctions, reporting to the FMU and record keeping;
 7. **Risk Based Customer Due Diligence (CDD)** – Explains the rationale and purpose of CDD, the timing of CDD, the categories of CDD, politically exposed persons (PEPs), reliance on third parties and ongoing CDD;
 8. **Targeted Financial Sanctions** – Explains the legal basis and how to implement targeted /financial sanctions;

- 9. Suspicious Transaction Report (STR)** - Outlines the reporting firm’s responsibilities of STR reporting to the Financial Monitoring Unit (FMU), the possible scenarios triggering such reporting and the procedures for reporting;
 - 10. Currency Transaction Report (CTR)** – Outlines the reporting firm’s responsibilities of filing CTRs to the FMU;
 - 11. Record Keeping** – Describes the reporting firm’s responsibility for the AML / CFT related record maintenance and retention.
- 16.** It is recognised that a “one-size-fits-all approach” does not work well for all reporting firms. Nevertheless, the Guidelines include templates on enterprise risk assessment, customer risk assessment and customer due diligence/acceptance to be used on a voluntary basis, or amended to suit the specific needs of the reporting firm. The aim is to reduce the regulatory burden on less well-resourced, or sole practitioner reporting firms who may not have funds or staff to develop timely tools for risk assessments and customer diligence or acceptance forms.

2. BACKGROUND

2.1 Why are accountants required to comply with AML / CFT?

17. The reason accountants are subject to the FATF standards and AML / CFT measures is because accountants are “gate keepers” to the financial system. Arising from the financial and consultancy nature of work, accountants may have a higher chance of crossing paths with money launderers or dealing with illicit funds from ML or TF. Money launderers or terrorism financiers may obtain assistance from accountants without them fully realizing it.

18. In consideration of their role in the business world, it is recognised that accounting firms (ranging from a sole practitioner to a large firm), and their staff can contribute to AML / CFT. Accordingly, it is crucial for firms and their staff to be familiar with the risks and crime of ML and TF, and their role to report actual and suspected ML and TF activities. There is also a role on countering proliferation financing (CPF), but this is limited to targeted financial sanctions under the AML / CFT legislations.

2.2 Financial Action Task Force (FATF)

19. Pakistan’s AML / CFT regulatory regime is strongly informed by the international AML / CFT standards promulgated by The Financial Action Task Force (FATF). The FATF is an international task force established in 1989 to develop international standards to combat ML, TF and the financing of proliferation (PF). The FATF published a revised set of 40 Recommendations on AML / CFT measures in 2012, which are being continuously updated. Further information on the FATF is available at <http://www.fatf-gafi.org/>.

2.3 FATF 40 Recommendations

20. The FATF 40 Recommendations (along-with their Interpretive Notes and Glossary) provide a complete set of counter-measures against ML and TF covering the criminal justice system and law enforcement, preventive measures in the financial and designated non-financial businesses and professions (DNFBPs), and international co-operation.

21. The FATF Recommendations of specific concerns to accountants are those covering DNFBPs. DNFBPs include the following:

- Casinos
- Real estate agents
- Dealers in precious metals and stones
- Trust and *company service providers*
- Lawyers, notaries, other independent legal professionals and **accountants** – when they prepare for or carry out transactions for their customer concerning the following activities:
 - buying and selling of real estate;*
 - managing of customer money, securities or other assets;*
 - management of bank, savings or securities accounts;*
 - organisation of contributions for the creation, operation or management of companies;*
 - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.*

22. The applicable FATF Recommendations for accountants (and other DNFBPs) are:

- FATF Recommendation 22 (DNFBPs: Customer due diligence)
- FATF Recommendation 23 (DNFBPs: Other measures)
- FATF Recommendation 28 (Regulation and supervision of DNFBPs)

23. Other FATF Recommendations which are not specifically targeted at DNFBPs, but are also applicable to DNFBPs include:

- FATF Recommendation 1 (Assessing risks & applying a risk-based approach)
- FATF Recommendation 6 (Targeted financial sanctions related to terrorism & TF)
- FATF Recommendation 7 (Targeted financial sanctions related to PF)
- FATF Recommendation 35 (Sanctions)

2.4 Asia/Pacific Group on Money Laundering (APG)

24. The Asia/Pacific Group on Money Laundering (APG) is a FATF Style Regional Body. The APG is an associate member of FATF. It is an international organisation, consisting of 41 member jurisdictions. The APG is focused on ensuring that its members effectively implement the FATF Recommendations against ML, TF and PF. (For further information on the APG, visit: <http://www.apgml.org/>.)

25. Pakistan is not a member of the FATF, but is a member of the APG. The APG undertook a mutual evaluation of Pakistan in 2019. A copy of the Mutual Evaluation Report of Pakistan 2019 is available at <http://www.apgml.org/documents/>. The report found many deficiencies on FATF Recommendations 22, 23 and 28 relating to DNFBPs i.e. accountants, real estate agents, jewellers, dealers in precious stones and metals and lawyers. They were rated either as non-compliant or partially compliant. For FATF Recommendations 1,6 and 7 on risk assessment and targeted financial sanctions, these were rated only partially compliant.

2.5 The FATF grey list

26. Pakistan is currently under the FATF International Cooperation Review Process (ICRG) “Jurisdictions under Increased Monitoring” or “Grey list” process. Pakistan has committed to working with the FATF to address strategic deficiencies to counter ML and TF. Pakistan has also committed to improving its broader compliance with the FATF standards as part of its membership with the APG.

2.6 Money laundering

27. Generally, money is the foremost reason for engaging in any type of criminal activity that generates funds. A predicate offense is the underlying crime that generates the funds to be laundered. The examples of predicate offences include inter-alia corruption, bribery, fraud, forgery, counterfeiting, kidnapping and corporate and fiscal offences. The offences listed in the Schedule to the AMLA have been declared as predicate offences.

28. ML is the method by which criminals disguise or attempt to disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence.

29. Section 3 of AMLA defines the offence of ML as follows:

“A person shall be guilty of offence of money laundering, if the person:

- a) acquires, converts, possesses, uses or transfers property, knowing or having reason to believe that such property is proceeds of crime;*
- b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of property, knowing or having reason to believe that such property is proceeds of crime;*

- c) *holds or possesses on behalf of any other person any property knowing or having reason to believe that such property is proceeds of crime; or*
- d) *participates in, associates, conspires to commit, attempts to commit, aids, abets, facilitates, or counsels the commission of the acts specified in clauses (a), (b) and (c).*

2.7 Terrorism financing

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

31. Section 11 of The Anti-Terrorism Act 1997 (ATA) defines and criminalises TF on the basis of the Terrorism Financing Convention. While all aspects of Section 11 are important for the criminalisation of TF, Section **11J “Funding Arrangements”** provides a definition of TF:

(1) A person commits an offence if he-

(a) enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another; and

(b) has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

(2) Any person in Pakistan or a Pakistani national outside Pakistan shall commit an offence under this Act, if he knowingly or wilfully makes money or other property or services available, directly or indirectly, wholly or jointly, for the benefit of a proscribed organization or proscribed person.”

2.8 Differences between money laundering and terrorism financing

32. The main differences between ML and TF are:

- For ML to occur, the funds involved must be the proceeds of criminal conduct, and the mental element is normally for profit.
- For TF to occur, the source of funds is irrelevant, i.e. the funds can be from a legitimate or illegitimate source, and the mental element is normally ideology or cause driven.
- TF occurs before the physical act of terrorism, while ML occurs after the predicate offence physical act has been completed.

3. PAKISTAN’S AML / CFT REGULATORY REGIME

33. This section and the next of the Guidelines should be read by all accountants to assist in ascertaining whether they provide specified services subject to AML / CFT.

3.1 AML / CFT regulatory regime in Pakistan

34. As of October 2020, the relevant laws and regulations applicable to accountants are contained in the following laws and regulations:

- The AMLA 2020
- The Anti-Money Laundering Regulations 2015 (AML Regulations 2015)
- SRB AML / CFT Regulations for Reporting firms

- FBR AML / CFT Regulations for DNFBPs
- The United Nations (Security Council) Act 1948 (UNSC Act)
- The Anti-Terrorism Act 1997 (ATA)
- United Nations Security Council (Freezing and Seizure) Order, 2019 (UN Act Freezing and Seizing Order);
- UNSC Act Statutory Regulatory Orders (UN SROs) by the Ministry of Foreign Affairs
- Ministry of Interior/National Counter Terrorism Authority (NACTA) Proscribed Organizations under ATA
- AML / CFT Sanction Rules 2020 SRO NO 950(I)/2020 (AML / CFT Sanctions Rules)
- Counter Measures for High Risk Jurisdiction Rules, 2020 (Counter Measures for High Risk Jurisdiction Rules)

AML / CFT LAWS AND ENFORCEABLE MEANS ON ACCOUNTANTS		
Law and enforceable means	Accountants - SRB supervised (ICAP and ICMA PAKISTAN)	Other Accountants - FBR supervised
<p>AMLA (as amended September 2020) covers the following:</p> <ul style="list-style-type: none"> - Risk assessment and mitigation - Compliance program - Record keeping - CDD - Reliance on third parties - Targeted financial sanctions - Reporting of STR and CTR - Monitoring - Sanctions 	Yes	Yes
<p>SRB AML / CFT Regulations for Reporting Firms cover the following:</p> <ul style="list-style-type: none"> - Risk assessment and mitigation - CDD and beneficial ownership - Targeted financial sanctions obligations - Reporting STR and CTR - Internal Controls - Record Keeping - Sanctions 	Yes	No
<p>FBR AML / CFT Regulations for DNFBPs cover the following:</p> <ul style="list-style-type: none"> - Risk assessment and mitigation - Record Keeping - CDD and beneficial ownership - Reliance on third parties - Targeted financial sanctions obligations - Reporting STR and CTR - Monitoring and compliance - Sanctions 	No	Yes
<p>ATA</p> <p>United Nations Security Council (Freezing and Seizure) Order, 2019</p> <p>UN SROs (Security Council) Act 1948</p>	Yes	Yes

- Cover targeted financial sanctions (TFS) for TF and PF		
Ministry of Interior / National Counter Terrorism Authority (NACTA) Proscribed Organizations under ATA	Yes	Yes
- Covers targeted financial sanctions (TFS) for TF		
AML / CFT Sanctions Rules	Yes	Yes
Counter Measures for High Risk Jurisdiction Rules	Yes	Yes

35. As mentioned at the beginning to the Guidelines, for ease of reference, the laws and regulations applicable to accountants will be generically referred to as “AML / CFT legislations”, unless there is a need to reference a specific law or regulation.

36. For a copy of the actual laws, regulations and guidelines, visit the websites of the following competent authorities or SRBs. Links to other important AML / CFT legislations are also provided below:

1. <http://AMLA amended September 2020.pdf>
2. <https://AML / CFT Regulations for ICAP Reporting firms.pdf>
3. <https://AML / CFT Regulations for ICMA Reporting firms.pdf>
4. <http:FBR AML / CFT Regulations for DNFBPs.pdf>
5. <https://AML-CFT-Sanction-Rules-2020-SRO-NO-950I-2020.pdf>
6. <http://mofa.gov.pk/unsc-sanctions/>
7. <https://nacta.gov.pk/proscribed-organizations/>
8. <https://nacta.gov.pk/pp/>
9. <https://nfs.punjab.gov.pk/>
10. <http://www.secdiv.gov.pk/page/sro-unscr-sanctions>

37. **Appendix A** provides a list of useful web links to other AML / CFT legislation and guidance documents.

3.2 Government authorities responsible for accountants

38. As mentioned, Pakistan’s three designated AML / CFT supervisors of accountants are the two SRBs (i.e. ICAP and ICMA PAKISTAN) and FBR. The two SRBs were designated under Ministry of Finance SRO 952(I)/2020 dated 1 October 2020 pursuant to Section 6C and Section 2(xxiv) of the AMLA.

39. Who is your AML / CFT supervisor depends on your membership of the accountancy body, which could be more than one. If you are neither a member of two SRBs, and membership is with another professional accountancy body, then your AML / CFT supervisor is FBR.

40. The Council of each of the two SRBs established an AML Supervisory Board which is supported by the AML Supervision Department. The AML Supervisory Board is responsible for supervising, regulating, implementing and enforcing the AML / CFT legislations. It is also responsible for performing other functions as are necessary for this purpose and may be delegated to it by the Council.

41. The FBR is mandated under the AMLA for ensuring (DNFBPs) including FBR-supervised accountants to comply with AML / CFT obligations.

- 42.** The FMU is the Financial Intelligence Unit of Pakistan. It is mandated to receive and analyse STRs and CTRs. All reporting firms must submit STRs and CTRs to the FMU.
- 43.** The Ministry of Foreign Affairs (MoFA) is responsible for issuing SROs relating to TF and PF. These resolutions are implemented in Pakistan through the United Nations (Security Council) Act, 1948. Under this Act, the Ministry of Foreign Affairs issues SROs to give legal effect in Pakistan to these decisions of the Security Council.
- 44.** The Ministry of Interior/NACTA issues Proscribed Organizations and Persons under the ATA for domestic designations on terrorism and TF.
- 45.** The Securities and Exchange Commission of Pakistan (SECP) is the supervisory body for the two SRBs as per the Ministry of Finance SRO. 952(I)/2020 dated 1 October 2020 pursuant to Article 6C of the AMLA. The SECP does not supervise accountants directly, but does supervise the SRBs for compliance with AML / CFT legislations.

4. SPECIFIED SERVICES SUBJECT TO AML / CFT

46. Not all services provided by accountants are subject to AML / CFT requirements. The specified services subject to AML / CFT requirements are clearly stated in Section (2) (xii) (c) (d) of the AMLA.

4.1 Specified services subject to AML / CFT

47. The following flowchart provides an easy guide on whether your firm provides specified services captured by AML / CFT legislations.

Is your firm providing the following services?	
<p>Accountant – means sole practitioners, partners or employed professionals within professional firms when they prepare for or carry out transactions for their client concerning the following activities:</p> <p>Accountancy services - when carryout monetary transactions for their customers concerning the following activities:</p> <p>(I) managing, operating, buying and selling of real estate, legal persons and legal arrangements and preparing documents therefore;</p> <p>(II) managing of client money, securities or other assets;</p> <p>(III) managing bank, savings or securities accounts; or</p> <p>(IV) organizing contributions for the creation, operation or management of companies</p> <p>Trust and company formation services - when they carry out monetary transactions or services for a client concerning the following activities:</p> <p>(I) acting as a formation agent of legal persons;</p> <p>(II) 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;</p> <p>(III) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;</p> <p>(IV) 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</p> <p>(V) acting as or arranging for another person to act as a nominee shareholder for another person.</p>	
YES	NO
You are <u>in scope</u> of the AMLA and the SRB and FBR AML / CFT regulations	You are <u>NOT in scope</u> of the AMLA and the SRB and FBR AML / CFT regulations

48. Essentially whether your firm is captured by the AMLA and AML / CFT Regulations for Reporting firms or the FBR AML / CFT Regulations for DNFBPs is based on services provided.

49. Your reporting firm is subject to the AML / CFT legislations if it provides any of the specified services, regardless of whether or not any fee is charged to the customer or a formal letter of engagement has been obtained. In other words, even if a reporting firm carries out these activities on a volunteer basis, it would be subject to the AML / CFT requirements detailed in AML / CFT legislations.

50. For the purpose of the Guidelines, specified services include any service provided under a contract for services (i.e. not a contract of employment).

4.2 Auditing, other assurance services, internal accounting and book keeping services

51. Based on the above-specified services, the activities of a firm such as audit of financial statements carried out according to the International Standards on Auditing (ISAs), as applicable in Pakistan or tax consultancy services are not subject to the measures e.g. CDD in the AML / CFT legislations.

52. The term “Accountants” is not meant to 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

53. If the firm is only providing book keeping services, it is not subject to the measures in the SRB AML / CFT Regulations for Reporting Firms and the FBR AML / CFT Regulations for DNFBPs as it does not control the funds of the customer.

4.3 Common examples of ‘specified services’

54. Some of the common examples of the specified services or activities could be:

1. Acting as a formation agent for legal persons or legal arrangements.
<p>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.</p> <p>The service does not include instances where the reporting firm provides advice, including referring the customer to a third party e.g. lawyer for more detailed advice. In the case of forming a company, if customer asks a lawyer to register the company or registers the company based on the advice by the practicing firm, the specified service would be undertaken by the lawyer (or by the customer) and the lawyer would have to apply their AML / CFT compliance programme to that service.</p> <p>The filing of Statutory Forms / Annual Returns is a regulatory requirement under the provisions of the Companies Act, 2017, therefore, it is NOT a specified service subject to AML / CFT.</p>
<p>Examples of this kind of captured service in practice</p> <ul style="list-style-type: none"> - Incorporation / Registration of a company with the SECP on behalf of a customer. - Incorporation of an entity (partnership/firm/society/company etc.) on behalf of a customer.
<p>ML / TF risks associated with this activity</p> <p>When a reporting firm 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. This obscures the beneficial owner(s). Further, international evidence shows that people use charitable organisations (such as incorporated societies and charitable trusts) to finance terrorism.</p>
2. Acting as a nominee director, shareholder or trustee.
<p>The reporting firm is engaged to act as a nominee director or shareholder for a company, or as a trustee of a trust.</p> <p>This is a specified service subject to AML / CFT.</p> <p>Where the firm has only assisted the company / partnership in appointment of 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 as a specified service subject to AML / CFT.</p>
<p>Examples of this kind of captured service in practice</p>

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

3. Managing customer funds, accounts, securities, or other assets

The reporting firm 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 firm receives or holds customer funds and controls the payment of those funds will also be a specified service and subject to AML / CFT.

The key determining factor is whether the reporting firm has control over the flow of funds (if it has the control then the activity is specified service).

Taking a payroll situation, for example, if the reporting firm is preparing the vouchers or uploading the payments in the system that are then actioned by the customer, in such a case the reporting firm is not controlling the funds, rather the customer is.

However, if the reporting firm 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

- The reporting firm has the authority to make payments on behalf of its customer’s business directly from customer’s bank accounts.
- The reporting firm 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 firm manages the sale and/or purchase of trust assets for the customer using funds from the customer’s bank accounts which the reporting Firm has the authority to transfer.
- The reporting firm 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.

4. Providing a registered office, business address or accommodation

A reporting firm 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

A company wants to use the address of the reporting firm 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.

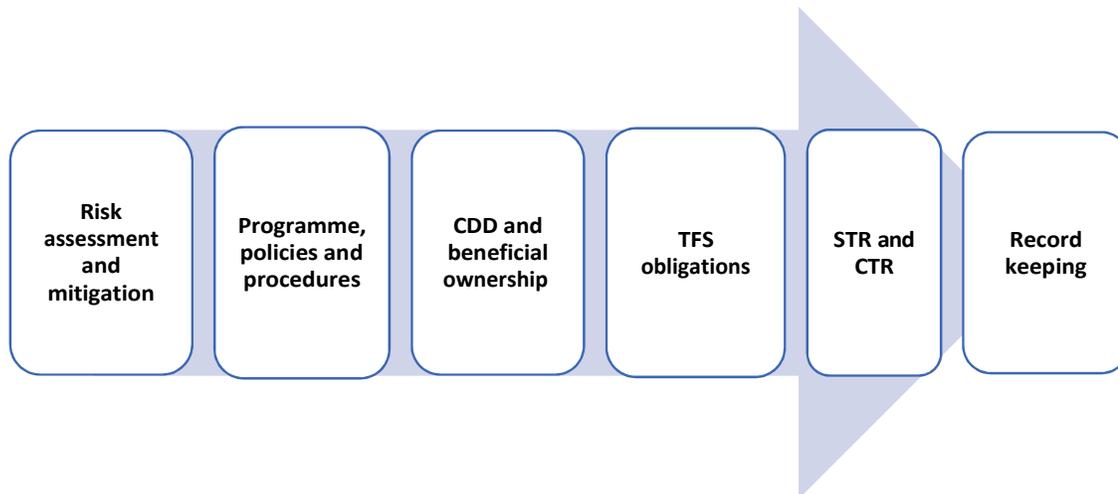
ML / TF risks associated with this activity

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 firm, 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.

55. 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.

56. If your reporting firm is captured, the key requirements and how to implement those requirements are detailed in the remainder of the Guidelines. The following is an overview of the requirements:



4.4 Support and guidance on AML / CFT

57. If, after considering the AML / CFT legislations and the Guidelines, a member of the SRB (either the ICMA PAKISTAN or ICAP) or non-member is unsure as to whether they are a reporting firm, they should contact their SRB, FBR or FMU and/or seek independent professional advice.

58. Where employees of the reporting firm have compliance questions, their first reference point should be the reporting firm’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.

59. Specific questions should be answered by the firm’s designated compliance officer or senior management.

60. The reporting firms can access support from a range of sources:

- Your professional accountancy body / SRB
- FBR
- FMU as the Financial Intelligence Unit
- Ministry of Foreign Affairs
- Ministry of Interior
- Independent professional advice from legal counsel
- AML / CFT consultants
- Open source information from relevant international bodies concerned with AML / CFT

61. The Guidelines are not the only source of guidance and information on ML / TF that can be referred. The reporting firms are reminded that other guidance issued by the FBR, FMU, SECP, SBP, NACTA and affiliates of the same corporate group (e.g. international accounting firm) that may also be relevant and useful.

62. **Appendix A** to the Guidelines contains a list of some useful and relevant web links.

5. RISK ASSESSMENT AND RISK MITIGATION

63. The purpose of the enterprise risk assessment for your reporting firm is to identify which customers, geographic regions, services and channel of delivery that are higher or lower risk for ML / TF, and to focus more attention on the higher risk areas. In other words, a risk based approach (RBA).

64. Section 5 of the Guidelines is focused on risk identification and assessment, while the subsequent sections are focused on the actual AML / CFT programme on risk management and mitigation. Because they are closely intertwined, it is matter of focus rather than exclusivity.

5.1 Statutory requirements under AML / CFT legislations

AML A: Section 7F requires reporting firms undertake an enterprise risk assessment for ML / TF.

SRB AML / CFT Regulations for Reporting Firms: Section 4 refers to the requirement in the AML A that reporting firms must identify, assess and understand their risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels).

Section also states that reporting firms must:

- (a) document their risk assessments;
- (b) consider 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) keep these assessments up to date; and
- (d) have appropriate mechanisms to provide risk assessment information to their SRB.

FBR AML / CFT Regulations for DNFBPs: With the exception of the name of the supervisor, Section 4 has identical requirements as above, and refers to Section 7F of the AML A.

5.2 Sanctions for non-compliance

AML A: Section 7I of AML A provides that a regulator may impose monetary and administrative penalties for violations of Section 7F.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by ICAP/ICMA PAKISTAN according to Clause (h) of Sub-section (2) of Section 6A of the AML A.

FBR AML / CFT Regulations for DNFBPs: Section 16 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under AML A.

AML / CFT Sanction Rules: Section 3 provides the powers for the SRB to sanction REAs for non-compliance pursuant to Section 7 of the AML A, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

5.3 ML / TF enterprise wide risk assessment

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

66. The enterprise risk assessment should be approved by the reporting firm’s senior management which is defined in Section 3. (1) Definitions in the SRB AML / CFT Regulations for Reporting Firms and Section 2. Definitions in the FBR AML / CFT Regulations for DNFBPs. Both definitions are very similar in scope. The risk assessment should, therefore, also include proposed mitigation measures needed, including AML / CFT controls and procedures identified by the risk assessment (refer to Section 6 of the Guidelines).

67. The ML / TF enterprise risk assessment is not a one-time exercise and must be kept up to date. The AMLA, AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFBPs are silent on the frequency of risk assessment updates, but based on international practices, it should be reviewed and updated at least once every two years, or when there are material or significant changes in specified services provided by the reporting firm.

68. The enterprise risk assessment is separate to a customer risk assessment; the latter must be completed before a new customer is accepted, and the risk rating reviewed and updated, if necessary, under ongoing CDD (refer to Section 7 of the Guidelines).

5.4 Difference between an inherent and residual enterprise risk assessment

An inherent risk assessment represents your reporting firm’s exposure to ML and TF risks in the absence of any mitigation measures, namely no AML / CFT procedures or controls. A residual risk assessment is undertaken after the mitigating effects of AML / CFT controls have been accounted for. While not explicitly stated in the AML / CFT legislations, the expectation is a residual risk assessment is undertaken.

69. It is important to note that the primary purpose and benefits of an enterprise risk assessment is to identify the weak spots in your reporting firm that may be abused by criminals or terrorists. So the initial focus is on identifying your inherent risks and taking appropriate mitigation measures. Once the mitigation measures have been applied, then an updated enterprise risk assessment will enable the reporting firm to focus more on the remaining vulnerable areas, where despite mitigation measures, they remain vulnerable. This could be in areas where there has been poor implementation of CDD measures for certain categories of customers.

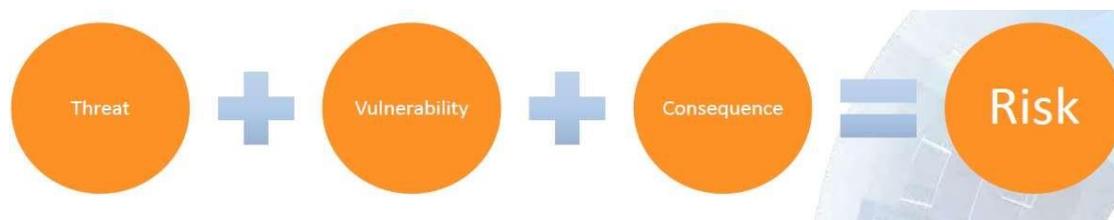
5.5 How to conduct the enterprise risk assessment on ML / TF

70. When conducting your enterprise risk assessment, you do not have to follow the processes in the Guidelines. As long as you comply with your obligations under the AML / CFT legislations, you can choose the method of risk assessment that best suits your reporting firm.

71. The following explains the key steps in conducting an enterprise wide risk assessment i.e. understand the meaning of ML / TF risk, identify the risk categories and then assess the risk, including quantitative and qualitative information collection.

(i) Step 1 – What is ML / TF risk

72. It is commonly accepted that risk is a function of three factors - threat, vulnerability and consequence, as shown below:



73. Threat: A threat is a person or group of people with the potential to cause harm by ML or TF.

74. Vulnerability: A vulnerability comprises those things that can be exploited by the threat or that may support or facilitate its activities.

75. Consequence: A consequence refers to the impact or harm that a threat may cause if eventuated. When determining impact of ML / TF, the reporting firm may consider a number of factors, including:

- (a) Nature and size of your business (domestic and international);
- (b) Potential criminal, financial and reputational consequences;
- (c) Terrorism-related impacts;
- (d) Wider criminal activity and social harm;
- (e) Political impact;
- (f) Negative media.

(ii) Step 2 – Identify the risks

76. Section 4 in both the AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFBPs specifies the following four mandatory risk categories:

- Customer risk
- Countries or geographic risk (internal and overseas)
- Products services risk ((including technology)
- Transaction or delivery channel risk ((including technology)

77. Weighting: The above risk categories may be weighted, or you may decide to assign equal weighting to each e.g. 25%. It depends on the nature of your business. For example, if you have no international exposure and based in a location in Pakistan that is not higher risk, then geographic risk may not be a significant risk category for your risk assessment. The converse may be true if your reporting firm has significant international exposure.

78. Other risk categories: When conducting your reporting firm’s ML / TF enterprise risk assessment, the risk categories need not be limited to the above categories, but the risk assessment must cover the above four risk categories. Your risk assessment could include other qualitative risk categories, such as the institutions your reporting firm deals with e.g. lawyers, real estate agents, money remitters etc.

79. Business lines: While not explicitly stated in the AML / CFT legislations, the enterprise risk assessment should identify the risk categories in the context of nature of the reporting firm’s business activities i.e. which business lines (e.g. that generate revenue through professional fees) deliver the specified services subject to AML / CFT, and/or have greater exposure to customer, geographic, products and services, and their delivery channel risks?

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

Risk Indicators

1. 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 summarised 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 (refer to Section on Risk Based CDD for more customer indicators);
- **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 firms 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** (e.g. travellers' cheques and electronic money purses) e.g. 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** e.g. higher value may indicate higher risk (refer to sub-section on source of wealth and funds in Section 7 on Risk Based CDD);
- **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.

2. Geographic risk

This risk category may be considered both a threat and vulnerability. A reporting firm 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
- prevalence of bribery and corruption
- association with terrorism and TF

Information on the above should be based on credible sources.

The “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: <http://www.fatf-High risk and other monitored jurisdictions>)
- FATF-style regional bodies e.g. APG
- FMU, FBR, SRBs (ICAP & ICMA PAKISTAN), SBP, MoFA and other Pakistan government agencies <https://nacta.gov.pk/proscribed-organizations/>
- Reporting firm’s experience or the experience of other group entities (where the reporting firm’s is part of a network) which may have indicated weaknesses in other jurisdictions
- Supra-national or international bodies such as the United Nations Security Council (<https://scsanctions.un.org/search/>), International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units
- Non-governmental organisations such as:
 - Basel AML Index (<https://www.baselgovernance.org/aml-index>)
 - Tax Justice Network (<https://fsi.taxjustice.net/en/>)
 - Transparency International: <https://www.transparency.org/en/cpi/2019/results>
 - Institute of Economics and Peace: <http://economicsandpeace.org/Global Terrorism Index>

3. Product and services risk (including technology risk)

The products and services your reporting firm offer are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF. A reporting firm 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 legislations. 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 firm 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?

4. 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; and
- 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?

(iii) Step 3 – Assess the risk

81. **Likelihood:** In order to assess the risk based on the equation i.e. Threat + Vulnerability + Consequence = Risk, there is an additional element that needs to be assessed, which is the likelihood of the event i.e. ML or TF. Likelihood could be (i) Almost certain (ii) Likely (iii) Unlikely and (iv) Possible.

82. The following are definitions for the different categories of likelihood:

- (i) **Almost certain:** There is a high probability of ML / TF occurring in this area of the business
- (ii) **Likely:** There is a medium probability of ML / TF occurring in this area of the business
- (iii) **Unlikely:** There is a low probability of ML / TF occurring in this area of the business
- (iv) **Possible:** There is a minuscule probability of ML / TF occurring in this area of the business.

83. When assessing the ML / TF risk, the following matrix, which is commonly refer to as a “heat map”, with Likelihood and Consequence scenarios provides a more structured approach.

Money laundering and terrorism financing risk matrix				
Likelihood	Almost Certain	Medium	High	High
	Likely	Low	Medium	High Customer 3
	Unlikely	Low Customer 1	Medium Customer 2	High
	Possible	Low	Medium	Medium
		Minor	Moderate	Significant
Magnitude of Consequence				
Risk Rating		Low	Medium	High

84. To understand how to apply this concept, the following three examples are provided:

- i. **Customer 1** is a government agency whom your reporting firm is providing payroll services. In this scenario, it is possible but highly unlikely the government agency would engage in ML. The consequence may be minor because of it is only payroll services for a government agency. The inherent risk is therefore low (*refer to above matrix*).
- ii. **Customer 2** is a well-known company in educational services whom your reporting firm is also providing payroll services and regular payments to two contractors for building maintenance for the last 10 years. In this scenario, it is unlikely that such a company would try to launder funds. The consequence may still be moderate, as it would damage the reputation of the reporting firm, and the business may be fined by the SRB. The inherent risk is therefore medium (*refer to above matrix*).
- iii. **Customer 3** is a politically exposed person who has been alleged to be engaged in corruption whom your reporting firm is providing nominee director services. The likelihood that he/she may be engaged in ML is likely - highly probable. The consequence is significant because of the negative reputational damage (e.g. extensive media coverage) and possible severe penalties – because the firm is providing higher risk services knowing that the customer is a PEP. The inherent risk is therefore high (*refer to above matrix*).

85. For the enterprise risk assessment, the reporting firm does not need to risk rate each individual customer. You may group customers with similar characteristics or risks.

5.6 Quantitative and qualitative information for enterprise risk assessment

86. Information needed for an enterprise risk assessment may be collected from various sources, as summarised below:

- (i) **Internal Information:** The reporting firm’s own information about the practice – how many business lines, locations, main services, how many accountants providing specified services, customers groups, technologies used etc.

Information from within the reporting firm 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 information needed. It is unlikely to obtain all the required information, but should be sufficient for informed conclusions to be made.

- (ii) **Pakistan’s National Risk Assessment:** This report contains information on the ML and TF threat environment in Pakistan including high risk activities and sectors.

The reporting firm should take account of the findings of the latest National Risk Assessment to inform your enterprise risk assessment of the ML and TF threat environment, and including high risk activities and sectors. The National Risk Assessment is not publicly available, so your reporting firm will need to obtain a copy of the National Risk Assessment from your AML / CFT supervisor or the FMU.

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

- (iv) **International and NGO:**

- FATF (FATF: http://www.fatf-High_risk_and_other_monitored_jurisdictions) and FATF-style regional bodies
- Supra-national or international bodies such as the United Nations Security Council (<https://scsanctions.un.org/search/>), International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units
- Non-governmental organisations such as Transparency International, Basel AML Index (<https://www.baselgovernance.org/aml-index>) and Tax Justice Network (<https://fsi.taxjustice.net/en/>).

5.7 Example of an enterprise risk assessment template

87. The example below of a small reporting firm combines the enterprise risk assessment and risk mitigation in a simple template. Depending on the complexity and size of your reporting firm, your risk assessment template and risk mitigation measures may be more comprehensive. The example template illustrates the benefits of adopting a matrix approach. The focus is on inherent risks.

Case Study: Small Reporting Firm
<p>The example template has been populated using the following case study.</p> <p>Case Study: Medium Sized Reporting Firm</p> <p>Your accountancy practice has 130 active customers. There are three partners and 10 staff, so a total of 13. The firm has one office in Karachi.</p> <p>The firm provides following specified services on a regular and on an ad hoc basis:</p> <ul style="list-style-type: none">• Regular services:<ul style="list-style-type: none">- Auditing services and bookkeeping services (Out of scope as not specified services)- managing of customer money, securities or other assets; and- managing of bank, savings or securities accounts;

Ad hoc and occasional:

- creating, operating or managing companies;
- creating, operating or management of legal persons or arrangements, and buying and selling of business entities.
-

Your firm accepts cash and cheque payment for services, but most payments of services are to your firm’s bank account. They do involve international wire transfers to, and from overseas.

You have a handful of expatriate customers based overseas in FATF member countries with excellent FATT assessment reports.

With the exception of the handful of overseas based customers, your firm normally has face-to-face meeting with customers based in Karachi.

Enterprise Risk Assessment Template with mitigation measures

Customer - types of customers we deal with (only customers receiving specified service - refer to tables on customer risk factors)	Are any of my firm’s customers a higher or lower threat for ML / TF?	Likelihood rating of ML/FT (refer table)	Consequence rating of ML / TF - minor, moderate, significant, severe (refer table)	ML / TF Risk level High, Medium, or Low (refer table)	Risk Mitigation Measures
1. Five local government authorities	Yes, lower risk	Unlikely	Minor	Low	Simplified CDD
2. 70 small businesses – family run – sole trader or simple company structure (about 25 customers)	Overall, medium risk. Businesses are not in higher risk sector, and while accept cash payments – is not cash intensive	Unlikely overall, although some may be higher risk	Minor / Moderate	Medium	Standard CDD
3. 10 Individuals based overseas in FATF countries who still owns family businesses in Pakistan – none in higher risk sectors	Standard risk because of geography	Unlikely	Moderate	Medium	Standard CDD
4. Some professionals such as doctors and lawyers.	One or two may be related to PEPs	Likely	Significant	High	Enhanced CDD
5. 25 small businesses – restaurant, jewellery, real estate	Higher risk business and sectors – cash intensive.	Likely	Significant	High	Enhanced CDD
6. A few customers being audited by FBR	Yes, as source of funds not totally clear, and agent for	Likely	Moderate	Standard	Review transactions

	tax returns – however only taxation returns services provided				
Geographic locations/ countries or region we deal with	Is it considered higher risk? Why?	Likelihood rating of ML/FT	Consequence rating of ML / TF	Risk level High, Medium, or Low	Risk Mitigation Measures
1. Customers in FATF member country	No	Unlikely	Moderate	Medium	Standard CDD
2. Managing payments for customers based overseas	Yes as international funds transfers overseas	Likely	Moderate/ Significant	High	Enhanced CDD on source of funds Transaction monitoring Specialised training for accountants on account monitoring Regular reviews of transactions
Services/Products Risk - types of products and services we offer	Are my services/ product at higher risk of abuse?	Likelihood rating of ML/FT	Consequence rating of ML / TF	Risk level High, Medium, or Low	Risk Mitigation Measures
1. Accept cash payments	Yes, higher risk based on indicators	Likely	Significant	High	Adopt policy of no cash payments or impose threshold Transaction monitoring Enhanced CDD
2. Managing bank accounts and domestic and international payments to 3 rd parties – multiple countries – some higher risk	Yes, as risk of abuse for ML or TF	Likely	Significant	High	Enhanced CDD on source of funds Transaction monitoring Specialised training for accountants on account monitoring Regular reviews of transactions
3. Occasionally assisting in opening companies for new and existing customers	No – simple company structure with one or two individual owners who are the directors	Unlikely	Moderate	Medium	Standard CDD Specialised training for accountants on beneficial ownership and ML / TF risks

4. Due diligence in the purchase of a business	No, very rare, and only case the purchaser/customer is an established company in the same delivery business	Unlikely	Moderate	Medium	Standard CDD Reputational due diligence check on delivery service and customer
Delivery Channels - how we deliver our services	Are my delivery channels more vulnerable to potential abuse?	Likelihood rating of ML/FT	Consequence rating of ML / TF	Risk level High, Medium, or Low	Risk Mitigation Measures
1. Mostly face-to-face and via telephone and emails	No, standard risk	Unlikely / likely	Moderate	Medium	Standard CDD
2. Non face-to-face for some non-resident customers / counter parties	Yes, as they are also based overseas	Likely	Significant	High	Enhanced CDD Electronic verification Liveness test Regular account monitoring

88. The above example shows that overall, the ML / TF risk for this reporting firm is medium. However, it faces higher risk for customers that are complex companies and PEPs. There are also non customer specific higher risks, as the firm accepts cash and manages funds including overseas wire transfers with higher risk countries. Measures to mitigate these risks could include senior management approval prior agreeing to provide services, enhanced training of staff working with these customers, and regular scrutinising of transactions and CDD documentation to ensure procedures are followed.

89. Once those risk mitigation measures have been applied, your reporting firm may review and update the risk assessment to identify the residual risk, which prior to the application of risk mitigation measures are identical to inherent risks. The same template can be used by adding another column on the right side of the template to reflect the residual risk rating. This should only be completed after the mitigation measures have been applied.

90. Reporting firms may consider using or amending this case study template for its own ML / TF enterprise risk assessment. Depending on the complexity and size of your reporting firm, your risk assessment template and risk mitigation measures may be more or less comprehensive.

6. AML / CFT Programme, Policies and Procedures

91. Your reporting firm needs to develop its own comprehensive risk-based AML / CFT compliance programme to comply with the AML / CFT legislations. The basis for this risk based programme, as discussed in the preceding section, is the ML / TF enterprise risk assessment.

6.1 Statutory requirements under AML / CFT legislations

AMLA: Under Sections 7G-H, reporting firms must have a compliance programme and have AML / CFT policies and procedures. A compliance programme includes the appointment of a compliance officer at a management level and staff training.

SRB AML / CFT Regulations for Reporting Firms:

Section 5: The reporting firm shall:

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

Section 6 states the reporting firm may take simplified measures to manage and mitigate risks, if lower ML / TF risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ML / TF.

Section 27. (1) In order to implement compliance programs as set out in 7G of the AMLA, the reporting firm shall implement the following internal policies, procedures and controls:

- (a) compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the reporting firm's compliance with these Regulations;
- (b) screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;
- (c) an ongoing employee training program.

Section 28. The reporting firm shall ensure that its foreign branches apply AML & CFT measures consistent with Pakistan requirements where the minimum AML & CFT requirements are less strict than Pakistan, to the extent of that host country laws. If the foreign country does not permit the proper implementation of AML / CFT measures consistent with that of Pakistan requirements, reporting firm should apply appropriate additional measures to manage the risks, and inform their SRB.

FBR AML / CFT Regulations for DNFBPs: With the exception of the name of the supervisor and reference to regulated person instead of reporting firm, Section 4 (2) on risk based approach is identical to the requirements as above Sections 5 and 6. Section 7 on compliance programs has all the requirements in Sections 27 and 28, and includes more explicit the need for an independent audit function to test the system in Section 7 (d), in 7 (3) clear terms of reference for the compliance officer in Section 7 (a), and in 7 (4) clear requirements on group compliance if part of a corporate group, including safeguards for the confidentiality on the use of information exchanged within the group.

6.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator may impose monetary and administrative penalties for violations of Section 7G and H.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by ICAP/ ICMA Pakistan according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under AMLA.

AML / CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction REAs for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

6.3 Role of senior management

92. The reporting firm's senior management (e.g. sole proprietor, chief executive officer, chief operating officer, managing partner or partner) must be engaged in decision making on AML / CFT policies, procedures and controls, and take ownership of its risk-based compliance programme. Strong leadership and engagement by senior management and the reporting firm's staff in AML / CFT are important for successful implementation.

93. Senior management must encourage a culture of compliance. It must ensure that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

94. Senior management should ensure sufficient resources are devoted to the implementation of the reporting firm's AML / CFT compliance programme. This requires the building of expertise including for example, 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.

6.4 Compliance officer

95. There must be a person designated as the AML / CFT compliance officer as required under Section 27 of AML / CFT Regulations for Reporting Firms and Section 7 of the FBR AML / CFT Regulations for DNFBPs. The compliance officer must be at a management level in the reporting firm. He / she is responsible for effectively implementing all of the elements policies and procedures; CDD, record keeping, ongoing training, risk assessment and monitoring the effectiveness, reporting to senior management and reporting to FMU.

96. Depending on the size of reporting firm, 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

97. 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 firm, irrespective of the employment conditions e.g. permanent or contractual.

Compliance Officer’s Terms of Reference

In order to implement an effective AML / CFT programme the compliance officer should:

- a) report directly to the chief executive officer, the senior partner or the AML Designated Partner of the reporting firm;
- b) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;
- c) be responsible for the areas including, but not limited to:
 - (i) ensuring that the internal policies, procedures and controls for the prevention of ML / TF are approved by the board of directors or senior management and are effectively implemented;
 - (ii) monitoring, reviewing and updating AML / CFT policies and procedures;
 - (iii) providing assistance in compliance to other departments and branches of the reporting firm;
 - (iv) timely submission of accurate data / returns as required under the applicable laws;
 - (v) monitoring and timely reporting of STR and CTR to the FMU; and
 - (vi) such other responsibilities as the reporting firm may deem necessary in order to ensure compliance with the AML / CFT legislations.

(Refer Section 7 (3) FBR AML / CFT Regulations for DNFBPs.)

A compliance officer may choose to delegate certain duties to other employees. However, where such a delegation is made, the compliance officer remains responsible for the implementation of the compliance programme.

6.5 Written policies and procedures

98. An AML / CFT programme must set out the written internal policies, procedures and controls to detect ML and TF, and to manage and mitigate the risks of occurrence as required in Section 5 of SRB AML / CFT Regulations for Reporting Firms and Section 4 (2) of the FBR AML / CFT Regulations for DNFBPs. These must be approved by senior management.

99. The written AML / CFT procedures should cover the following to comply with the requirements of the AML / CFT legislations:

AML / CFT PROCEDURES OF REPORTING FIRM

Table of Contents

- a) Enterprise Risk Assessment
- b) Technology Risk Assessment
- c) AML / CFT programme, policies and procedures
- d) Compliance Officer,
- e) Staff vetting and training
- f) Customer due diligence (CDD)
 - Identify and verify customers (and person acting on behalf)
 - Identify and verify beneficial owners
 - Risk rating customers – high, medium or low
 - Simplified, standard or enhanced customer due diligence
 - Delayed verification
 - Customer rejection
 - CDD and tipping off

- | |
|---|
| <ul style="list-style-type: none">– Politically Exposed Persons (PEPs)– Reliance on third partiesg) Ongoing CDD, including business relationship monitoringh) Targeted financial sanctions monitoringi) Suspicious transaction report (STR) and currency transaction report (CTR) to FMUj) Record keepingk) Independent audit |
|---|

100. The reporting firm has a certain amount of discretion to decide on how to implement policies, procedures and controls that are suitable for your business. But such policies, procedures and controls need to be adequate and effective.

Maintenance and distribution of AML / CFT procedures

101. The adopted procedures must be clearly dated to allow for easier identification by staff of any subsequent changes. Ideally, the adopted procedures should be made available via the reporting firm's intranet, if one is available, if not via email distribution. Any changes to the procedures should be communicated to all staff, and reflected in the AML / CFT training.

6.6 Group compliance

102. If your reporting firm has branches / offices, or subsidiary undertakings, either in Pakistan or overseas, there should be a group AML / CFT policy and procedures i.e. group compliance in accordance with either Section 27 of AML / CFT Regulations for Reporting Firms and Section 7.4-5 of the FBR AML / CFT Regulations for DNFBPs. This includes a head compliance officer, if there are compliance officers for each branch or subsidiary. The monitoring and review, including independent audit of the AML / CFT programme should be conducted at a group level. There should also be safeguards for the confidentiality on the use of information exchanged within the group.

103. For any branches / offices and subsidiary undertakings that carry on the same business as the practice in a place outside of Pakistan, they must have procedures in place to comply with CDD and ML / TF risk management, and group level information sharing, to the extent permitted by the law of that location.

6.7 Staff vetting and employment

104. Reporting firms must have adequate screening procedures in place to ensure high standards when hiring employees, as required under Section 27 (1) (b) of the AML / CFT Regulations for Reporting Firms and Section 7 (1) (b) of the FBR AML / CFT Regulations for DNFBPs. If your reporting firm already has adequate and effective procedures in place for staff vetting that are also suitable for AML / CFT purposes, your firm could include them in your AML / CFT programme and procedures. Suggested employee onboarding requirements could include:

- How vetting is differentiated for senior managers, compliance officer and customer – facing roles
- How vetting is applied when people change roles
- How vetting is applied to temporary staff and / or contractors
- Event – triggered vetting (e.g. adverse media or report about a staff member)

105. Assessment may include written references from previous employers, character statements from people of good standing in the community (e.g. religious figure, medical practitioner, police officer) or an internet search for key staff positions such as the compliance officer. For new graduates, a reference letter from a university lecturer, university society or from a person of good standing in the community.

106. While not explicitly stated in the AML / CFT legislations, the employment conditions of staff of your reporting firm should include the requirement to comply with AML / CFT legislations and the reporting firm's AML / CFT procedures, adding that repeated violations may result in a reduction in remuneration or employment termination.

6.8 AML / CFT training

107. The reporting firm must provide its staff with AML / CFT training as required under Section 27 (1) (c) of the AML / CFT Regulations for Reporting Firms and Section 7 (1) (c) of the FBR AML / CFT Regulations for DNFBPs. Staff training is an important element of an effective system to prevent and detect ML / TF activities. The effective implementation of even a well – designed internal control system can be compromised if staff members using the system are not adequately trained.

108. All partners and staff (those who interact with customers, handle funds or otherwise assist with compliance) should be made aware of AML / CFT legislations and are trained regularly (e.g. annually) to recognise and deal with transactions / events / circumstances, which may be related to ML / TF, as well as to identify and report anything that gives grounds for suspicion.

Training content

109. Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them.

110. For many in your reporting firm, knowledge of CDD requirements will be critical when staff interact with new and existing customers.

111. The programme itself should include how to determine if the customer is low risk or high risk, to decide whether to apply simplified CDD, standard CDD or enhanced CDD:

- What are the firm's internal policies / procedures on AML / CFT?
- When to do customer due diligence (CDD)?
- How to identify and verify a customer's identity?
- What to say when a customer does not want to produce identity documents?
- How to identify and verify beneficial ownership?
- What are targeted financial sanctions?
- How to identify and report suspicious transactions?
- What to do when an employee / organization encounters potentially suspicious activity?
- How to report suspicious transactions / activity on goAML?
- What records need to be kept?
- What penalties/ consequences might apply to the employees and the firm if they do not comply with AML / CFT legislations?

The compliance officer will need more specialised external training provided by professional providers, SRB, or by government authorities such as the FMU, FBR, SECP, ICAP / ICMA PAKISTAN.

Frequency of AML / CFT training

112. The AML / CFT legislations are silent on frequency of training, but they should include training 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.

113. Records should be kept showing who has received training, the training received and when 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.

6.9 Monitoring and review of AML / CFT programme

114. Your reporting firm must develop appropriate compliance management arrangements to monitor compliance with the firm's AML / CFT policy and procedures, as required under the AML / CFT legislations. It is important for the reporting firm through its compliance officer to undertake checks whether the AML / CFT procedures are being implemented, and whether there have been any violations. This could involve a sample of CDD documentation to ascertain whether all required information and documents had been collected.

115. Regular reviews, ideally on a monthly basis, or at least quarterly will identify gaps for rectification such as amending procedures, additional training or staff counselling or punishment. It is important to identify gaps earlier to minimise the problem and rectification work. The more the problem builds, the harder and more costly it will be to rectify.

6.10 Independent audit function

116. In addition to regular monitoring by the compliance officer, a regular independent testing of the adequacy and effectiveness of the AML / CFT policies, controls and procedures with the AML / CFT legislations is required under AML / CFT Legislations. The AML / CFT legislations are silent of the frequency of such an audit; ideally it should be conducted at least biennially.

117. The review could be undertaken by the reporting firm's business line that provide auditing services, as those services are not subject to the requirements of the SRB AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFbps. A reporting firm's compliance officer would not meet the independence test as that person would be actively involved in the implementation of the reporting firm's AML / CFT policies, procedures and controls. However, sole practitioners, who do not employ or manage staff would not be expected to carry out a particularly formal review, but would be expected to be able to demonstrate to the supervision team that they understand the concepts and requirements of AML compliance. The sole practitioner would, in effect, be the compliance officer and the auditor.

118. Further, this position does not necessarily have to be an in-house position – an external person could be engaged to do this independent audit. The independent audit should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.

119. If the independent audit identifies areas of weakness and makes recommendations on how to improve the reporting firm's AML / CFT policies and procedures, then senior management should monitor how the reporting firm is acting on those recommendations.

7. Risk Based Customer Due Diligence (CDD)

120. Risk based customer due diligence (CDD) is the engine room for effective implementation of AML / CFT. It may require a fundamental change in the reporting firm’s customer acceptance policy or a new engagement policy. While some aspects, such as obtaining the name and particulars of the customer are not new, other requirements such as verifying customer identity, identifying and verifying beneficial ownership, and sources of wealth or funds, may be new. They will add to the resources and time required before a new customer or new engagement is accepted i.e. business relationship is entered into.

121. The FATF Recommendations use the term customer and the AML / CFT legislation uses both terms. Firms typically refer to those benefiting from their services as clients rather than customers, but for the purposes of AML / CFT, the term customers is used also in the Guidelines and should be considered as synonymous with clients.

7.1 Statutory requirements under AML / CFT legislations

AMLA: Under Section 7A the AMLA, every reporting entity (including reporting firm) with regard to the specified services must conduct CDD including the circumstances where CDD is applicable and to identify and verify the identity and beneficial owner of the customer. Section 7B provides for reliance on third parties in conducting CDD. Section 7D requires CDD to be completed prior to providing the specified services or terminating the relationship if any. It also provides for ceasing the CDD process to avoid tipping off. Section 7E prohibits anonymous business relationships and transactions.

Relevant sub-section is reproduced as under:

*“Every reporting entity shall, in accordance with the regulations issued by relevant regulatory authority of that reporting entity, **conduct customer due diligence** and maintain record of transactions, account files and documents obtained through such diligence.”*

SRB AML / CFT Regulations for Reporting Firms:

Sections 8-16 sets out the mandatory CDD requirements on identifying and verifying the customer, beneficial owner and person purporting to act on behalf of the customer using reliable and independent documents, data or information.

Sections 17-18 provides for delayed verification subject to certain conditions, and only when the risks are low.

Sections 19-20 imposes ongoing due diligence on existing customers including scrutinising transactions and reviewing and keeping CDD records up to date, including on the basis of materiality and risks.

Section 21 states that the reporting firm must apply enhanced due diligence when there is a higher risk, called upon by the FATF for designated countries and for PEPs, including their close associates and family members.

Section 22 states that the reporting firm must apply counter measures when required on high risk countries.

Section 23 states that the reporting firm may apply simplified due diligence after lower risks have been identified through proper risk assessments, but not when there is suspicion of ML / TF.

Section 24 provides for reliance on a third party subject to certain conditions.

FBR AML / CFT Regulations for DNFBPs:

Section 8 (1) – (12) prescribe the mandatory CDD requirements on identifying and verifying the customer, beneficial owner and person purporting to act on behalf of the customer using reliable and independent documents, data or information.

Section 8 (13)-(14) provide for delayed verification subject to certain conditions.

Section 8 (15)-(16) impose ongoing due diligence on existing customers including scrutinising transactions and reviewing and keeping CDD records up to date, including on the basis of materiality and risks.

Section 9 (1) – (3) state that the reporting firm must apply enhanced due diligence when there is a higher risk, called upon by the FATF for designated countries and for PEPs, including their close associates and family members.

Section 10 states that the reporting firm may apply simplified due diligence after lower risks have been identified through proper risk assessments, but not when there is suspicion of ML / TF.

Section 11 states that the reporting firm must apply counter measures when required on high risk countries.

Section 12 provides for reliance on a third party subject to certain conditions.

7.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator may impose monetary and administrative penalties for violations of Sections 7A to 7H.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by ICAP/ ICMA Pakistan according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under AMLA.

AML / CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction REAs for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

7.3 Who to conduct CDD on

122. Your reporting firm must conduct CDD on:

- Your customer
- Any beneficial owner of your customer
- Any person acting on behalf of your customer.

Target of CDD	
Who do you must conduct CDD on?	Comment
Your customer	Means any person engaging a reporting firm for the purposes of requesting, acquiring, or using accountant or any services or carrying out any transaction or business with the reporting firm but only for specified services as explained in Section 4 of the Guidelines. • Reference: Definition in Section 3(c) of the SRB AML / CFT Regulations for Reporting Firms and Section 2(f) in the FBR AML / CFT Regulations for DNFBPs
Any beneficial owner of a customer	(a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or (b) natural person who exercises ultimate effective control over a legal person or legal arrangement; Reference: AMLA – Section 1. Definitions (iv). <i>(Refer to section 7.7 on Identifying and Verifying Beneficial Ownership below for more detailed explanation)</i>
Any person acting on behalf of a 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.

7.4 Timing of CDD

123. The timing of CDD must be undertaken in accordance with Section 7A of the AMLA, as shown in the table below.

Timing of CDD		
When is CDD required / When should CDD be completed	New Customer	Existing customer
	<p><i>Before commencing a business relationship</i></p> <p>The CDD process should commence after both parties have started discussion about potential services, but should be completed before the reporting firm has agreed to provide such services i.e. accepted the customer or new engagement.</p> <p><u>Identification</u> of a new customer must be completed before accepting the new customer.</p> <p><u>Delayed verification</u> is accepted in certain, very limited circumstances.</p>	<p><i>Notices a significant change in the nature of business relationship or the ownership and control structure of the customer's business.</i></p> <p>These will not be common, but in servicing an existing customer, the reporting firm may acquire knowledge that there is a new director requiring CDD, or a new beneficial owner, or a new company representative requiring CDD.</p> <p>The above could be identified when an existing customer seeks the services of the reporting firm for a new engagement (including migrating from a non-specified service e.g. auditing to a specified service e.g. managing bank account), or monitoring the transactions of an existing customer.</p> <p>For other existing customers where there are no changes, there is no fixed deadline for updating</p>

	<p><i>Definition of business relationship:</i></p> <p>“business relationship” means professional or commercial relationship between a reporting entity and a customer to conduct transaction, activity or to provide service or product.</p> <p>As noted, reporting firms are only subject to the SRB AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFBPs if they provide specified services.</p> <p>Reference. AMLA Section 2. Definitions (v).</p>	<p>CDD. Updating is based on your reporting firm’s assessment of the risk of existing customers. This review could be done annually or biennially, depending on your reporting firm’s resources and risk profile of your existing customers.</p> <p><i>Suspects money laundering or terrorist financing.</i></p> <p>Since, there are no occasional customers or transactions, this applies to existing customer. These includes existing customers before the AML / CFT requirements took effect.</p> <p>This could be triggered from scrutinizing transactions showing unusual transactions, or the income or transactions are no longer consistent with the reporting firm’s understanding of the customer’s business.</p> <p><i>Doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.</i></p> <p>It may be more applicable to existing customers i.e. persons that were already customers prior to the AMLA or AML / CFT regulations coming into effect so they were not subjected to the same level of due diligence.</p> <p>Or 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.</p> <p>The trigger could be when they return for another engagement and the reporting firm needs to collect and verify information on beneficial ownership which were not previously obtained.</p>
--	--	--

7.5 CDD components

124. The table below outlines the key foundations of the CDD process.

CDD components
1. Identify legal identity (name and date of birth or formation) and address
<p>The reporting firm must identify the legal identity of the customer – either individual, legal persons (companies or non-profit organisations) or legal arrangements (e.g. trusts).</p> <p>The reporting firm must also obtain either (i) date of birth and address of the natural person customer (ii) date of incorporation of the legal person customer or (iii) the date of trust formation.</p> <p>The address for all three categories should be a physical address.</p>

2. Verify legal identity (name and date of birth or formation) and address
<p>The reporting firm must verify the customer identity, including name and date of birth / formation and address using reliable and independent source documents, data or information.</p> <p><i>Refer to separate Table on acceptable verification documents in Section 7.6 of the Guidelines .</i></p>
3. Identify and verify beneficial ownership
<p>This is a significant new requirement associated with AML / CFT legislations.</p> <p>For the customer who is an individual, unless there are indication to the contrary, the person is considered both the legal and beneficial owner.</p> <p>For a non-complex company structure, the natural person director(s) may also be the beneficial owner(s), prima facie. 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.</p> <p>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 take reasonable measures to verify the beneficial owner.</p> <p>Please refer to <i>Section 7.7 Identifying and Verifying Beneficial Ownership</i> for a detailed explanation.</p>
4. Identify and verify any person acting on behalf of the customer
<p>The reporting firm 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.</p> <p>Examples of the person acting on behalf of a customer include:</p> <ul style="list-style-type: none"> • 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 <p>The requirements are the same in Steps 1-2 which is 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 firm must always identify and verify an individual or individuals.</p> <p>The reporting firm 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.</p>
5. Information on the purpose and the intended nature of the relationship
<p>The reporting firm must obtain information on the purpose and intended nature of the business relationship.</p> <p>In most instances, this will be self-evident when the customer approaches the reporting firm to seek accountancy services, and whether one off or ongoing. There are additional requirements in that the information must be documented, and if the customer is rated high risk, as more information will need to be collected.</p> <p>Unlike for identity, there is no requirement to verify the information.</p>
6. Establish or obtain information on the source of wealth or funds
<p>The AML / CFT legislations only state that the reporting firm must obtain information on the source of wealth or funds under enhanced CDD for higher risk customers. For PEPs, including their beneficial owners, family members and close associates, the reporting firm must take reasonable measures to establish the source of wealth and funds.</p>

For accountants, many of the professional services provided by accountants put them in a relatively good position to acquire this knowledge.

Please refer to Section 7.8 Sources of funds and Wealth for a detailed explanation.

7. Ongoing customer due diligence

The reporting firm 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.

This topic is also covered in the Table on Timing of CDD in Section 7.4 on Timing of CDD.

7.6 Customer verification documents, data or information

125. Section 15 of the SRB AML / CFT Regulations for Reporting Firms and Section 8 (11) of the FBR AML / CFT Regulations for DNFBPs list acceptable reliable and independent document, data or sources for verification of customer, beneficial owner and person acting on behalf of the customer. A list of acceptable documents is in the Table below (as extracted from the SRB and FBR AML / CFT regulations) and are consistent with those used by financial institutions.

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 persons 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

	<ul style="list-style-type: none"> (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
<p>5) Legal arrangements</p>	<ul style="list-style-type: none"> (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.
<p>6)NGOs/ NPOs/ Charities</p>	<ul style="list-style-type: none"> (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.
<p>7) Government institutions and entities</p>	<ul style="list-style-type: none"> (i) CNICs of the authorized persons; and (ii) letter of authorization from the concerned authority – for the individual authorised for act on behalf of the institution

Original: For purposes of verification, original documents need to be sighted, photocopied and attested (i.e. person verifying should mark 'original sighted' on the copy) by the reporting firm.

Certified true copy of document: Where the client is unable to produce original documents, the reporting firm may consider accepting documents that are certified to be true copies by an independent and qualified person (a notary public, or an external law firm).

The original of the certified true copy must be provided – 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 on-line 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 non-face-face and only email copies of documents are provided, in addition to the above mitigation measures, a live virtual meeting (video call) should be undertaken. However, a video call is not equivalent to electronic verification.

7.7 Identifying and verifying beneficial ownership

126. As noted, the definition of beneficial ownership in the AMLA is “*a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or (b) natural person who exercises ultimate effective control over a legal person or legal arrangement;*”

Reference: AMLA – Section 1. Definitions (iv).

127. The AML / CFT legislations state that the reporting firm must also identify the beneficial owners of the customer, and take reasonable measures to verify the identity of such persons using the relevant information or data obtained from reliable, independent sources. This may be a resource intensive and time consuming process, therefore in recognition of the challenges, the requirement is to take “reasonable measures”.

128. There is a legal definition of the term in the SRB AML / CFT Regulations for Reporting Firms, Section 3. Definitions - (1) (k) “Reasonable measures” means appropriate measures which are commensurate with the money laundering or terrorist financing risks; the reporting firm has to demonstrate it has taken reasonable measures. The definition is identical in the FBR AML / CFT Regulations for DNFBPs, Section 2.

129. The following sub-sections aims to:

- a) explain the concept of beneficial ownership for a customer that is an individual, legal person (e.g. company) and legal arrangements (e.g. trust); and
- b) how to identify and take reasonable measures to verify beneficial ownership for each of those categories of customers.

(i) Beneficial ownership is not legal ownership in all circumstances

130. The three key points to understand are:

- i. legal ownership is not synonymous with beneficial ownership. People tend to think the legal owners are the beneficial owners, and therefore do not differentiate between the two. In AML / CFT, the distinction is very important;
- ii. an individual can be an indirect owner of a company through another company in which the individual has ownership; and
- iii. the beneficial owner is always an individual who ultimately owns or controls a legal entity or arrangement, such as a company, a trust, a foundation, etc.

(ii) Natural persons

131. Normally, the legal ownership and beneficial ownership of the individual customer is the same. There may be circumstances where this is not the case. For example, a son / daughter opening an account to operate for their parents. The parents are the beneficial owners, while the children are the legal owners of the account. Therefore, unless there are reasons to doubt, the reporting firm may assume the individual customer is also the beneficial owner.

(iii) *Legal persons (e.g. company)*

132. The separation of beneficial ownership from legal ownership occurs more frequently with legal persons and arrangements e.g. companies and trusts. In many cases, the legal owner of the legal person is the beneficial owner, but not in all circumstances.

133. The Companies Act 2017 also provides a definition of beneficial ownership as stated in Section 123A, as follows:

“For the purpose of this section, the term “ultimate beneficial owner” means a natural person who ultimately owns or controls a company, whether directly or indirectly, through at least twenty-five percent shares or voting rights, or by exercising control in that company through other means, as may be specified.”

134. Importantly, it provides for 25% and above ownership, directly or indirectly, for the controlling ownership test which is further explained below.

135. Essentially there are three tests for identifying the beneficial owner of a company as provided in the AML / CFT legislations: controlling ownership test, control through other means test and senior management test. The three tests are a cascading process, to be used in succession when a previous test has been taken but has not resulted in the identification of the beneficial owner. They are explained in the Table below.

Identifying Beneficial Ownership for Legal Persons – Three Cascade Tests	
Limited Companies / Corporations	
<i>TEST 1: Identifying the beneficial owner through controlling legal ownership</i>	
<p>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.</p> <p>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.</p>	
<p>1. <i>Ownership threshold approach:</i></p> <p>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).</p>	<ul style="list-style-type: none"> – 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 123A of the Companies Act. – While 25% or more may be used for the controlling ownership test, If the 25% threshold does not identify any beneficial owners, or there are concerns or doubts that the 25% threshold has correctly identified all the beneficial owners, it is recommended that a lower threshold of 20% be used, and then 10%, if needed. <p>It is also important to highlight that this approach includes the notion of indirect ownership through a chain of companies.</p> <p>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.</p> <p>These concepts will be explained in the examples following this table.</p>

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

<p>2. Majority interest approach:</p> <p>Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity.</p>	<p>– For example, to appoint or remove the majority of the board of directors, or its chair, or CEO of the company.</p> <p>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.</p> <p>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.</p>
<p>3. Connections or contractual relations approach:</p> <p>Natural persons who may control the legal person through other means</p>	<p>– 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.</p> <p>– 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.</p>
<p>4. Company director’s position approach:</p> <p>The natural person(s) responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal person.</p>	<p>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.</p>

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.

<p>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</p>	<p>This is only permitted when the reporting firm cannot identify or verify the beneficial owner in limited circumstances, for example:</p> <ul style="list-style-type: none"> – Dispersed ownership; – Multiple layers of ownership, including in overseas secrecy jurisdiction, or bearer shares are permitted; <p>The senior management test. For, example, may include the chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president.</p>
--	--

	It is the natural person(s) who has significant authority over a legal person’s financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.
--	---

136. Before we provide examples of beneficial ownership, and how to identify and verify, a description of useful identification and verification documents is needed. The two documents are:

- (i) Register of Ultimate Beneficial Ownership Information by the Company, SECP Circulars No.16 and No. 20 of 2018, Section 123A of Companies Act; and
- (ii) Section 119 (XIX) of the Companies Act, 2017

137. Section 119 of the Companies Act should provide both legal and beneficial ownership in most cases where the company is owned only by individuals. The Register of Ultimate Beneficial Ownership should provide legal and beneficial ownership information in most cases where the company has at least one other company as an owner. However, the reporting firm cannot just rely on the register because it is only required where one or more legal persons / companies are members / shareholders of the company. If there is no legal person as a member / shareholder, the reporting firm will need to use Section 119 of the Companies Act.

138. Basically for simple company structures where individuals own the company directly, the reporting firm will need Section 119 (XIX) of the Companies Act. Where another company owns your customer (company), then the reporting firm will need the Register of Ultimate Beneficial Ownership. That register should identify beneficial ownership, even when that company (a shareholder of your customer) is owned by other companies through a chain of corporate ownership.

139. The Table below provides a summary of information in both documents.

Summary of information contained in the Register of Beneficial Ownership and Section 119		
	Register of Beneficial Ownership	Section 119 of the Companies Act
Applicability	All the companies having natural persons as ultimate beneficial owners (UBO) in that company through legal persons i.e. names and ID details of individuals	Every substantial shareholder (having not less than 10% interest), officer of the company or the company itself, having shareholding or other interest in a foreign company or body corporate
Represents	Ultimate Ownership of the company	Investment by substantial shareholders, officers or the company
Information to be maintained by the company	Yes	Yes
Information to be notified to the registrar or Commission	No, unless demanded	Yes
Information is publicly available	No	Yes
Penal provision for non-compliance	Yes	Yes

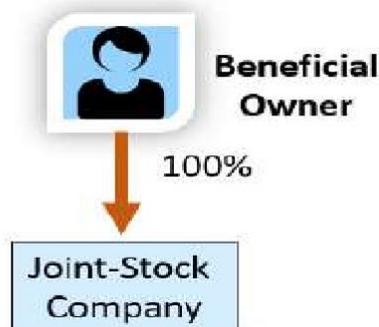
Source: SECP

140. We will use seven examples to show how to identify beneficial ownership using the three tests.

Example 1: Direct Ownership (Test 1: Identifying the beneficial owner through controlling legal ownership)

141. Example 1 below demonstrates a simple use of the ownership test to identify the beneficial owner, namely identify the person that owns 25% or more. In this example, there is one individual who is the sole shareholder (i.e. 100%). The person directly owns the company. Unless there is information to the contrary, this individual is also both the legal and the beneficial owner of the company.

Source: IDB and OECD



142. In reality, a company is likely to have more than one direct individual owner. But the same logic applies. You could have a situation of four individuals with direct ownership of 25% each, or two individuals with 50% each and they are the beneficial owners, unless there is information to suggest otherwise (nominee owner acting for another person). Alternatively, there could be one individual holding 65%, another individual holding 30% and one individual 5%. The first two are beneficial owners, but not the individual holding 5% as it is below the 25% threshold.

143. For identification and verification purposes, as mentioned earlier, the reporting firm needs to collect from the customer the relevant documents, including Section 119 of the Companies Act to both identify and verify legal and beneficial ownership information. These must be either original, certified true copy or electronic verification (SECP). This is to ensure that the name or names listed are true and correct, and no omission accidentally or otherwise.

144. CDD also requires the ID documents or information of the individuals who are beneficial owners. The documents need to be original, certified true copy or electronic verification using the NADRA database. This is to ensure that the name or names listed are not false or fictitious because a scanned copy or photocopy can be easily tampered with.

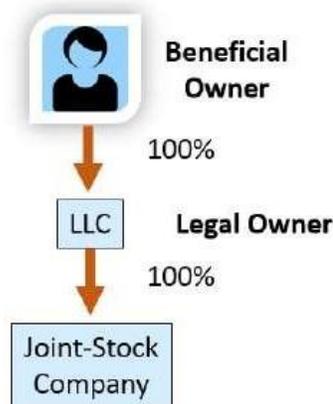
145. If one of the beneficial owner is a non – Pakistani based overseas, the customer should obtain the passport details via email and forward to the reporting firm, and a hard copy of the certified true copy sent via mail or courier. Alternatively, if the reporting firm has access to an identification service provider, the ID may be electronically verified.

146. Delayed verification is permitted under the AML / CFT legislation, and obtaining the certified true copy of the ID verification document from overseas is an acceptable scenario for delayed verification.

147. The reporting firm will need to complete the above measures to show that it has taken reasonable measures to verify the beneficial owners. The reporting firm should be able to complete the identification and verification of the beneficial owner in this example.

Example 2: Indirect ownership with one layer (Test 1: Identifying the beneficial owner through controlling legal ownership)

Source: IDB and OECD



148. Example 2 above shows an additional layer – the limited liability company (LLC) – between the legal vehicle (the Joint Stock Company) and its beneficial owner. This is indirect ownership. The LLC, as the shareholder of the Joint Stock Company, is its direct legal owner, while the beneficial owner indirectly controls the joint stock company through the LLC.

149. For identification and verification purposes, the requirements are the same as in Example 1, and the information should be contained in the Register of Beneficial Ownership information provided by the customer. However, if the information contained in the Register of Beneficial Ownership incorrectly states the beneficial owner is the LLC company – which is the 100% legal owner, this will not provide the reporting firm with information on the beneficial owner.

150. If the customer does not provide the information, you will need to ask your customer for information on the LLC company that is the 100% legal owner of your customer i.e. the Joint Stock Company. If the customer does not provide this, the reporting firm may need to obtain the LCC company information directly from the SECP or from a company registry overseas, depending where the LLC is registered or incorporated. Once obtained, the reporting firm would then be able to identify the beneficial owner i.e. the natural person owner of the LLC company who owns 100% of the customer indirectly.

151. CDD also requires the ID documents or information of the individuals who are beneficial owners. The documents need to be original, certified true copy or electronic verification using the NADRA database, if the beneficial owner is a resident. If the beneficial owner is a non-Pakistani resident overseas, then the process is the same as in Example 1 e.g. certified true copy via mail, and delayed verification. Verification may be delayed but still achievable as there is a direct relationship between the beneficial owner and your customer.

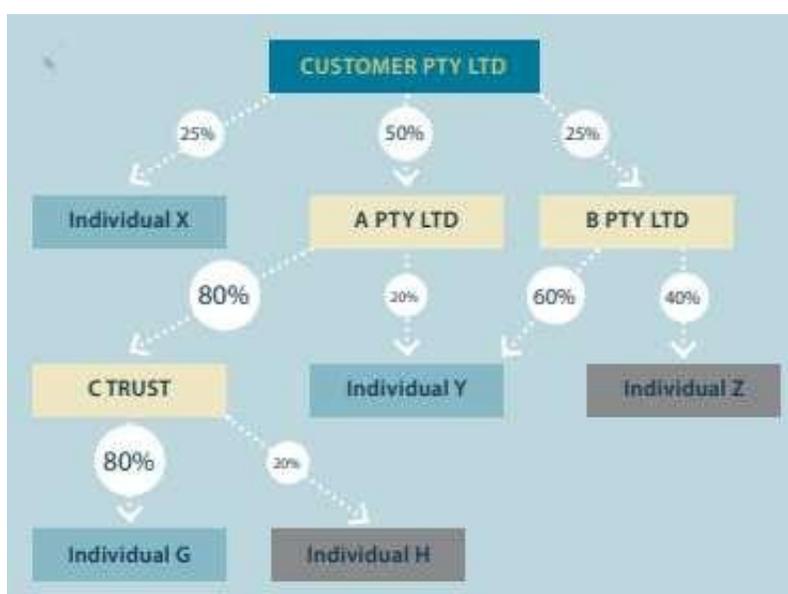
152. The reporting firm will need to complete the above measures to show that it has taken reasonable measures to verify the beneficial owner. The reporting firm should be able to complete the identification and verification of the beneficial owner in this example.

Example 3: Indirect ownership with multiple layers (Test 1: Identifying the beneficial owner through controlling legal ownership)

153. However, there may be more layers involved in the ownership structure, perhaps a chain of entities between the customer and its beneficial ownership, and there could be multiple beneficial owners.

154. Example 3 below shows the following: [Source: Austrac]

- **Individual X** is a beneficial owner because they directly own 25% of CUSTOMER PTY LTD
- **Individual G** is a beneficial owner because they hold 80% of the units in C TRUST (a unit trust) which in turn owns 80% of A PTY LTD, which owns 50% of CUSTOMER PTY LTD (meaning Individual G has an indirect $0.8 \times 0.8 \times 0.5 = 32\%$ ownership of CUSTOMER PTY LTD)
- **Individual Y** is a beneficial owner because they have two interests that collectively amounts to an indirect 25% of CUSTOMER PTY LTD:
 - o The first is their 20% interest in A PTY LTD, which owns 50% of CUSTOMER PTY LTD (providing an indirect $0.2 \times 0.5 = 10\%$ ownership of CUSTOMER PTY LTD).
 - o The second is their 60% interest in B PTY LTD, which owns 25% of CUSTOMER PTY LTD (providing an indirect $0.6 \times 0.25 = 15\%$ ownership of CUSTOMER PTY LTD).
 - o Adding these together, **Individual Y** has a $10\% + 15\% = 25\%$ interest in CUSTOMER PTY LTD



155. As with Examples 1-3, for identification and verification purposes, the reporting firm must obtain from the customer the information as explained in those examples, including the ID information of the beneficial owners (Register of Beneficial Owners) and verify either with the original, certified true copy or electronically. Assuming they are all resident in Pakistan, the verification may be completed electronically using the NADRA.

156. The reporting firm should be able to complete the identification and verification of the beneficial owners if the beneficial owners are all resident in Pakistan.

157. If they are not all residents, then the approach will be similar to Examples 1-3 i.e. if one of the beneficial owner is a non-Pakistani based overseas, the customer should obtain the passport details via email and forward to the reporting firm, and a hard copy of the certified true copy sent via mail or courier. Alternatively, if the reporting firm has access to an identification service provider, the ID may be electronically verified.

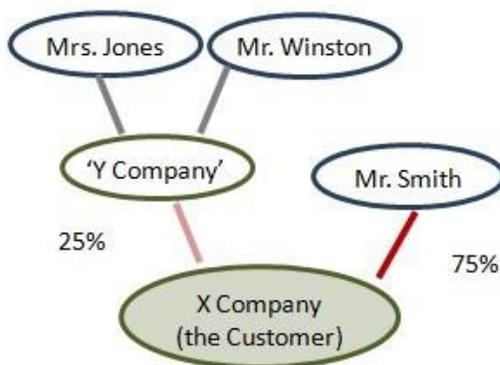
158. The reporting firm will need to complete the above measures to show that it has taken reasonable measures to verify the beneficial owner. However, if you have undertaken reasonable measures to verify the ID of Individual G but failed because the beneficial owner’s relationship with the customer is separated by two corporate layers (A Pty Ltd and C trust), you may still proceed with accepting the customer despite the

non – verification. The reporting firm may also experience problems with verifying the IDs of Individuals Y and Z. However, the customer may need to be classified as higher risk. The reporting firm will still need to conduct the other CDD measures e.g. sanction screening of the names, and as a risk mitigation measures, an internet search to ascertain if any negative news on these overseas based beneficial owners.

Example 5: Direct and indirect ownership of private company (Test 2: Identifying the beneficial owner through control by other means)

159. The point of Example 5 is to illustrate how to identify the beneficial owner through control by other means. If we use the ownership test with the 25% threshold, Mr. Smith would be the sole beneficial owner as he owns 75%. While Mrs. Jones and Mr. Winston own 50% each of Y Company, and Y Company owns 25% of the customer – X Company, individually they own only 12.5% of the customer. This is below the 25% threshold.

Source: New Zealand – FMA, DIA and RBNZ



160. However, the reporting firm discovers after reviewing the company registration details of Y company that Mrs. Jones and Mr. Winston, both live in the same residential address and are married, but Mrs. Jones has kept her maiden name. They would be working collectively to control Y company which in term would exercise its 25% control of X Company, the customer. Therefore, both Mrs. Jones and Mr. Winston are deemed to be also beneficial owners based on the control test.

Example 5: Indirect ownership of private company with multiple layers / overseas (Tests 2 / 3: Identifying the beneficial owner through control by other means / senior management)

161. Example 5 below shows a more complex scenario. Mr. Smith (foreign national resident overseas) is the beneficial owner, but he is hiding through four layers of ownership in four separate countries, not counting Company A (private company) who is the customer based in Pakistan.

Source: IDB and OECD



162. In this Example, neither Section 119 of the Companies Act nor the Registrar of Beneficial Ownership is likely to provide all the beneficial ownership information needed, given the chain of ownership includes one company that issues bearer shares (ownership is not recorded by the company – whoever holds the certificate has ownership – similar to cash) and a trust.

163. If the beneficial ownership information is not provided, then the reporting firm should take measures both by asking the customer again, or accessing the company register of Country E on Company B to ascertain who the directors are, and ownership. The company registry in Country E should show that ownership is held by Company LLC in Country D which issues bearer shares, and owned by nominee shareholders in country C.

164. Despite your efforts you may come to a dead end. The reporting firm has failed to identify the beneficial owner. At this point, the reporting firms need to decide whether to accept or reject the customer. This is clearly a high risk customer.

165. If the reporting firm decides to proceed, it must undertake enhanced due diligence prior to customer acceptance, and apply Test 2 to identify the beneficial owner. The firm should have the company directors and CEO (or equivalent) details from the customer. The reporting firm will need to be reassured, given the high risk, that the directors are not just nominee directors with no real control of the company.

166. The ID information of the directors will need to be verified. As an extra measure, the ID information of the CEO should also be verified.

167. If the reporting firm determines that the directors are nominee directors and they do not exercise control, then Test 3 may be needed. The reporting firm will need to determine whether the CEO is controlling the company e.g. major business and financial decisions etc. If confirmed, then the ID information will need to be obtained – verification may be using the original, certified true copy (someone of good standing) or electronic verification using NADRA.

168. If neither the directors nor CEO have a controlling influence, and merely actioning directives from a person whom the customer is not willing to disclose, then it is strongly advised to reject the customer and file a STR.

Example 6: Direct and indirect ownership by 10 shareholders (Test 3: Identifying the beneficial owner through control by other means / senior management)

169. The purpose of Example 6 is to highlight a situation of dispersed legal ownership and control. This simple example is of Company A which has 10 shareholders all owning 10% each. All are direct owners, and they all 10 owners are on the board of directors.

Customer – Company A	
Shareholder 1	10%
Shareholder 2	10%
Shareholder 3	10%
Shareholder 4	10%
Shareholder 5	10%
Shareholder 6	10%
Shareholder 7	10%
Shareholder 8	10%
Shareholder 9	10%
Shareholder 10	10%

170. In this scenario, there are no beneficial owners using Test 1 (ownership test) as no one owns 25% or more. Using Test 2 (control test) has not identified any owner that has control, as all are directors are with equal voting rights. Assuming owners are not forming any alliances or voting blocs, Test 3 on senior management would be the best approach.

Example 7: Publicly listed company

171. Under Section 23 of the SRB AML / CFT Regulations for Reporting Firms and Section 10 of the FBR AML / CFT Regulations for DNFBPs, reporting firms may apply simplified due diligence subject to a customer risk assessment. The company must be publicly listed company in either Pakistan, a FATF member country or another country with beneficial ownership requirements (for publicly listed companies) commensurate with those of Pakistan or FATF members.

172. Simplified due diligence for a publicly listed company may include waiving the requirement to identify and verify the beneficial owners.

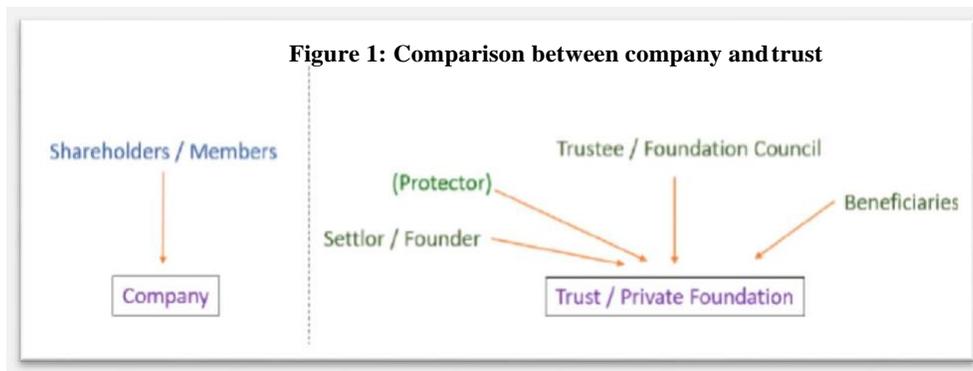
173. However, consistent with the requirements of simplified due diligence, the reporting firm must undertake the following:

- i. Confirm from information provided by the customer that it is a publicly listed company, including independently checking the relevant stock exchange in either Pakistan or overseas; and
- ii. Undertake a risk assessment to confirm the company is low risk, including checking (e.g. internet research) that the publicly listed company is not subject to any charges / convictions of money laundering or serious offences. Depending on the nature of these charges / convictions, if any, the publicly listed company may not be low risk and, therefore, ineligible for simplified due diligence.

174. It is important to remember, the waving of the beneficial ownership requirement for a publicly listed company is not automatic; it requires a risk assessment. The reporting firm will still have to complete other CDD requirements such as verification of the legal status of the company, and the ID of the authorised representative.

(iv) Legal arrangements (trusts)

175. It is one thing to identify the beneficial ownership when ownership and control are exercised by shareholders, or members who are of equal standing (left-hand panel of Figure 1), such as in a company or partnership. It is another thing to identify which individual is the beneficial owner of a trust. These arrangements have much more complex structures because they usually do not have owners but parties with different roles, rights, and obligations (right-hand panel of Figure 1). Therefore, all parties to a trust are treated as beneficial owners. Source: IDB and OECD



176. Section 14 of the SRB AML / CFT Regulations for Reporting Firms and Section 8 (10) of the FBR AML / CFT Regulations for DNFBPs require the reporting firm to identify and take reasonable measures to verify the identity of beneficial owners as follows:

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

177. 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 firm 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	
<i>Category</i>	<i>Identification and verification</i>
1. <i>Settlor (or equivalent)</i> – natural, legal person or arrangement who transfers ownership of their assets to trustee by means of a trust deed or similar arrangement.	Trust deed / Agreement Once verified based on the trust deed / agreement, the identification and verification is the same as if the person is an individual, legal person or legal arrangement (trust) customer of the reporting firm.
2. <i>Trustee (or equivalent)</i> – 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. <i>Protector (or equivalent)</i> – 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 (trust) customer of the reporting firm. If the protector is a corporate protector, the individual authorised to represent the corporate e.g. director needs to be identified and verified.
4. <i>Beneficiaries (or equivalent)</i> – 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.

	<p>If the beneficiary is a corporate beneficiary, then all CDD requirements of a legal person would need to be undertaken.</p> <p>If the beneficial is another trust – then all the CDD requirements of a trust would need to be undertaken.</p>
--	--

7.8 Politically Exposed Person (PEP)

(i) Who is a PEP?

178. Politically – exposed persons (PEPs) are individuals who, by virtue of their position in public life, may be vulnerable to corruption. The definition of PEP is not provided in the AMLA. PEPs are defined in the Definitions sections of the SRB AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFBPs as:

“Politically exposed person” or “PEP” means 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:

(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.”

179. The following provides more details on the definition of a PEP, particularly for PEPs in Pakistan:

- a. heads of states, heads of governments, ministers and deputy or assistant ministers;
- b. members of senate, provincial assembly or national assembly;
- c. members of supreme courts, high courts, constitutional courts or any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- d. Government servants equivalent of BPS-21 or above;
- e. ambassadors;
- f. Military officers with a rank of Lt General or higher and its commensurate rank in other services;
- g. directors and members of the board or equivalent function of an international organization;
- h. members of the governing bodies of political parties;
- i. members of the board or equivalent function in corporations, departments or bodies that are owned or controlled by the state.

180. The definition of PEPs is broad and it covers domestic, foreign and international organisations.

(ii) Why are family members and close associates included?

181. Family members and close associates are included because based on law enforcement investigations globally, a corrupt PEP would use either a family member or a close associate to facilitate money laundering. Criminals including corrupt PEPs like to maintain control of illicit proceeds, while at the same time distance themselves from the proceeds of corruption. They place those illicit funds in the control of those that they can trust – not strangers.

182. Family members and close associates of a PEP are also defined in the Definitions sections of the SRB AML / CFT Regulations for Reporting Firms and FBR AML / CFT Regulations for DNFBPs as.

“Family member” of a politically exposed person includes—

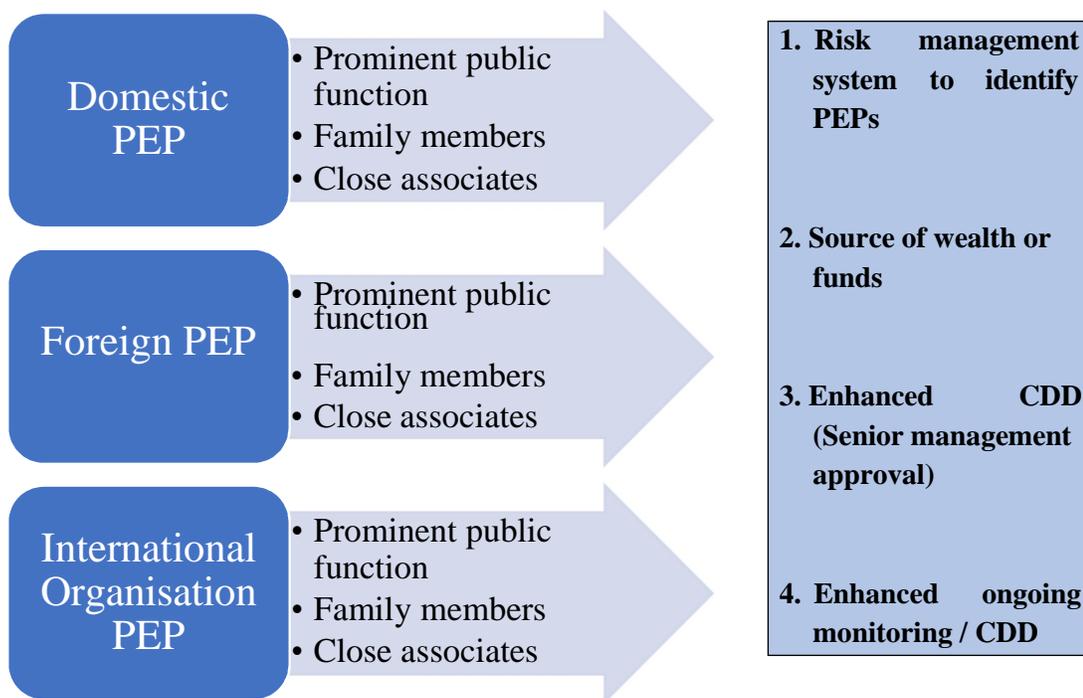
- (i) a spouse of the PEP;*
- (ii) lineal descendants and ascendants and siblings of the PEP;*

“Close associate” of a PEP means—

- (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. [Clause (iii) only in the FBR AML / CFT Regulations for DNFBPs].

(iii) Enhanced due diligence on PEPs, family members and close associates



183. Section 21 of the SRB AML / CFT Regulations for Reporting Firms and Section 9 of the FBR AML / CFT Regulations for DNFBPs state that reporting firms must undertake enhanced CDD on PEPs, and their close associates and family members, and have risk management systems in place to identify PEPs, which includes whether any beneficial owners are PEPs. This includes whether any such persons are beneficial owners of a company or a trust. This is summarised in the figure above.

(iv) Is enhanced due diligence applicable to PEPs (and family member and close associate) in all circumstances?

184. Your reporting entity will be required to undertake enhanced due diligence as described above under the following circumstances:

- PEP (& family members and close associates) who is an individual customer
- PEP (& family members and close associates) who is a beneficial 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 a settlor or protector (if any) of a trust
- PEP (& family members and close associates) who is a beneficiary of a trust's income or wealth

185. The following circumstances do NOT require the application of enhanced CDD 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:

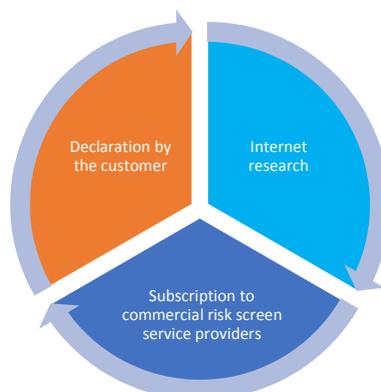
Authorised representative of a legal person	Non beneficial owner of a company
<ul style="list-style-type: none"> • For example, authorised representative of a government entity • Note: While enhanced due diligence is not required, the reporting firm will still need to identify and verify the identity of the authorised representative, and that the individual is so authorised by his/her organisation. 	<ul style="list-style-type: none"> • 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 management, and thereby control the company.

186. There is nothing precluding a reporting firm from applying enhanced due diligence to a PEP in the above circumstances, even if is not rule mandated in the AML / CFT legislations. Importantly, the AML / CFT legislation also requires a risk based approach.

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

(v) Procedures to identify a PEP (and family member and close associate)?

188. There are three main methods of identifying a PEP, which are not mutually exclusive. These are shown below:



189. Firstly, the reporting firms' procedures 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.

190. Secondly, the reporting firm should undertake an independent check. The reporting firm's procedures may include:

- an internet search of the customer's or beneficial owner's background
- databases and reports from commercial service providers

191. Commercial risk screening service providers do provide databases of PEPs. They may be good for foreign PEPs, but may not be as good for Pakistani PEPs and their family and close associates. Importantly also, they may be too expensive for sole practitioners or small reporting firms.

192. Your reporting firm 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. This may occur if the individual customer is promoted into a more senior role, or an ownership of a company changes and an individual acquires 25% or more, or some other controlling interest, or for some other reasons.

7.9 Source of wealth or funds

(i) Source of wealth

193. The source of wealth refers to the origin of the customer's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the customer acquired such wealth. Although, the reporting firm may not have specific information about assets, it may be possible to gather general information from commercial databases or other open sources (e.g. internet search).

(ii) Source of funds

194. The source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between the customer and the reporting firm as part of the business relationship.

(iii) Enhanced due diligence

195. The requirement to obtain information on the source of wealth or source of funds is limited to customers subject to enhanced due diligence under Section 21(2)(c) of the SRB AML / CFT Regulations for Reporting Firms and Section 9(2) (c) of the FBR AML / CFT Regulations for DNFBPs. The requirement is for information only – supporting documentation is not required unless there are doubts on the veracity of the information provided, or because of risk.

(iv) PEPs

196. PEPs which are subject to enhanced due diligence have additional requirements, namely to take reasonable measure to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP under Section 21(3)(b) of the SRB AML / CFT Regulations for Reporting Firms and Section 9(3)(b)(ii) of the FBR AML / CFT Regulations for DNFBPs.

197. While all PEPs are subject to enhanced due diligence, they are not all high risk. Depending on the risk of the PEP customer, the level of due diligence will vary. There is no explicit requirement for verification of source or wealth or funds. However, for PEPs, taking reasonable measures may require verification of

source of wealth and funds. If there is an adverse news report on a PEP (or family members and associates), then more due diligence would be required than one that has no negative news. Also, for the reporting firm, establishing the source of wealth or funds will also vary depending on the specified services provided.

198. Some examples are highlighted below:

<p style="text-align: center;">Example 1</p> <p style="text-align: center;">PEP wants to form new company for construction business</p> <p>Source of funds: Are funds from existing business, business loan, savings etc needed for buying equipment etc for new business?</p>	<p style="text-align: center;">Example 2</p> <p style="text-align: center;">PEP wants to sell his sole trader business</p> <p>Source of wealth: How long has the PEP held the business? How did the PEP acquired the business e.g savings, business loan?</p>
<p style="text-align: center;">Example 3</p> <p style="text-align: center;">PEPs wants his business payroll account managed (he is the principal owner)</p> <p>Source of wealth / funds: How long has the business been operating? How did it start? What are the main sources of revenue? Do you have access to monthly bank statements to monitor deposits (to establish legitimate sources of funds) and other payments?</p>	<p style="text-align: center;">Example 4</p> <p style="text-align: center;">PEP wants the partner of your reporting firm to be the trustee for his family trust</p> <p>Source of wealth / funds: The wealth portfolio including any businesses and income streams will need to be collected to establish sources of both wealth and funds. This is very important as the partner will be making trust distributions based on the wealth / income portfolio.</p>

199. Further, if the reporting firm has doubts that the stated source of wealth or funds may be incorrect, then it should request documents to confirm of source of wealth or funds. For example, a financial statement, or taxation return. Unlike for ID documents, these do not need to be original or certified true copy, unless the reporting firm has doubts on the veracity of the documents provided.

200. The Table below provides some examples of acceptable sources.

INFORMATION AND VERIFICATION OF SOURCE OF WEALTH OR FUNDS			
<p>a) Employment Income</p> <ul style="list-style-type: none"> • 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 	<p>b) Business income / Profits / Dividends</p> <ul style="list-style-type: none"> • Copy of latest audited financial statements; • Board of Directors approval • Rental statements • Dividend statements 	<p>c) Savings / deposits / assets / property</p> <ul style="list-style-type: none"> • Statement from financial institution • Bank Statement • Taxation returns • Accountant’s statements • Property ownership certificate • Share certificates 	<p>d) Inheritance</p> <ul style="list-style-type: none"> • Succession Certificate.
<p>e) Sale of Property / Business</p> <ul style="list-style-type: none"> • Copy of sale agreement / Title Deed 	<p>f) Loan</p> <ul style="list-style-type: none"> • Loan agreement 	<p>g) Gift:</p> <ul style="list-style-type: none"> • Gift Deed; • Source of donor’s wealth; • Certified identification documents of donor. 	<p>h) Other income / wealth sources:</p> <ul style="list-style-type: none"> • 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.
--	--	--	--

7.10 Enterprise risk assessment and customer risk assessment

201. Sections 4 in both the SRB AML / CFT Regulations for Reporting Firms and the FBR AML / CFT Regulations for DNFBPs state that the reporting firm must identify and assess the ML / TF risks in relation to its customers, together with other risk categories.

202. The enterprise risk assessment and customer risk assessments are closely linked, but they are not exactly the same. Your reporting firm is required to both (a) conduct the enterprise risk assessment and (b) assess individual customer risk, particularly for new customers. The enterprise risk assessment provides a macro assessment of risk in your firm, while the individual customer risk assessment is a micro perspective. Customer risk assessment determines the risk profile of the customer only. That said, 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.

203. They are different because not all your risks are directly related to your customers, although the customer is the glue that connects the various risk variables. Some may be due to your products, services, or channels for delivering your services or products. For example, if your reporting firm accepts cash payments or manage cash payments, these are inherently higher risk than through the regulated financial sector e.g. banks, as there is a clear paper record. You may decide to apply risk mitigation measures such as not dealing in cash or imposing a threshold – these measures would then apply to all customers irrespective of individual customer risk.

7.11 Customer risk assessment and risk based CDD

204. The risk assessment methodology for the customer risk assessment is the same as the enterprise risk assessment:

Threat + Vulnerabilities (Likelihood and Consequence) = Risk.

205. The customer risk assessment must be sufficiently precise to allow the development of a risk matrix that grades customers, products, geography, and delivery channels into risk categories to derive an overall customer risk rating. Each customer must receive an initial AML / CFT risk rating at the beginning of the business relationship, and it must be kept current based on updates and changes in the relationship. For example, if a customer is inactive over a longer period of time, the risk rating may need to be revised.

206. **Lower risk:** For specified services subject to AML / CFT legislations, this would be not common for reporting firms, except if the customer is a publicly listed company, financial institutions regulated by the SBP or SECP, or a welfare recipient (which is unlikely to need an accountant).

207. **Medium risk:** Standard customer due diligence is the most common level of due diligence and would be the most common situation facing the reporting firm.

208. Higher risk: Section 21 of the SRB AML / CFT Regulations for Reporting Firms and Section 9 of the FBR AML / CFT Regulations for DNFBPs state that when a customer or beneficial owner of a customer is a (i) politically exposed person (PEP), and (ii) the business relationship and transactions are with natural and legal persons from countries for which this is called for by the FATF, they are automatically higher risk and subject to enhanced due diligence.

209. It is the responsibility of each business line or customer facing staff member to undertake CDD, including assigning a risk rating. It is the decision of each reporting firm to decide who approves the acceptance of a new customer (e.g. compliance officer, manager of the concerned staff member, or staff member), except that under enhanced due diligence, it cannot be the staff member dealing with the customer. It has to be a senior management as required under the AML / CFT legislations.

a. The following Table lists indicators where the risk of ML / CFT is higher.

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 trusts).	Companies with complex ownership structures.
Non – Government Organization (NGO), 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.
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 FATF (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.
Providing services that involve the provision of nominee directors, 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 the Reporting firm, or undertaking wire transfers on behalf of the customer.
Products/services identified as high risk in NRAs.	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 that client.
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)	
---	--	--

210. When engaging with the prospective customer, the reporting firm will need to gather information about the prospective customer sufficient to undertake the customer risk assessment.

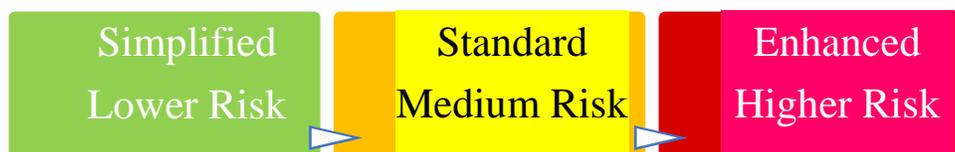
211. An example of a customer risk assessment template is at [Annex 1](#).

7.12 Three categories of CDD

212. Once the customer risk has been determined i.e. low, medium or high, the required customer due diligence is determined. In practice, the reporting firm has to commence the CDD process first and gather sufficient information to determine whether it is simplified CDD, standard CDD, or enhanced CDD.

213. The figure below highlights the relationship between low, medium and high customer risk, and the levels of CDD.

Relationship between customer risk and level of CDD



7.13 Simplified CDD

214. **Required information and verification:** Section 23 of the SRB AML / CFT Regulations for Reporting Firms and Section 10 of the FBR AML / CFT Regulations for DNFBPs state that simplified due diligence may be applied to both the customer or beneficial owner, but only where lower risks have been identified through an adequate analysis through its own risk assessment; any other risk assessments publicly available or provided by either the relevant SRB or FBR; and in accordance with the AML / CFT regulations and commensurate with the lower risk factors.

215. Under simplified CDD, verifying the legal identity and beneficial ownership may occur after customer on boarding and the degree on ongoing CDD may be reduced. The following is a summary of the main CDD requirements for simplified due diligence:

Simplified CDD measures on customers

- Information to identify and verify identity
- Information to identify and verify address
- Information to identify and verify beneficial ownership
- If necessary, identify and verify natural person representing the customer
- Scope for delayed verification of customer identity and beneficial ownership
- Reduced the degree of on – going monitoring and scrutinizing transactions

216. Subject to a risk assessment confirming low risk, simplified due diligence may be applied to publicly listed companies (in Pakistan, FATF member country or a country with equivalent transparency standards on such companies), or 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.

7.14 Standard CDD

217. Neither the AMLA nor the AML / CFT regulations of the two SRBs and FBR is explicit on the requirements or circumstances where standard due diligence would apply. It is inferred that standard requirements on customer due diligence will apply if the customer is not identified as assessed a higher risk and subject to enhanced customer due diligence, or lower risk and subject to simplified customer due diligence.

Standard CDD measures on customers

- 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 the identity of the beneficial owner
- Take reasonable measures to verify identity of beneficial owner
- Ongoing due diligence

7.15 Enhanced CDD

218. As mentioned, enhanced CDD applies to all PEPs and their families and close associates, and to customers and transactions to, or from countries when called upon by the FATF. Enhanced CDD also applies to any other customer rated higher risk. The possible indicators are detailed in the above table.

219. The required enhanced customer due diligence measures are summarised below:

Enhanced CDD measures on customers

- 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 take reasonable measures to verify the identity of the beneficial owner
- Information on the source of funds or wealth of the customer
- Establish source of funds and wealth, if a PEP.
- Senior management approval before accepting customer
- Enhanced ongoing monitoring

7.16 Examples of standard and enhanced CDD

220. The following provides two case examples of the application of risk based customer due diligence.

Case Study 1: Example of Standard Customer Due Diligence: Managing payroll for a small construction company

Customer	Solid Construction (Private Company) Ltd
Specified service	Managing customer funds – making payroll payments to staff
ML / TF risk	Medium
Level of CDD required	Standard CDD
Steps to complete standard CDD	
How this applies to the example	
1.	Obtain information about the nature and purpose of the proposed business relationship
	Mr. Shozib explains that with the business growing, it is the right time to obtain professional accounting services for maintaining the payroll bank account and making payroll payments directly to staff.

2.	Obtain and verify name of customer and address – including all directors, registered and business addresses	<ul style="list-style-type: none"> • Certificate of Incorporation • Memorandum of Association • Articles of Association • List of members, shareholder and directors required to be filed under the Companies Act, 2017 (XIX of 2017), • SECP registered declaration for commencement of business as required under Companies Act, 2017 • Register of Beneficial Ownership • Utility bill for company with physical address <p>The above information verified the name and address of Solid Construction (Private Company) Ltd. and Mr. Shozib is listed as the sole director and shareholder of Solid Construction (Private) Limited.</p> <ul style="list-style-type: none"> • Mr. Shozib provides the original of his CNIC ID document. • Original of CNIC is sighted by the reporting firm, photocopied and signed by a staff member.
3.	Obtain and verify names of beneficial owners	<ul style="list-style-type: none"> • Section 119 (XIX) lists just Mr Shozib as the sole member and shareholder • List of directors required to be filed under the Companies Act, 2017 (XIX of 2017) • Memorandum of Association • Articles of Association • The natural person owner is also the beneficial owner.
4.	Obtain and verify name of person acting on behalf of customer	<ul style="list-style-type: none"> • Mr. Shozib as the sole director is also acting on behalf of his own company. • For the completion of paperwork, he provides a signed letter indicating as the sole director, he is so authorised to act on behalf of the company as per the company formation documents (e.g. article and memorandum of association)
5.	Assess the ML / TF risk of customer	<ul style="list-style-type: none"> • Name (company and beneficial owner) checked against Ministry of Foreign Affairs and Ministry of Interior lists, and the UNSC website – all okay. • Internet check or subscriptions services for adverse news – all okay. • The reporting firm determines that the ML / TF risk is medium, so it can apply standard CDD. • This was based on the four risk variables and indicators for each of those variables, sanctions screening and reputational risk screening. <ul style="list-style-type: none"> ○ Customer risk: Simple company structure and beneficial ownership. ○ Geographic risk: No connection to higher risk geographic regions in Pakistan or overseas. ○ Service risk: Straightforward payroll management – all domestic payments to employees bank accounts. ○ Delivery channel risk: Face to face with customer.
5.	Source of wealth / income Senior management approval Enhanced ongoing CDD / monitoring	<ul style="list-style-type: none"> • Information gathered but verification not required, as rated medium risk and not higher risk. (Note – it is not mandatory to gather such information except for high risk customers; however, it is good practice to do so.) • No need for senior management approval. • Only standard ongoing CDD.
6.	If the identity information and verification requirements are satisfied, then Reporting firm may accept Solid Construction as a new customer.	<ul style="list-style-type: none"> • The reporting firm accepts the engagement with Solid Construction (Private) as a new customer.

Case Study 2: Example of CDD (high risk): Secretarial services for a tech start – up company

Customer	Mr. Aatif, who is launching a start – up company
Specified service	Forming a company – The reporting firm is requested to form a company for Mr. Aatif. Further, the reporting firm is asked to provide a registered address for that company.
ML / TF risk	High
Level of CDD required	Enhanced CDD
Steps to complete EDD	
How this applies to the example	
1. Obtain information about the nature and purpose of the proposed business relationship	Mr. Aatif explains that the purpose of his start-up business is to generate income from the smartphone applications. Users will make subscription payments via an online platform for using the applications. Mr. Aatif explains that he would like the reporting firm’s advice on how best to set up this company and also require assistance to form it i.e. prepare all the paper work and submit to SECP. He explains that he also requires the reporting firm to offer a registered address for the company as he is a frequent traveller.
2. Obtain and verify name of customer and address – including all directors, registered and business addresses	In this case, the company has not been formed. The primary focus is on Mr Aatif, as he is the customer. The reporting firm asks Mr. Aatif to provide identity information about himself (including proof of his address). Mr. Aatif provides his original CNIC. The reporting firm views and takes a clear copy, and the employee signs and notes on the copy the date in which the original was sighted. Mr. Aatif also provides a copy of his mobile telephone account and utility account for his address. Both are the original statements. The reporting firm copies both documents and the employee signs and dates the copies, noting when the originals were sighted. However, the reporting firm also needs to understand the ownership and structure of the proposed company as required under the AML / CFT regulations. Based on questions asked, following information was provided by the customer: <ul style="list-style-type: none"> • Mr. Aatif explains that 50% of the seed funding is coming from his parents (Mr. A Aatif and Mrs K Aatif, with a further 50% from his friend (Mr. M Khan, a Pakistani expatriate) who lives overseas. • There is a loan agreement between him and his friend. • Mr. Aatif proposed business would be part funded by an investor (his friend), who lives in a country that is a high risk jurisdiction. • The country risk is a red flag indicator. • Mr. Aatif will be one company director, and his parents the other company director. • Share ownership would be in his name and that of his parents.
3. Obtain and verify names of beneficial owners	Based on information provided, the beneficial owners are: Mr. Aatif His parents Mr. A Aatif and Mrs. K Aatif His friend (Mr Khan), while not listed as director or shareholder, has control. The reporting firm asks Mr. Aatif to provide identity information and verification documents about his parents and his investor friend. Mr. Aatif parents live in Skardu and he provides their CNICs. These are not the originals, nor certified true copies, just email versions. The reporting firms

		<p>confirms that they are authentic by checking the NADRA database by paying a small fee.</p> <p>The reporting firm was also provided with a copy of Mr Khan’s Pakistan CNIC which had been certified by a suitable professional in the overseas country. However, this is not the original of the certified true copy, just an attachment to an email.</p> <p>As Mr Khan is overseas, the validity of the ID (CNIC) was validated via NADRA’s online user system.</p>
<p>4.</p>	<p>Assess the ML / TF risk of customer</p>	<p>An assessment is made of customer risk</p> <ol style="list-style-type: none"> 1. Sanctions screening: All the names were checked against the Ministry of Foreign Affairs’ list and Ministry of Interior’s list of proscribed entities – all okay, as no match. A check also was made of the UN Security Council’s consolidated list, and also no match. 2. Customer risk – higher risk as a new business and customer has no established business record – and funding is from overseas in high risk country and the son of a PEP. 3. Geographic risk – high risk as 50% of funds is from a high risk country and noted by the FATF as weak in AML / CFT. It is not subject to any UN sanctions or embargoes. This was based on a check of the FATF’s website and UNSC sanctions page. 4. Services – providing a registered mailing address is considered higher risk service by the reporting firm. 5. Delivery channel risk – while the service to the customer is face-to-face, his company once established will be virtual, and interactions will be more non face-to-face given his absence from the country – the reason he has given for the using the reporting firm as the registered business address. 6. Risk screening: A google search has also indicated that his father is a former senior government official. So he and his parents also meet the definition of politically exposed person. Under the AML / CFT regulations, this alone requires enhanced due diligence, notwithstanding all the above factors requiring enhanced due diligence.
<p>5.</p>	<p>Source of wealth / income</p>	<p>Given the customer is subject to enhanced CDD, the following additional measures were undertaken on his source of wealth / funds.</p> <p>Mr. Aatif also provided his bank statements that show his home address and lump sum payments from two sources: his parents and his friend (friend’s contribution originated by wire transfer from the overseas country. However, this does not fully enable Identification of the actual source of the funds).</p> <p>Mr. Aatif parents live in Skardu and he provides details of recent Sale and purchase agreement that shows they have a profit from a property sale – some of which has been given to their son for the seed money.</p> <p>The reporting firm enquires whether the funds provided are a gift or a loan. Mr. Aatif inform that they are a gift from parents, in lieu of future inheritance, and that appropriate paperwork has been filed via their lawyer. They have this paperwork with them. The reporting firm makes copies of all these documents, and signs and dates the photocopies.</p> <p>The reporting firm requests for further documents relating to the source of the friend’s funds. The reporting firm is provided with a copy of a five-year term deposit bank statement held at a bank in the overseas country, which has been certified by the banker and the friend’s lawyer. This shows that the term deposit concluded shortly before the date on which Mr. Aatif received funds in Pakistan.</p> <p>There are certified copies of accompanying bank records showing the instruction.</p>

6.	Senior management approval	<p>The staff member in the reporting firm seeks senior management approval as required in the firm’s internal AML / CFT procedures and AML / CFT regulations as all high risk customers / enhanced due diligence must require senior management approval.</p> <p>As also required by the firm’s internal AML / CFT procedures and AML / CFT regulations, the recommendations detailed enhanced ongoing monitoring which includes ensuring the reporting firm’s address is not being used for mail not related to the newly formed company.</p>
7.	Enhanced ongoing CDD / monitoring	<p>The only ongoing relationship with the customer is providing the registered address of the company.</p> <p>Ensure non business mails e.g. mail is not received at this address for any other business owned by the customer or beneficial owners.</p> <p>Check the company registration details on an annual basis e.g. ownership has not changed.</p>
8.	If CDD has been completed satisfactorily the, reporting firm may proceed to accept the person as a new customer.	<p>The reporting firm based on steps concludes that this customer and activity is not suspicious.</p> <p>The reporting firm accepts the engagement with Mr Aatif as a new customer.</p> <p>The reporting firm then form the company for Mr. Aatif and keeps the record of the incorporated company for record keeping as required under the AMLA and AML / CFT regulations.</p>

221. The templates for customer on boarding for private companies, individuals and trusts are available at *Annex 2*. These are for voluntary use, and your reporting firm may decide to amend to suit the specific circumstances of your business.

7.17 Prohibited customers and risk screening

222. Section 25 of the SRB AML / CFT Regulations for Reporting Firms and Section 8(13) of the FBR AML / CFT Regulations for DNFBP prohibit the reporting firm and any other business from providing services to any persons or entities and their beneficial owners that are designated / proscribed by the Statutory Regulatory Orders (SROs) / notifications issued by the Ministry of Foreign Affairs, National Counter Terrorism Authority and Ministry of Interior. All new customers must be screened against the SROs issued, and existing customers on a regular basis (every time there are updates to the sanctions lists). This is covered in detail in the section of the Guidelines on targeted financial sanctions.

223. 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 firm cannot accept the new customers as the legal person no longer exists.

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

7.18 Delayed verification

225. 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 rare.

226. Delayed verification is provided in Sections 17-18 of the SRB AML / CFT Regulations for Reporting Firms and Section 8 (13)-(14) of the FBR AML / CFT Regulations for DNFBPs. They provide for delayed verification subject to certain conditions – refer to table below.

227. There should be no reason why information on the identity and address of the customer and any authorised representative should be delayed, and nor are they legally permitted under the AML / CFT legislations.

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 interrupt 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.

7.19 Unable to complete CDD

228. Section 7D of the AMLA states very clearly that where a reporting firm is unable to complete CDD, the reporting firm:

- (a) shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship if any; and
- (b) shall promptly consider filing a Suspicious Transaction Report in relation to the customer.

229. The AMLA is very clear that if the reporting firm cannot complete the CDD process, even when verification is delayed after the start of the business relationship for whatever reason, the reporting firm must not provide, or cease to provide services. These circumstances could be:

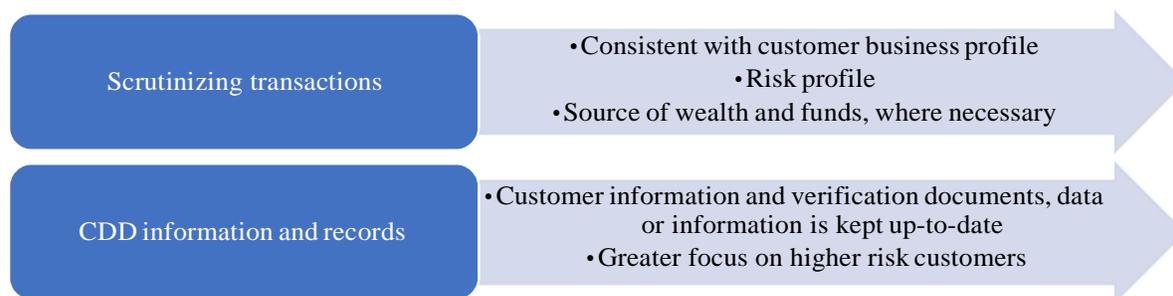
- (i) If a prospective customer refuses to provide evidence of identity or other information properly requested as part of CDD;
- (ii) where the reporting firm is not satisfied with the information and verification commensurate with the higher risk profile of the customer; and
- (iii) where too many questions may be tipping off the customer of suspicion by the reporting firm.

7.20 CDD and tipping off

230. As noted above, if continued CDD may tip off a potential customer then, if the reporting firm under 7D (2) of the AMLA forms a suspicion of ML or TF, and reasonably believes that performing the CDD process will tip-off the customer, the reporting entity (e.g. reporting firm) shall not pursue the CDD process and shall file a STR.

7.21 Ongoing monitoring of new customers

231. Section 19 of the SRB AML / CFT Regulations for Reporting Firms and Section 8 (6) of the FBR AML / CFT Regulations for DNFBPs require ongoing due diligence of the business relationship. 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. However, there is ongoing CDD which consists of two major components:



232. The extent to which your reporting firm has to undertake both will depend on the specified services provided. If your reporting firm is providing services that manages the funds, assets or properties of your customers e.g. bank account, then scrutinising 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.

233. Ongoing CDD is important to maintain up-to-date information on customers so that:

- the risk assessment of a particular customer in case of change in circumstances can be updated e.g. from medium to higher risk; and
- further due diligence measures can be carried out, if necessary.

Event-driven reviews

234. The events triggering a CDD information update may include:

- a) a change in the customer's identity;
- b) a change in beneficial ownership of the customer;
- c) a change in the service provided to the customer;
- d) information that is inconsistent with the business' knowledge of the customer; or
- e) a suspicion of ML / TF.

235. 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 a STR has been made, care should be taken to avoid making any disclosures which could constitute tipping off.

Periodic reviews

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

237. 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.

7.22 Existing customers

238. Section 20 of the SRB AML / CFT Regulations for Reporting Firms and Section 8(16) of the FBR AML / CFT Regulations for DNFbps state that the reporting firm shall apply CDD requirements to existing customers 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.

239. Existing customers refer to customers of the reporting firm prior to new AML / CFT CDD requirements coming into force and effect. For members of the two SRBs, this was up to 30 September 2020. For other accountants supervised by the FBR, this was up to 28 September 2020, as the FBR AML / CFT Regulations for DNFbps came into force and effect at once upon promulgation on 29 September.

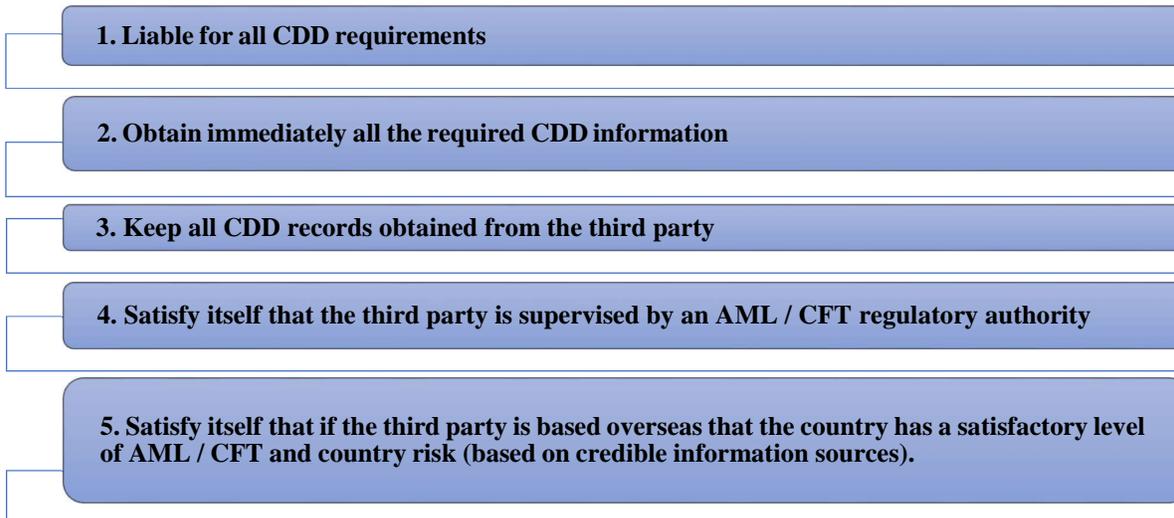
240. It is important for the reporting firm, especially if it is a larger firm, to have a centralised database of customers with all the information collected. A centralised system will allow information collected on the customer from various business lines to be access by all staff interacting with the customer. It will help avoid the same questions and information asked of the customer and will enhance customer satisfaction.

241. A centralised 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. Refer to Table below:

Table on existing and new customers		
Existing customers (prior to AML / CFT requirements)		New customers (After AML / CFT requirements coming into force and effect)
Dormant	Active	
<p>No ongoing business relationship or services</p> <p>They will need senior management decision whether they should be treated</p>	<p>Ongoing services</p> <p>CDD would be trigger if suspicion of ML / TF, or material change in the customer’s profile based on a new engagement, or ongoing monitoring.</p>	<p>Subject to the full CDD requirements</p>

<p>as new customers, or existing if they again provide services.</p> <p>For example, if dormant for 2-3 years, they could be treated as new customers to minimise risk.</p>	<p>There should also be a periodic review of existing customers, particularly those that may be in the higher risk categories.</p>	
---	--	--

7.23 Reliance on third party to conduct CDD



242. The CDD measures / steps can be carried out by a third party on behalf of the reporting firm. Accordingly, the reporting firm is permitted to rely on certain other parties (subject to their agreement) to complete all or part of CDD.

243. Section 7B of the AMLA provides for reliance on third parties in conducting CDD. This principle is further detailed in Section 24 of the SRB AML / CFT Regulations for Reporting Firms and Section 12 of the FBR AML / CFT Regulations for DNFBPs. The conditions attached on the reporting firm relying on the third party are summarised in the above figure.

244. Where the third party is part of the same corporate group as the reporting firm, the later may deem the requirements in the above diagram to be met if:

Corporate group compliance	AML / CFT supervision of corporate group	Corporate group mitigation policies for higher country risk
<ul style="list-style-type: none"> •The corporate group applies CDD and record-keeping requirements in accordance with the AMLA and its associated regulations 	<ul style="list-style-type: none"> •The implementation of the group CDD, record keeping and PEP requirements is supervised by an AML / CFT regulatory authority or an equivalent foreign authority 	<ul style="list-style-type: none"> •The corporate group has adequate measures in place to mitigate any higher country risks

245. Other examples of a third party could be from a bank or lawyer, or even another accountant if the customer is also a customer of those other reporting entities subject to AML / CFT legislations. Of course, the reporting firm would have to obtain the CDD information and verification documents from the other third party – only one is needed.

8. Targeted Financial Sanctions

246. Targeted Financial Sanctions (TFS) means both assets and funds freezing and prohibitions to prevent assets or financial services from being made available, directly or indirectly, for the benefit of designated persons and entities, except as authorized by the Competent Authority i.e. Ministry of Foreign Affairs or Ministry of Interior/ National Counter Terrorism Authority(NACTA).

8.1 Statutory requirements under AML / CFT legislations

Targeted financial sanctions obligations are provided under the following legal instruments:

- UN Security Council Act
- Statutory Regulatory Orders (SROs) issued under UN Security Council Act
- UNSC (Freezing and Seizure) Order, 2019
- Anti-Terrorism Act, 1997 (ATA)
- Notifications issued under ATA
- AMLA, 2010

AMLA: Under Sections 7G reporting firms must have a compliance programme and have AML / CFT policies and procedures, including for targeted financial sanctions.

SRB AML / CFT Regulations for Reporting Firms: Section 25 states that the reporting firm must undertake the following:

(i) develop mechanisms, processes and procedures for screening and monitoring customers and potential customers to detect any matches or potential matches with the stated designated / proscribed person – or if beneficial owners of the designated/proscribed person – in the SROs and notifications issued by Ministry of Foreign Affairs, National Counter Terrorism Authority (NACTA) and Ministry of Interior.

(ii) If during the process of screening or monitoring of customers or potential customers a positive or potential match is found, the reporting firm shall:

- a) freeze the relevant funds and assets, without delay, in accordance with the respective SRO;
- b) not provide any services, property or funds to the person in question in accordance with the respective SRO; and
- c) reject the transaction or attempted transaction or the on boarding of the customer, if the relationship has not commenced

(iii) In all cases referred to in (ii), the reporting firm shall file a suspicious transaction report to the FMU under Section 7 of the AMLA and notify the SRB in the manner as may be directed by the SRB from time to time.

(iv) Implement any other obligation under the AMLA, UNSC Act and ATA and any regulations made there under.

FBR AML / CFT Regulations for DNFBPs: Section 13 includes the same mandatory requirements as above, although the reporting is to the FMU and the FBR. The regulations are more prescriptive on beneficial ownership requirements, as detailed in Section 13 (2) below:

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

8.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator may impose monetary and administrative penalties for any violations of the provisions of the SRB AML / CFT Regulations or FBR AML / CFT Regulations pertaining to TFS.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by the SRB [ICAP / ICMA PAKISTAN] according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under AMLA.

AML / CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction REAs for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

Penalty for Violation of SROs issued under UNSC Act: Section 2 of the UNSC Act clearly states that provision may be made for the punishment of person (s) found in violation of the SROs. The United Nations Security Council (Enforcement) Order, 2012 notified vide S.R.O. 381 (I)/2012 dated 29th March 2012 and last amended on 11th January 2013 prescribed the penalty for violation of SROs.

If any person, including a company or other juristic body, fails or refuses to comply with any SRO issued under UNSC Act 1948, the Federal Government may, if satisfied, after giving the opportunity of being heard, that the non-compliance or violation was wilful, can impose a fine of up to 10 million rupees.

Penalty for Violation of SROs issued under the ATA: For measures pursuant to UNSCR 1373, s 11O(2) of the ATA 2014 provides that any natural or legal person who violates a freeze on funds or other assets for prescribed individuals (s 11EE) and organisations (s 11B) are liable for a one-off maximum fine of 10 million rupees. Directors, officers and employees of legal persons found guilty of violation of a freezing action are also liable for a one-off maximum fine of 10 million rupees.

8.3 United Nations Security Council and Pakistan Sanctions

247. There are three categories of sanctions, all which relate to Pakistan’s membership of the United Nation, and as a member, its obligations to implement United Nation Security Council Resolutions (UNSCRs) relating to targeted financial sanctions for TF and proliferation financing.

248. Both the two SRBs and the FBR have issued SROs, guidelines or frequently asked questions on targeted financial sanctions under UNSCRs. These are available via the links below:

- <https://www.icap.org.pk/aml-supervision/targeted-financial-sanctions-tfs/>
- https://www.ICMA Pakistan.com.pk/FAQs_on_TFS_Obligations.pdf
- <https://.fbr.gov.pk/TargetedFinancialSanctionsStatutoryRegulation.pdf>

249. The following outlines the requirements under the three categories of targeted financial sanctions.

UN Security Council Sanctions on AI-Qaida/Da'esh and Taliban (terrorism financing)

250. A National Committee for overseeing implementation of sanctions against individuals and entities designated by UNSCRs 1267 and 1989/2253/2368 (AI-Qaida/Da'esh Sanctions regime) and UNSCRs 1988/2254 (Taliban Sanctions regime) was constituted vide S.R.O 1015 (I)/2018 dated 24 August 2018.

251. Accordingly, the Government of Pakistan under the UN Security Council Act, gives effect to the decisions of the UNSCRs whenever the consolidated list maintained by the UN is updated. In this regard

The Ministry of Foreign Affairs issues SROs from time to time to provide legal cover for implementing sanction measures under the UNSCRs.

252. The relevant links to the list are provided below:

- Ministry of Foreign Affairs SROs for UN Security Council sanctions:
<http://mofa.gov.pk/unsc-sanctions/>
- UN Security Council ISIL (Da'esh) & Al-Qaida Sanctions Committee:
https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list/summaries
- UN Security Council Taliban Sanctions Committee:
<https://www.un.org/securitycouncil/sanctions/1988>

Pakistan Government sanctions (terrorism financing)

253. In addition to UNSCRs 1267 (AI-Qaida/Da'esh Sanctions regime) and 1988 (Taliban Sanctions regime), UNSCR 1373 requires member states to have its own designation process to make autonomous designations or respond to a foreign state's request.

254. The Government of Pakistan under section 11B of the ATA can declare an organization believed to be concerned with terrorism as a "Proscribed Organization" or "Proscribed Persons". In this regard, Ministry of Interior / NACTA the formal notification of proscription of an organization or person.

255. The relevant links to the lists are provided below:

- a. <https://nacta.gov.pk/proscribed-organizations-3/>
- b. <https://nacta.gov.pk/pp/>
- c. <https://nfs.punjab.gov.pk/>

UN Security Council Sanctions on Democratic Republic of Korea (DPRK) and Iran (proliferation financing)

256. International efforts in countering proliferation financing have intensified in response to the nuclear weapons programmes of DPRK and Iran. Recommendation 7 of the FATF Standards requires countries to implement proliferation financing-related targeted financial sanctions made under UNSCRs.

257. The two UNSCRs are 1718 for DPRK and 2231 for Iran.

258. Pakistan's Strategic Export Control Division (SECDiv) of the Ministry of Foreign Affairs issues SROs under to S2 of the UN Security Council Act to give effect to Pakistan's UN obligations related to proliferation financing.

259. The relevant links to the lists are provided below:

- Ministry of Foreign Affairs Strategic Export Control Division (SECDIV) SROs
<http://www.secdiv.gov.pk/page/sro-unscr-sanctions>
- UN Security Council 1718 (DPRK) Sanctions Committee:
<https://www.un.org/securitycouncil/sanctions/1718/materials>
- UN Security Council Resolution 2231 Iran Sanctions:
<https://www.un.org/securitycouncil/content/2231/background>

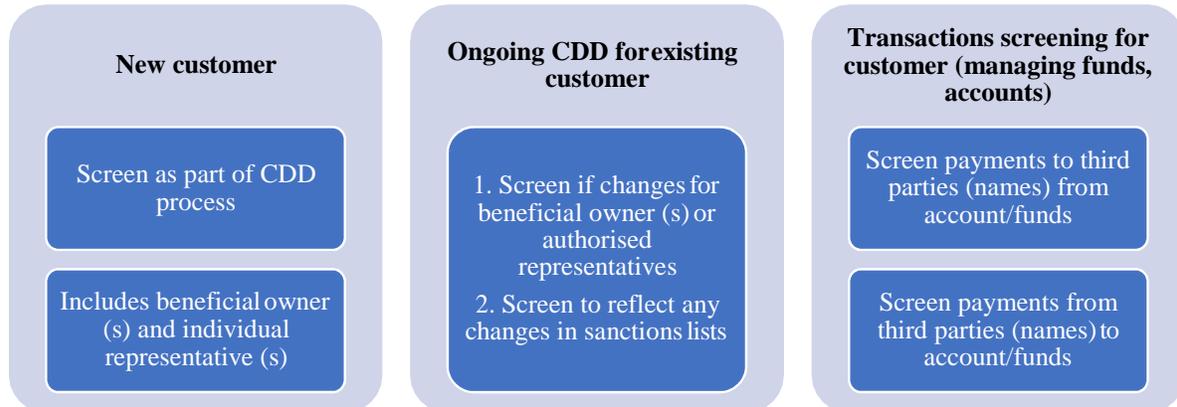
8.4 Ministry of Foreign Affairs Updates

260. To ensure prompt transmission of SROs issued by MOFA to relevant stakeholders, including accountants, the MOFA has put in place an email subscription service. Accountants supervised by the FBR and the SRBs are required to sign up for this service. For those needing or wanting to subscribe – the link to the MOFA's website is: <http://202.83.172.66/app/signup/>.

8.5 Screening new and existing customers and their transactions

261. The reporting firm should use two main screening controls to achieve their objectives: transaction screening and customer screening. Customer or name screening (including beneficial ownership and customer representative) is designed to identify persons or entities during on-boarding or ongoing CDD post on-boarding with the reporting firm. Together, transaction and customer screening are designed to form a robust set of controls for identifying sanctions targets.

262. The three main categories are shown in the chart below:

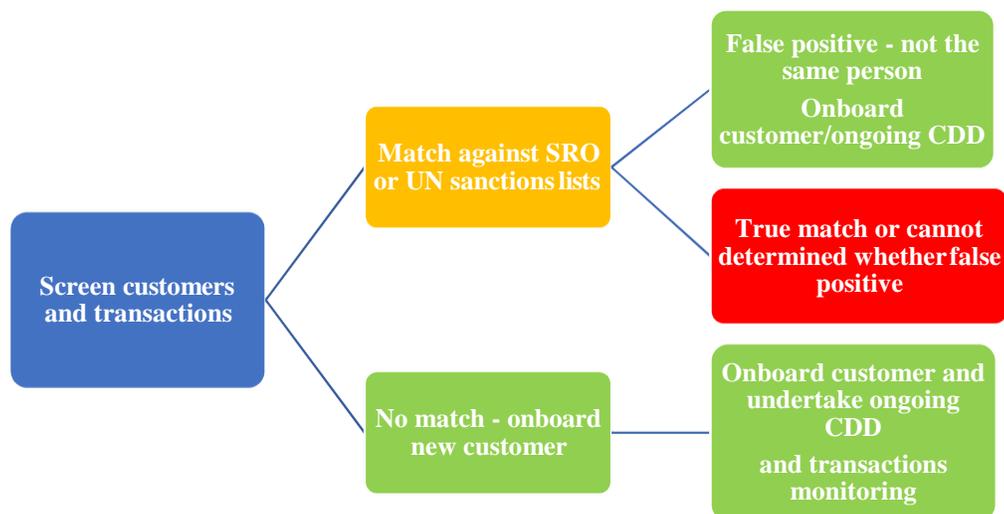


263. The following is a flowchart of the likely outcomes of the screening:

264. **Screening tools / information sources:** There are many commercial service providers that include sanctions screening as part of their risk screening of new and existing customers. It is important that the service providers include sanctions promulgated by Pakistan, which may not be on lists issued by sanction committees of the UN Security Council. These include those issued by Pakistan’s Ministry of Foreign Affairs and Ministry of Interior/(NACTA).

265. If the reporting firm does not have access to commercially available screening tools, as mentioned, the Ministry of Foreign Affairs and Ministry of Interior publishes their SROs, and also the UN Security Council sanction committees. The Ministry of Foreign Affairs also offers an email subscription service.

**Chart on Sanctions Screening for New Customer
(including beneficial owners & representative)**



266. **Search function on UN Security Council website:** The reporting firm may wish to use the search function available at the UN Security Council’s website: <https://scsanctions.un.org/search/>.

267. There is also a consolidated list of all UN Security Council sanctions available at: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

268. Please note the search function and consolidated list are not limited to just terrorism and proliferation financing – but also other UN Security Council sanctions.

269. **False positives:** If your reporting firm is undertaking the screening on a manual basis, there should be no or very few false positives. If you have a 100% match with names, date of birth and location, then it is a true match from your reporting firm’s perspective. They should be reported and transactions frozen, or customer rejected. The authorities will have more information to determine whether it is a true match from their perspective. It is not uncommon for the same name and date of birth to be identified, and then authorities conclude that it is not the person listed in the sanctions list.

270. If your reporting firm is using an automatic screening service, and depending on the sophistication of the screening service, false positives will be very common. The reason is some of those screening systems are configured to generate a “match” based purely on name or part name match, and not on all of the identifiers e.g. name, date of birth, address or geographic region. If the electronic system produces a match, the reporting firm will need to check manually whether it is a true match or a false match by reviewing all the identifiers.

271. **True match:** If a reporting entity (e.g. reporting firm) identifies a true match – either the customer, beneficial owner or representative, or payee or payer (incoming or outgoing funds transfer), the reporting firm must, under undertake the following:

New customer / updating CDD	New transaction for existing customer
1. REJECT the Customer	1. FREEZE without delay the client’s fund or block the transaction (if it is an existing customer). - This includes funds incoming into, and outgoing from the customer’s account.
2. LODGE a STR with the FMU (refer to section on STR)	
And	
3. REPORT to your SRB (ICAP / ICMA PAKISTAN) or FBR depending on who is your AML / CFT Supervisor.	

272. The reporting firm must not inform the customer, or give prior notice of the above actions to the customer, as this would be tipping off and contravene the AML / CFT legislations.

273. The reporting firm must also not return the funds to the customer or the sender. The obligation is to freeze.

9. Suspicious Transaction Report (STR)

274. The purpose of suspicious transaction reporting (STR) is to provide quality information about the suspicion of ML / TF to the FMU. Good quality STRs leads to actionable financial intelligence by law enforcement agencies to conduct successful inquiries and investigations into ML, TF and other criminal offences.

9.1 Statutory requirements under AML / CFT legislations

AML A: Under Section 7(1) of the AMLA, the reporting entity which includes the reporting firm (as per Section 2 (xxxiv) and 2 (xii) of AMLA) must file a STR to the FMU promptly for a conducted or attempted transaction if the reporting firm knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part:

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

Under Section 34(1) Disclosure of information: The directors, officers, employees and agents of any reporting entity or intermediary which report a STR or CTR pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with regulations made hereunder.

SRB AML / CFT Regulations for Reporting Firms: Section 26 merely reminds reporting firms of their STR filing obligations as prescribed by the FMU under Section 7 of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 14 merely reminds reporting firms of their filing obligations as prescribed by the FMU under Section 7 of the AMLA.

9.2 Sanctions for non-compliance

AML A: Section 71 AMLA provides that a regulator may impose monetary and administrative penalties for violations of STR filing obligations.

Under Section 33. Liability for failure to file an STR and for providing false Information.

(1) Whoever wilfully fails to comply with the STR requirement as provided in Section 7 or give false information shall be liable for imprisonment for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or both. (2) In the case of the conviction of a reporting entity, the concerned regulatory authority may also revoke its licence or registration or take such other administrative action, as it may deem appropriate.

In Section 34(2): A violation of the sub-section 34(1) [Tipping off] is a criminal offence and shall be punishable by a maximum term of five years' imprisonment or a fine which may extend to two million rupees or both.

AML / CFT Sanction Rules: Section 3 provides the powers for the FMU, SRBs and FBR to sanction reporting firms for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020

and imposed by the SRB (ICAP/ICMA PAKISTAN) according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 refers to available sanctions in the AMLA.

275. The FMU has issued a new *Guidelines for the Reporting Entities on Filing of Suspicious Transaction Report* on 5 May 2020. The link to these guidelines is:

<http://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-filing-of-Suspicious-Transaction-Reports-for-the-Reporting-Entities.pdf>.

276. The following captures the key points from the FMU’s guidelines. For more comprehensive information, the FMU guidelines should be consulted.

9.3 Reporting of STRs

277. Section 7(1) of the AMLA is quite broad – not just in the coverage of ML and TF, and conducted or attempted, but also on both transactions and activities. According to Section 7, if the reporting firm knows, suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it must report promptly its suspicions to the FMU. These are further examined below:

Table on Reporting		
Knows money laundering or terrorism financing	Has reasons to suspect	Suspects
<p>To know is a higher threshold for reporting. To know is to have objective evidence of ML or TF.</p> <p>Known or knowledge means actually knowing something to be true. The knowledge must have come to the reporting firm (or to its staff) in the course of business.</p> <p>For example, you are informed by the bank that the cheque given by your customer is a fraudulent cheque. This action constitutes an element of a fraud.</p>	<p>Reasons to suspect are an objective test to submit a STR and is a step above suspicion, meaning that there is likelihood that ML / TF offence has occurred. Your suspicion must be reasonable and, therefore, not biased or prejudiced. This means that after considering all the information and circumstances available, a reasonable person would conclude that a STR should be submitted</p> <p>This could be based on matches against AML / CFT red flags or suspicious indicators issued by the FMU.</p>	<p>There should be a reason or reasons why there is suspicion and the suspicion needs to be explained, but there is no requirement to demonstrate that the suspicion is reasonable to another person.</p>

9.4 Scope of STR reporting

278. The thresholds of knowing, reasonably suspects or suspects must be applied under Section 7 of the AMLA when the reporting firm or its staff, when engaging with a new or existing customer, or transactions, that the following has occurred or will occur:

1. Illegal activities conducted	2. Illegal activities intended for no lawful purpose	3. Terrorism financing or Terrorism	4. Avoiding STR requirements
	5. Unable to complete CDD	6. True match against Sanctions	

9.5 AML / CFT red flag indicators for accountants

279. In addition to the guidelines on STR reporting, the FMU has also issued a Circular No.04/2020 – Red Flag Indicators for Accountants:

<http://www.fmu.gov.pk/docs/Circular-for-Accountants-Red-flags.pdf>.

280. The recognition of an indicator, or better still indicators, of suspicious transaction or activity is the first step in identifying the suspicious activity. The use of suspicious indicators promulgated by the FMU will assist the reporting firm in confirming the suspicion or have reasons to suspect. These should not be exhaustive, and any useful information arising from CDD and transaction monitoring will assist in concluding that the reporting firm knows, has reasonable grounds to suspect or suspects.

9.6 Internal reporting procedures

281. There should be clear procedures within the reporting firm for determining whether any of the thresholds is met. Once that has been established, Section 7 (1) of the AMLA requires a STR to be promptly submitted to the FMU. The following is an example of internal processes for STR reporting.

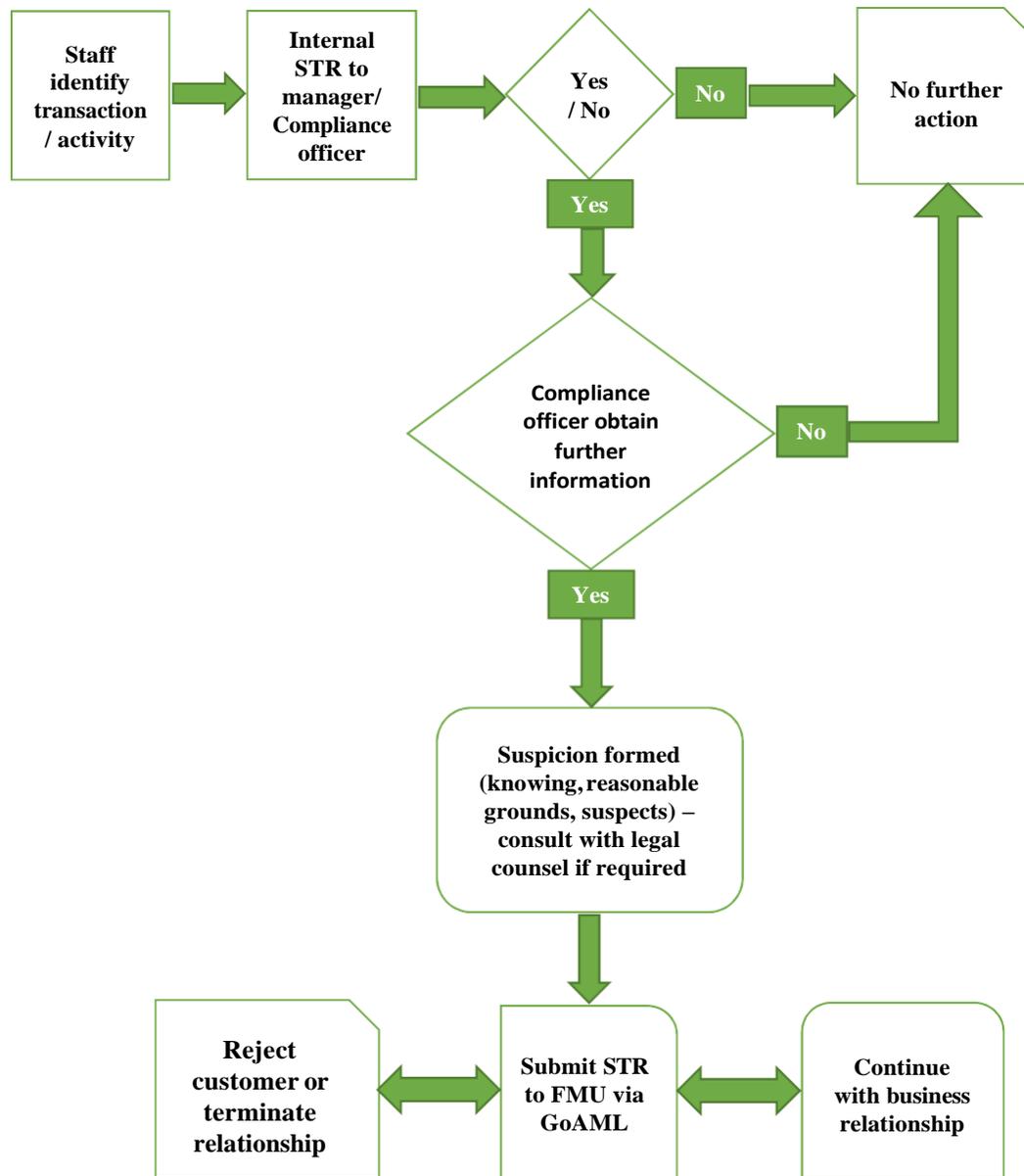
282. The relevant employee of the reporting firm should report the matter to the designated compliance officer, or any other person designated to receive information (or STR reporting authorised officer) of the reporting firm. Of course, if the reporting firm is a sole practitioner, the above steps will not apply.

283. The designated compliance officer may make an initial assessment whether the matter requires further investigation, in which as the in-house AML / CFT expert, he/she will check the activity or transactions against the suspicious indicators issued by the FMU and previous transaction or CDD records.

284. The compliance officer may want to make reasonable enquiries of other relevant employees and systems within the business, or even the prospective customer. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for STR.

285. However, prior to making further enquiries the risk of tipping-off should be considered. Accordingly, before disclosing any matter to the customer or third parties, it is fundamental to analyse and consider whether to do so is likely to constitute an offence of tipping off or prejudicing an investigation.

286. The compliance officer may also consult on a confidential basis with the reporting firm's senior management or legal counsel, but only persons designated in the AML / CFT procedures privy to such information.



9.7 Reporting to FMU via goAML

287. As required by the FMU, all STR reporting is via the FMU’s online goAML system. The link to this system is as follows: www.fmu.gov.pk/goaml

288. There are two ways to report STRs to the FMU via goAML which include:

- (i) XML (This shall NOT be mistaken as simple excel format, please consult your IT department to develop XML extractors.); and
- (ii) Web Form.

289. Reporting firms are recommended to report STRs via goAML Web Form instead of developing XML extractor through their system.

290. In order to report STR, reporting entities (including reporting firms) are, at first, required to register themselves as an Organization on goAML. The link of the goAML registration guide is provided as follows: <http://www.fmu.gov.pk/docs/RegistrationGuideFMU.pdf>.

291. The designated compliance officer is responsible for registering with the FMU and submitting any STRs. It is highly recommended that the designated compliance officer should register with goAML as soon as possible, and understand how to use the system prior to any need to submit STR via goAML. The link of the goAML reporting guide is provided as follows:

<http://www.fmu.gov.pk/docs/Financial-Monitoring-Unit-FMU-goAML-Web-Users-Guide-Updated-2020.pdf>.

9.8 Content of STR

292. There are detailed descriptions in the FMU’s *Guidelines for the Reporting Entities on Filing of Suspicious Transaction Report* issued on 5 May 2020. These are summarised below:

Reason for Reporting of STR

293. Reason for reporting is mandatory requirement for filing of STR(s). In order to ensure quality reporting, the reason(s) for suspicion should be supported with proper analysis and should contain 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 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.

Action taken by Reporting Entity

294. The reporting firm is required to provide detail of any action already taken by the firm on the customer, other than filing of the STR. Examples include:

- Freezing action
- Shared with LEA
- Rejection of customer
- Termination of customer relationship

Report indicators

295. There are varieties of indicators in goAML and the Reporting firm is required to select relevant indicator (s) while filing the STRs in goAML. The indicator(s) selected for the STR must be aligned with the reason for suspicion. The Reporting firm can select one or more indicators while reporting the STR.

296. The selection of appropriate indicator for the STR is mandatory requirement. Following are some scenarios in which single indicator is not enough and reporting entities are required to provide an additional indicator to enhance the quality of STR:

- Attempted transaction/account
- LEA Inquiry
- Adverse Media Report
- Political Exposed Person (PEP)

Contents of STRs also include the:

- to and from party information which include multiple details,
- reporting entity details (multiple fields)

9.9 Types of STRs

297. There are two types of suspicious reports which can be submitted by the reporting firm to FMU.

Report Parties (STR-A):

298. STR- A is to be reported on parties (Person, Account or Entity) involved in any suspicious activity, which does not involve transaction (s) or transmission of funds, However, STR-F should be filed in case where the transactions have been conducted.

299. While reporting of STR-A which is based on non-financial activity, please provide the suspected party details in “Person / Account / Entity. In this section reporting can add multiple other linked parties to the suspect while reporting of STR. By clicking on + Button.

Transaction (STR-F):

300. STR-F is to be reported on parties (Person, Account or Entity) for reporting of transactions and/or financial activity in which funds are involved and appears to be suspicious. An activity/event in which funds transmitted from one party to another must be reported as STR-F.

301. After filling the transactions details (i.e. Amount, Branch, Channel details) following points are to be noted:

- While reporting of STR-F which is based on any financial activity or while reporting of CTR on goAML. The reporting entities are also required to provide details of both **From Party** (Person/Account/Entity) and Destination **To Party** (Person/Account/Entity) details.
- **From Party** in goAML is the party from where funds have originated / remitted. While **To Party** in goAML is the party (Person/Account / Entity) which have received the funds or beneficiary of the funds.

9.10 Timeline for STR reporting

302. Under Section 7 (1) of the AMLA, the requirements is for the STR must be filed promptly by the reporting firm with the FMU.

9.11 No tipping off to customer

303. The reporting firm is required to ensure that a customer is not informed of the STR submission to FMU. Disclosure of such information to a customer is termed as tipping-off, and unlawful disclosure of such information is an offence under Section 34(2) of the AMLA.

9.12 Protection for reporting in good faith

304. Section 12 of the AMLA states that the reporting firm and its officer shall not be in breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FMU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

10. Currency Transaction Report (CTR)

305. The purpose of Currency Transaction Report (CTR) is to identify cash transactions (deposits and withdrawals) with the financial system, either directly or via designated non businesses and professions (DNFBPs), including by reporting firms. Similar to STRs, the aim is to provide additional information to the FMU to develop financial intelligence for law enforcement agencies to investigate potential ML, TF or other offences.

10.1 Statutory requirements under AML / CFT legislations

AMLA: Section 7 (3) specifies that every reporting entity (including reporting firms for the purpose of this Guide) should:

“(3) All CTRs shall, to the extent and in the manner prescribed by the FMU, be filed by the reporting entities with the FMU immediately, but not later than seven working days, after the respective currency transaction.”

Under Section 2(xi): Definitions in the AMLA, a CTR is defined as:

“CTR” means report on currency transactions exceeding such amount as may be specified by the National Executive Committee by notification in the official Gazette;

As per Gazette notification SRO 73 (I)/2015 dated 21-01-2015, the minimum amount for reporting a CTR to FMU is two million rupees. Accordingly, all cash-based transactions of two million rupees or above involving payment, receipt, or transfer are to be reported to FMU as CTR.

Under Section 34 (1) Disclosure of information: The directors, officers, employees and agents of any reporting entity or intermediary which report an STR or CTR pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with regulations made hereunder.

SRB AML / CFT Regulations for Reporting Firms: Section 26 merely reminds reporting firms of their filing obligations as prescribed by the FMU under Section 7 of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 14 merely reminds reporting firms of their filing obligations as prescribed by the FMU under Section 7 of the AMLA.

10.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator may impose monetary and administrative penalties for violations of CTR filing obligations.

34(2) A violation of the sub-section 34(1) (i.e. no tipping off) is a criminal offence and shall be punishable by a maximum term of five years’ imprisonment or a fine which may extend to two million rupees or both.

AML / CFT Sanction Rules: Section 3 provides the powers for the FMU, SRBs and FBR to sanction reporting firms for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by the SRB [ICAP/ICMA PAKISTAN] according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 refers to available sanctions in the AMLA.

10.3 Currency threshold for CTR

306. All cash-based transactions above PKR 2.0 million or equivalent 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 reporting of CTR, the same may be reported in the form of an STR.

307. Section 5 of AML Regulations 2015 further explains that the CTR is filed when a cash-based transaction involving payment, receipt, or transfer of an amount, as specified by the National Executive Committee, on a prescribed format.

10.4 Reporting to FMU via goAML

308. Similar to STR reporting to the FMU, all CTR reporting is via the FMU’s online goAML system – refer: <https://goamlweb.fmu.gov.pk/PRD/Home>.

309. The FMU guidance on CTR reporting is available at the following link: http://www.fmu.gov.pk/docs/CTR_Guidance_Notes.pdf.

310. The currency transaction form is available at the following links:

- http://www.fmu.gov.pk/docs/Currency_Transaction_Report_Form.pdf
- <http://www.fmu.gov.pk/reporting-forms/>

311. Unlike for STR reporting, the person submitting CTR reports need not be the designated compliance officer. Given the nature of the report, it could be someone in the finance department.

10.5 Two Types of CTRs and Contents of CTR

312. There are two types of CTR. (a) those relating to just one currency i.e. Pakistan rupees. (b) those with multiple currencies. This includes cash-based foreign currency transaction equivalent to two million rupees or above. This group involves currency exchange businesses in Pakistan.

313. As per the standardized CTR format, the REQUIRED information relates to the:

Person involved in transaction	Other individual conducting the transaction	Amount and type of transaction	Reporting firm where transaction takes place
<ul style="list-style-type: none"> •Name, address, other contact information •CNIC, NTN number •Nationality •Occupation / type of business •Relationship with reporting firm 	<ul style="list-style-type: none"> •Name, address, other contact information •CNIC, NTN number •Nationality •Occupation / type of business •Relationship with reporting firm 	<ul style="list-style-type: none"> •Date of transaction •Total cash in/ out •Type of transaction 	<ul style="list-style-type: none"> •Name •Address •Details of reporting officer

10.6 Timeline for CTR reporting

314. Under Section 7 (3) of the AMLA, the CTR must be filed by the reporting entity with the FMU *not later than seven working days*, after the respective currency transaction.

10.7 No tipping off to customer

315. The reporting firm is required to ensure that a customer is not informed of the CTR submission to the FMU as required under Section 34 (1) of the AMLA. Disclosure of such information to any person (with the exception as provided by the AMLA for government authorities upon request) is generally termed as tipping-off, and unlawful disclosure of such information is an offence under Section 34 (2) of the AMLA.

11. Record Keeping

316. Reporting firms are required to maintain records either in hard or digital form. The purpose is multiple, including for the reporting firm’s own benefit, as evidence to authorities that the reporting firm is implementing the requirements of the AML / CFT legislations e.g. onsite supervision, and in the event of an investigation by law enforcement authorities. The latter could be in the event of a search warrant or production order, or additional information requested by the FMU in response to a submitted STR or CTR.

11.1 Statutory requirements under AML / CFT legislations

AMLA: The AMLA defines record as follows:

Section 2. Definitions —

(xxxii) “record” includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed.

The AMLA Section 7C states the general record keeping requirements:

“Every reporting entity shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through CDD and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship.”

Further, Section 7(4) requires the record to be maintained for a period of 10 years for submitted STRs and CTRs after reporting of the transaction:

“Every reporting entity shall keep and maintain all record related to Suspicious Transaction Reports and CTRs filed by it for a period of at least ten years after reporting of transaction under sub-sections (1), (2) and (3).”

SRB AML / CFT Regulations for Reporting Firms: Section 29 -31 requires reporting firms to maintain the required records as stated in Section 7C of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 6 requires reporting firms to maintain the required records as stated in Section 7C of the AMLA.

AML / CFT Sanction Rules: Section 3 provides the powers for the Regulatory Authorities to sanction REAs for non-compliance pursuant to Section 7 of the AMLA, AML / CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts. Sections 7 and 8 outlines the process for issuing sanctions in writing and the appeal process, respectively.

11.2 Sanctions for non-compliance

AMLA: Section 7I of AMLA provides that a regulator may impose monetary and administrative penalties for violations of any of the provisions of Sections 7(1), 7(3) to 7(6) and 7A to 7H.

SRB AML / CFT Regulations for Reporting Firms: Section 32 states that any violation of any provision of these regulations will be subject to sanctions in accordance with the AML / CFT Sanctions Rules, 2020 and imposed by the SRB [ICAP/ICMA PAKISTAN] according to Clause (h) of Sub-section (2) of Section 6A of the AMLA.

FBR AML / CFT Regulations for DNFBPs: Section 16 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under AMLA.

11.3 Table on record keeping requirements

317. The following Table summarises the key requirements.

Record keeping requirements	
Record Type	Retention period
1.CDD documents (Section 7C of AMLA) (Section 29 of SRB AML / CFT Regulations for Reporting Firms and Section 6 of the FBR AML / CFT Regulations for DNFBPs)	<ul style="list-style-type: none"> • 5 years after the end of the customer relationship
2.Transaction records (Section 7C of AMLA) (Section 29 of SRB AML / CFT Regulations for Reporting Firms and Section 6 of the FBR AML / CFT Regulations for DNFBPs)	<ul style="list-style-type: none"> • 5 years after completion of transaction
3.STR and CTR records – including CDD and transaction records related to the STR or CTR (Section 7 (4) of AMLA)	<ul style="list-style-type: none"> • 10 years after submission

318. While not explicitly stated, the reporting firm should keep records for 5 years of enterprise risk assessments, procedures and AML / CFT training records including staff attendance.

Annex 1 – Customer Risk Assessment Template

CUSTOMER RISK ASSESSMENT TEMPLATE

Explanatory Notes:

1. This is an example template for customer risk assessment for voluntary use, or the reporting firm may wish to amend this template to suit its own circumstances.
2. The following factors should be considered by the reporting firm in carrying out its risk assessment for new customers. The list is not exhaustive, and the reporting firm may consider additional factors relevant to their working environment.
3. If the response to any of the questions listed in Section 1.1 is “**YES**”, this means that the Reporting firm must **NOT** establish business relationship with the customer.
4. If the response to any of the questions listed in Sections 1.2 - 1.6 is “**YES**”, this accounts for the indicators of higher risk factors. When there are multiple “**YES**” responses in the aforementioned sections, or yes to a Politically Exposed Person (PEP), the reporting firm is required to conduct enhanced customer due diligence which involves approval by senior management of the reporting firm prior to accepting the new customer. The concerned staff member should also consult with the designated Compliance Officer with regards to the risk factors identified.
5. Please note that this template is for risk assessment only. There is a separate template for customer due diligence which contains mandatory requirements. After the completion of CDD, the reporting firm can then decide whether to accept the new customer or not.

SECTION 1.1: PROHIBITED PERSONS/ORGANISATIONS SCREENING

(refer point # 3 of the explanatory notes)

	Response	
<p>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?</p> <p>(a) The “Lists of Proscribed Individuals and Entities” issued by the Ministry of Interior available on NACTA website;</p> <p>(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.</p> <p>UN Sanctions:</p> <p>https://www.un.org/securitycouncil/content/un-sc-consolidated-list https://scsanctions.un.org/search/</p> <p>Ministry of Foreign Affairs:</p> <p>http://mofa.gov.pk/unsc-sanctions/ http://www.secddiv.gov.pk/page/sro-unscr-sanctions</p>	YES	NO

<p>Ministry of Interior/NACTA</p> <p>https://nacta.gov.pk/proscribed-organizations-3/ https://nacta.gov.pk/pp/ https://nfs.punjab.gov.pk/</p> <p><i>Note: If there is a true match, the reporting firm must also submit a Suspicious Transaction (STR) 7 days of identifying the match and other authorities.</i></p>		
<p>SECTION 1.2: CUSTOMER’S RISK FACTORS <i>(refer point # 4 of the explanatory notes)</i></p>		
	Response	
<p>Is the customer or its beneficial owner a Politically Exposed Person (PEP), family member of a PEP or close associate of a PEP?</p> <p><i>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 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.</i></p>	YES	NO
<p>The customer or beneficial owners is non-resident in Pakistan?</p>	YES	NO
<p>The customer or potential customer is a Non-Government Organization (NGO), Not for Profit Organisation (NPO) or charity?</p> <p><i>Note: The list of registered charitable organizations / NGOs / NPOs can be obtained from http://pcp.org.pk/pagestyle.php</i></p>	YES	NO
<p>Business that is cash-intensive?</p>	YES	NO
<p>Is the customer in a high – risk industry?</p> <p><i>Note: High risk industry includes (but not limited to) following businesses;</i></p> <ul style="list-style-type: none"> - Businesses dealing with precious metals (gold, silver, diamond and 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
<p>Is the customer a shell company, especially in cases where there is foreign ownership which is spread across jurisdictions?</p> <p><i>Note: Shell Company means an inactive company used as a vehicle for various financial maneuvers or kept dormant for future use in some other capacity.</i></p>	YES	NO
<p>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?</p> <p><i>Note: The above excludes publicly listed companies in Pakistan and FATF member countries, or other countries with equivalent transparency standards for such countries.</i></p>	YES	NO
<p>The business relationship will be conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting firm and the customer), non-resident customers?</p>	YES	NO
<p>The customer is a legal persons or arrangement that is a personal asset-holding vehicle?</p>	YES	NO

SECTION 1.3: COUNTRY / GEOGRAPHICAL RISK FACTORS		
<i>(refer point # 4 of the explanatory notes)</i>		
	Response	
<p>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?</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> - For countries in black list, please refer https://www.fatf-gafi.org/countries/#high-risk - For countries in grey list, please refer https://www.fatf-gafi.org/countries/#other-monitored-jurisdictions 	YES	NO
<p>Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations?</p> <p>United Nations: https://scsanctions.un.org/search/</p>	YES	NO
<p>Countries identified by credible sources as having significant levels of corruption or other criminal activity?</p> <p>Transparency International: https://www.transparency.org/en/cpi/2019/results</p>	YES	NO
<p>Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country?</p> <p>Institute of Economics and Peace: http://economicsandpeace.org/Global Terrorism Index</p>	YES	NO
<p>Does the customer, beneficial owner or person acting on behalf of the customer have dealings in high risk geographic regions, including Pakistan as identified in the National Risk Assessment 2019?</p> <p><i>Note: The high risk areas / jurisdictions includes western borders / FATA / Southern Punjab and the eastern border.</i></p>	YES	NO
<p>Countries known for high levels of financial secrecy or with low tax rates?</p> <p>Tax Justice Network: https://fsi.taxjustice.net/en/</p>	YES	NO
SECTION 1.4: SERVICES / PRODUCTS RISK FACTORS		
<i>(refer point # 4 of the explanatory notes)</i>		
	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 would involve receipt of funds from unknown or un-associated third parties for services and / or transactions provided by the customer?	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 on behalf of the customer?	YES	NO

SECTION 1.5: DELIVERY CHANNEL RISK FACTORS <i>(refer point # 4 of the explanatory notes)</i>		
		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 <i>(refer point # 4 of the explanatory notes)</i>		
		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
<input type="checkbox"/> Lower Risk → Simplified Due Diligence <input type="checkbox"/> Medium Risk → Standard Due Diligence <input type="checkbox"/> Higher 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:

Name: _____

Designation: _____

Date: _____

Signature: _____

Approved by:

Name: _____

Designation: _____

Date: _____

Signature: _____

Annex 2 - Customer Due Diligence Form – Template (Company)

CUSTOMER FORM (COMPANY)

EXPLANATORY NOTE – All information and documents requested in this form are required to be provided by any new Client / Customer.

The information and documents are required in order to comply with Pakistan’s laws and regulations on Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT), particularly the:

- Anti- Money Laundering Law
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

[Note: Your reporting firm may select the applicable AML / CFT regulations depending on which authority or body is your AML / CFT supervisor, and delete the other two AML / CFT regulations.]

The information collected is to be used for compliance with the AML / CFT legislations. They remain confidential, unless formally requested by government authorities or government designated self-regulatory bodies pursuant to AML / CFT legislations.

PART 1. LEGAL IDENTIFICATION INFORMATION	VERIFICATION DOCUMENTS
Full Legal Name:	Certificate of Incorporation
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	VERIFICATION DOCUMENTS
<p>1. Shareholders:</p> <p>e.g. Names of individuals (natural persons) shareholders holding 25% or above ownership</p> <p>Note: This includes where the customer is owned by one or more companies.</p>	<p>Note for staff: Documents required from customer: [these documents may be obtained from the network firm, if available]</p> <p>Details of company:</p> <p>1. SECP registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017), as applicable;</p>
<p>2. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g.</p> <p>- appoint or remove the majority of the board of directors, or its chair, or CEO of the company:</p>	<p>2. List of directors, members and shareholders required to be filed under the Companies Act, 2017 (XIX of 2017), as applicable</p> <p>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</p> <p>4. Articles of Association/Memorandum of Association</p>
<p>3. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g.</p> <p>- personal connections to persons in positions described above or that possess ownership</p> <p>- close and intimate family relationships</p> <p>- historical or contractual associations if a company defaults on certain payments</p>	<p>Details of individuals (beneficial owners):</p> <p>Originals or certified true copies of:</p> <p>1. Residents: CNICs/ Smart National Identity Card (SNIC) issued by NADRA</p> <p>2. Non Residents:</p> <p>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</p>
<p>4. Senior managing official: Where no natural person is identified under 1 to 3 above after reasonable measures have been made</p> <p>- the identity of the relevant natural person who holds the position of senior managing official.</p>	<p>Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistanis who have given up Pakistan nationality; or</p> <p>Form B or Juvenile card issued by NADRA to children under the age of 18 years; or</p> <p>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.</p> <p>Note: If only photocopies and not originals or certified true copies provided of the above, electronic verification</p>

	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 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
2. Are you a family member of the above?	Yes	No
3. Are you a close associate of the above?	Yes	No
PART 3: 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 4: 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 5: INDIVIDUAL 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)	

<p>Address:</p>	<p>Incorporation certificate with physical address; or</p> <p>Utility or telephone bill with physical address; or</p> <p>Other document with evidence of physical address</p>
<p>Relationship to customer:</p> <p>e.g. company director, employee or lawyer/accountant.</p>	<p>Attach original of official company letter authorising individual to enter into contractual relations with reporting firm on behalf of the customer e.g. from the governing body/board if not a company director.</p>
<p>PART 6: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION</p>	
<p>1. Certificate of Incorporation</p>	
<p>2. SECP registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017)</p>	
<p>3. List of directors required to be filed under the Companies Act, 2017 (XIX of 2017)</p>	
<p>4. Register of Beneficial Ownership maintained by the Company</p>	
<p>5. Article of Association, Memorandum of Association</p>	
<p>6. Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA of all directors and beneficial owners</p>	
<p>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</p>	
<p>8. Utility statement, telephone account statement etc. with physical address</p>	
<p>9. If applicable, letter authorising individual to act on behalf of the customer</p>	
<p>Note: If only photocopies and not originals provided of the above, electronic verification is required of the authenticity and information contained in the photocopies.</p>	

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.

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

Annex 3 - Customer Due Diligence Form – Template (Individual / Sole Proprietor)

CUSTOMER FORM (INDIVIDUAL/SOLE PROPRIETOR)

EXPLANATORY NOTE – All information and documents requested in this form are required to be provided by any new Client / Customer.

The information and documents are required in order to comply with Pakistan’s laws and regulations on Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT), particularly the:

- Anti- Money Laundering Law
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

[Note: Your reporting firm may select the applicable AML / CFT regulations depending on which authority or body is your AML / CFT supervisor, and delete the other two AML / CFT regulations.]

The information collected is to be used for compliance with the AML / CFT legislations. They remain confidential, unless formally requested by government authorities or government designated self-regulatory bodies pursuant to AML / CFT legislations.

PART 1. BASIC IDENTIFICATION INFORMATION	VERIFICATION DOCUMENTS
Full Legal Name (as per ID document):	<p>Residents:</p> <p>CNICs/ Smart National Identity Card (SNIC) issued by NADRA</p> <p>Non Residents:</p> <p>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</p> <p>Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistanis who have given up Pakistan nationality; or</p> <p>Form B or Juvenile card issued by NADRA to children under the age of 18 years; or</p>

	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.
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: DETAILS ON THE BUSINESS	
VERIFICATION DOCUMENTS	
Business Name:	Certificate of Registration
Business Address:	Certificate of Registration Utility statement with address, telephone account statement with address, etc.
Registration Number:	Certificate of Registration
Please provide details of the industry and business (e.g. products / services)	N/A
Does the company have operations in other geographic regions in Pakistan? If the above is “Yes”, please provide the names of those regions?	N/A
Which are the primary countries in which the business has dealings with, if any?	N/A
PART 4: SOURCE OF FUNDS OR WEALTH	
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 reporting firm 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 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:
Date:
Location:

Annex 4 - Customer Due Diligence Form – Template (Trust)

CUSTOMER FORM (TRUST)

EXPLANATORY NOTE – All information and documents requested in this form are required to be provided by any new Client / Customer.

The information and documents are required in order to comply with Pakistan’s laws and regulations on Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT), particularly the:

- Anti- Money Laundering Law
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Chartered Accountants Reporting Firms
- Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants Reporting Firms
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

[Note: Your reporting firm may select the applicable AML / CFT regulations depending on which authority or body is your AML / CFT supervisor, and delete the other two AML / CFT regulations.]

The information collected is to be used for compliance with the AML / CFT legislations. They remain confidential, unless formally requested by government authorities or government designated self-regulatory bodies pursuant to AML / CFT legislations.

PART 1. BASIC IDENTIFICATION INFORMATION	VERIFICATION DOCUMENTS
Full Legal Name of Trust:	Trust deed / agreement
Date of Trust Formation:	
Physical Address of Trust:	
Trustee/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 settlor
Name of Protector, if any:	Trust deed CNIC # and address of the protector
Beneficiaries	
Names of all beneficiaries with 10% or above share:	Trust deed CNIC # and address for each beneficiary
If a beneficiary is a corporate beneficiary, the name of the individual authorised to represent the corporate beneficiary:	Trust deed Certificate of incorporation CNIC # and address for each authorised representative
If a beneficiary is another trust, the full details of that trust (as required in this form).	Trust deed and information required on the trust
If more than 10 beneficiary, or beneficiaries are not names, the names of the different groups of beneficiaries e.g. grandchildren, children, groups benefiting from the charity etc.	Trust deed Memorandum of Association and Rules & Regulations of your Trust.
Contact details	
Landline Number:	N/A
Email Address:	N/A
PART 2: POLITICALLY EXPOSED PERSON	
Are you or any beneficial owners entrusted with a prominent public function by the State of Pakistan, a foreign country or an international organization and includes Heads of state or government, and members and senior officials of legislature, judiciary, executive, military and regulatory authorities, and senior executives of corporations, departments or bodies that are owned or controlled by the state?	Yes/No
Are you or a beneficial owner a family member of the above?	Yes/No
Are you or a beneficial owner a close associate of the above?	Yes/No
PART 3: DETAILS ON THE BUSINESS	
Please provide details of the industry and business (e.g. products / services):	
Does the company have operations in other geographic regions in Pakistan? If the above is “Yes”, please provide the names of those regions?	

Which are the primary countries in which the business has dealings with, if any?	
PART 4: SOURCE OF INCOME OR WEALTH	
What is the main source of income of the business?	
Income last financial year?	
Assets held by the customer?	

PART 5: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION
Certificate of Registration
Trust deed/agreement
Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA of trustee, settlor or beneficiaries
If non-resident, original or certified true copy of foreign passport of trustee, settlor 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:
Date:
Location:

Appendix A – Useful web links to publications / documents / information

Document	Web links
1. AMLA 2010	http://AMLA amended September 2020.pdf
2. Anti – Terrorism Act 1997	http://www.fmu.gov.pk/wp-content/uploads/2020/04/The-Anti-Terrorism-Act-1997-as-amended-up-to-Feb-2017-1.pdf
3. AML Regulations 2015	http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf
4. SRB AML / CFT Regulations for Reporting Firms	https://AML / CFT Regulations for ICAP Reporting firms.pdf https://AML / CFT Regulations for ICMA Reporting firms.pdf
5. FBR AML / CFT Regulations for DNFBPs	http://FBR AML / CFT Regulations for DNFBPs.pdf
6. Circular for Accountants – Red Flags	http://www.fmu.gov.pk/docs/Circular-for-Accountants-Red-flags.pdf http://www.fmu.gov.pk/docs/Red-Flag-Indicators-for-Accountants-final.pdf
7. Guidelines on filing of Suspicious Transaction Reports for the Reporting Entities	http://www.fmu.gov.pk/wp-content/uploads/2020/05/Circular-02-of-2020-.pdf http://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-filing-of-Suspicious-Transaction-Reports-for-the-Reporting-Entities.pdf
8. Guidelines on Reporting of Suspicious Transaction Reports (STRs) on Designated /Proscribed Individuals / Entities and their Associates	http://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-Reporting-of-Suspicious-Transaction-Reports-STRs-on-Designated-Proscribed-Individuals-Entities-and-their-Associates.pdf
9. Financial Monitoring Unit (FMU) goAML Web User’s Guide For Stakeholders	http://www.fmu.gov.pk/docs/goAML-Userguide-for-Stakeholders-LEAs-Updated-Version.pdf
10. FMU reporting forms	http://www.fmu.gov.pk/reporting-forms/
11. FAQs on Targeted Financial Sanctions under UN Security Council Resolutions	https://www.icap.org.pk/files/per/aml/FAQs-on-TFS-Obligations.pdf https://www.icmap.com.pk/downloads/FAQs on TFS Obligations ICM APakistan.pdf
12. Guidance on TFS	https://www.icap.org.pk/files/per/aml/Guidelines-TargetedFinancialSanctions.pdf https://www.icmap.com.pk/News Pdf/GuidelinesTargetedFinancialSanctions TFS.pdf
13. Introducing Guidelines for DNFBPs on Targeted Financial Sanctions under UN Security Council Resolutions – FBR	https://download1.fbr.gov.pk/Docs/20201021610362290TargetedFinancialSanctionsStatutoryRegulation.pdf
14. Guidelines Implementations of the UN Security Council Resolution 1267	http://www.fmu.gov.pk/wp-content/uploads/2019/08/1267-Guidelines.pdf
15. Guidelines Notes on 1267	http://www.fmu.gov.pk/wp-content/uploads/2019/08/Guidance_Note_UNSCR_1267.pdf
16. NACTA GUIDELINES ON UN Security Council Resolution 1373	https://nacta.gov.pk/GUIDELINES-ON-ACTIONS-TO-BE-TAKEN-BY-COMPETENT-AUTHORITIES-FOR-IMPLEMENTATION-OF-UNITED-NATIONS-SECURITY-COUNCIL-RESOLUTION-NO.-1373-without-covering-

17. National Counter Terrorism Authority (NACTA) 'prescribed persons'	https://nacta.gov.pk/proscribed-organizations/ https://nacta.gov.pk/pp/
18. Ministry of Foreign Affairs SROs for UN Security Council sanctions	http://mofa.gov.pk/unsc-sanctions/
19. UN Security Council AI-Qaida/Da'esh Sanctions	https://www.un.org/sc/suborg/en/sanctions/1267/ai_sanctions_list/summaries
20. UN Council Taliban Sanctions	https://www.un.org/sc/suborg/en/sanctions/1988/materials/summaries
21. Ministry of Foreign Affairs Strategic Export Control Division (SECDIV) SROs	http://www.secdiv.gov.pk/page/sro-unscr-sanctions
22. SECP Circular 16 of 2018 on Register of Ultimate Beneficial Ownership by the Companies	https://www.secp.gov.pk/document/circular-no-16-of-2018-register-of-ultimate-beneficial-ownership
23. UN Security Council DPRK Sanctions	https://www.un.org/securitycouncil/sanctions/1718/materials
24. UN Security Council Iran Sanctions	https://www.un.org/securitycouncil/content/2231/background
25. FATF	http://www.fatf-gafi.org/
26. APG	http://www.apgml.org/