Federal Board of Revenue

Anti-Money Laundering and Counter Financing of Terrorism

Guidelines for Dealers in Precious Metals and Stones

January 2021

Table of Contents

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, 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 FBR 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.

Acronyms/terms

AMLA	Anti-Money Laundering Act 2010
AML	Anti-Money Laundering
AML/CFT legislations	AMLA 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
AML/CFT Sanction Rules	AML/CFT Sanction Rules 2020 SRO NO 950(I)/2020

ATA	Anti-Terrorism Act 1997
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
CTR	Currency Transaction Report
Counter Measures for High Risk Jurisdiction Rules	Counter Measures for High Risk Jurisdiction Rules, 2020
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 Dealers in Precious Metals and Stones
ML	Money Laundering
PF	Financing of proliferation
NACTA	National Counter Terrorism Authority
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
SBP	State Bank of Pakistan
SECP	Securities and Exchange Commission of Pakistan
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 ***Federal Board of Revenue (FBR) Anti-Money Laundering and Counter Financing of Terrorism* (AML/CFT) - *Guidelines for Dealers in Precious Stones and Metals ("The Guidelines")*** is to provide guidance to **Dealers in Precious Stones and Metals (DPMS)** in implementing and complying with requirements in AML/CFT legislations.

1.2 Target audience

2. The focus of the Guidelines is on DPMS engaged in the buying and/or selling of precious stones and metals as defined in the:

   - Anti Money Laundering Act (AMLA), Section 2.Definitions (xii) (b)

     dealers in precious metals and precious stones, including jewellers and gem dealers, when performing the prescribed activities in the prescribed circumstances and manner;

   - FBR AML/CFT Regulations for DNFBPs in Section 2.Definitions (1) (k):

     "Jeweler" means a person who is a bullion dealer or engaged in sale of jewelry, precious stones and metals including all articles made wholly or mainly of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semi-precious stones or pearls, when they engage in a cash transaction with a customer of a value equivalent to two Million rupees or more.

3. All DPMS should review Section 4 in the Guidelines to determine whether they (i) meet the definition of a DPMS and (ii) engage in cash transactions with customers equal or above the cash threshold of PKR 2 million.

4. If they are subject to AML/CFT, Sections 5 to 11 of the Guidelines explain the AML/CFT requirements and how to implement them.

5. You do not need to read the whole Guidelines, but you should read and understand the sections that are applicable to your DPMS. In most instances, all DPMS staff involve in sales will need to read and understand the sections on risk assessment, customer due diligence (CDD), targeted financial sanctions, Suspicious Transaction Report (STR), Currency Transaction Report (CTR) and record keeping.

1.3 Scope and terminology

6. The Guidelines are focused on AML/CFT measures such as risk assessment, AML/CFT programme, CDD, beneficial ownership, politically exposed persons, reliance on third party, targeted financial sanctions, STR, CTR and record keeping. Those measures are further explained in the Guidelines.

7. The Guidelines do not add new regulatory requirements upon DPMS.

8. 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.

9. The main law and regulations referred to in the Guidelines are:

- Anti-Money Laundering Act (AMLA)
- 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)

10. The Guidelines use the term "Customer" rather than "client".

11. 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.

12. The term "jeweller" used in the Guidelines is synonymous with "DPMS" and are used interchangeably.

13. The term "DPMS" In the Guidelines refer to both the singular and plural.

1.4 Structure

14. 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 DPMS;
4. **Specified Services Subject to AML / CFT** – Describes the AML / CFT requirements applicable to DPMS engaged in the specified activities / services;
5. **Risk Assessment and Risk Mitigation** – Explains the rationale and purpose of risk based approach for AML / CFT system and procedures, summarizes the categories of ML /TF risks and outlines the risk assessment methodology for DPMS;
6. **AML/CFT Programme** – Explains the key components of an AML/CFT programme including written policies and procedures, compliance officer, staff onboarding, training, monitoring and interdependent audit;
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 obligations of STR reporting to the Financial Management Unit (FMU), the possible scenarios triggering such reporting and the procedures for reporting;

10. **Currency Transaction Report (CTR)** – Outlines the obligations of filing CTRs to the FMU;

11. **Record Keeping** – Describes the requirements for the AML/CFT related record maintenance and retention.

15. It is recognised that a "one-size-fits-all approach" does not work well for all DPMS. 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 DPMS. The aim is to reduce the regulatory burden on less wellresourced, or single person DPMS 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 DPMS required to comply with AML / CFT?

16. Precious stones and metals may be abused by criminals and terrorists because of a number of factors. They can be of very high value, but still very small and therefore very easy to carry, transport and conceal. Transferring ownership does not required any formal registration process unlike for real estate, motor vehicle or share ownership. The holder of the precious stone and metal is the owner and can be held can be held anonymously without a need for records to be kept. In terms of gold, it can be considered as a universally accepted currency and therefore, investing in gold to launder illegal earnings would be easy as well as profitable.

2.2 Financial Action Task Force (FATF)

17. 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 Asia/Pacific Group on Money Laundering (APG)

18. 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/.)

19. 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/.

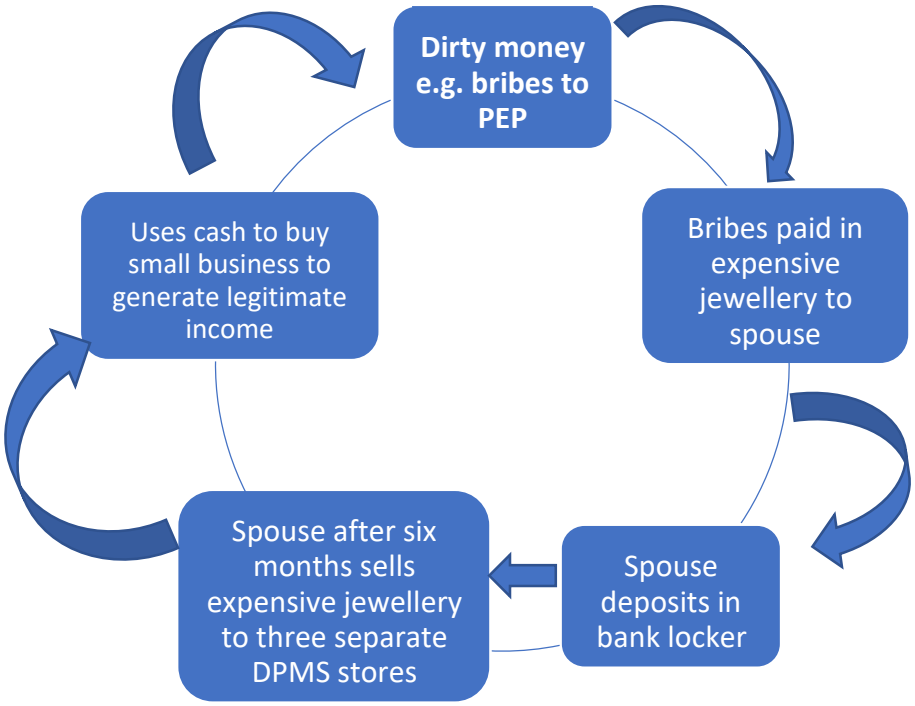
2.4 The FATF grey list

20. 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.

2.5 Money laundering

21. 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.

22. 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.



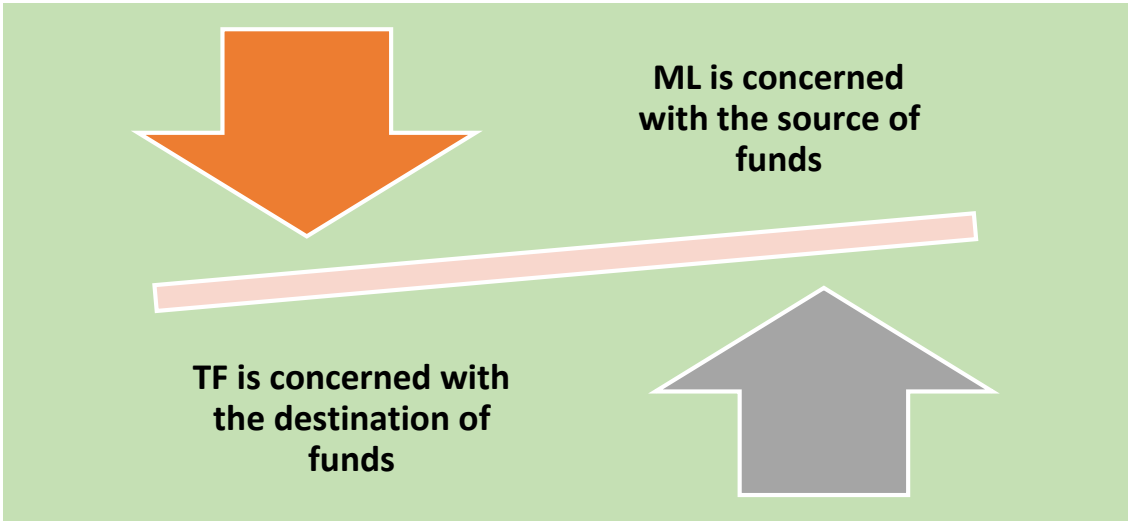
2.6 Terrorism financing

23. 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.

2.7 Differences between money laundering and terrorism financing

24. 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 AML/CFT Regulatory Regime

25. This and the next section of the Guidelines should be read by all DPMS to assist them in ascertaining whether they meet the definition of a DPMS and whether they engage in activities or provide services subject to AML/CFT.

3.1 AML/CFT regulatory regime in Pakistan

26. As of October 2020, the relevant obligations applicable to DPMS are contained in the following laws and regulations:

- The AMLA 2020
- FBR AML/CFT Regulations for DNFBPs
- AML/CFT Sanctions Rules
- 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 Schedule-1 and Proscribed individuals under Schedule-4 of ATA

Law and enforceable means

AMLA (as amended September 2020) **Covers the following:** - Risk assessment and mitigation - Compliance program - Record keeping - CDD - Reliance on third parties - Targeted financial sanctions - Reporting of STR and CTR - Monitoring - Sanctions
FBR AML/CFT Regulations for DNFBPs **Cover the following:** - 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
ATA **United Nations Security Council (Freezing and Seizure) Order, 2019** **UN SROs (Security Council) Act 1948**
- Cover targeted financial sanctions (TFS) for TF and PF
Ministry of Interior/ (NACTA) Proscribed Organizations/Persons under ATA - Cover targeted financial sanctions (TFS) for TF
AML/CFT Sanction Rules 2020 SRO NO 950(I)/2020 (AML/CFT Sanctions Rules) - **Covers measures in the FBR AML/CFT Regulations for DNFBPs**
Counter Measures for High Risk Jurisdiction Rules, 2020 (Counter Measures for High Risk Jurisdiction Rules) - Covers circumstances when the FBR issues instructions to DPMS to take action on certain categories of customers

27. For ease of reference, the laws and regulations applicable to DPMS will be generically referred to as "AML/CFT legislations", unless there is a need to reference a specific law or regulation.

28. For a copy of the actual laws, regulations and guidelines, visit the websites of the following competent authorities. For REAs, the FBR AML/CFT Regulations for DNFBPs and the AMLA are the

most relevant. Links to other important AML/CFT legislations (including regulations and rules) are also provided below:

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

29. **Appendix A** provides a list of useful weblinks to other AML/CFT legislation and guidance documents.

3.2 Government authorities responsible for DPMS

30. The FBR, as mentioned, is the designated AML/CFT Regulatory Authority for DPMS. This includes DPMS that are private sector businesses and DPMS that are government authorities.

31. The Financial Monitoring Unit (FMU) is the Financial Intelligence Unit of Pakistan. It is mandated to receive and analyze STRs and CTRs. All DPMS must submit STRs and CTRs to the FMU.

32. The Ministry of Foreign Affairs is responsible for issuing SROs on 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 these decisions of the Security Council.

33. The Ministry of Interior/NACTA issues Proscribed Organizations and Persons under the ATA for domestic designations on terrorism and TF.

4. Dealers in Precious Stones and Metals (DPSM) Subject to AML/CFT

34. The specified activities subject to AML/CFT requirements are clearly explained in the FBR AML/CFT Regulations for DNFBPs. Whether your business is subject to AML/CFT depends on whether your business meets the following two criteria:

i. *Your business engages in the selling or buying of articles made wholly or mainly of precious stones and metals; and*
ii. *Your business engages in a cash transaction (includes bearer negotiable instruments) with a customer of a value equivalent to PKR 2 million or more.*

35. In general, your business must meet both criteria to be classified as a DPMS and subject to AML/CFT obligations. These criteria are further explained in this Section of the Guidelines.

4.1 Businesses subject to AML/CFT

36. There is a definition of a DPMS under the AMLA, as extracted below:

AMLA, Section 2.Definitions (xii) (b)

dealers in precious metals and precious stones, including jewellers and gem dealers, when performing the prescribed activities in the prescribed circumstances and manner;

37. The term DPMS is further defined in the definition of jeweller in the FBR AML/CFT Regulations for DNFBPs.

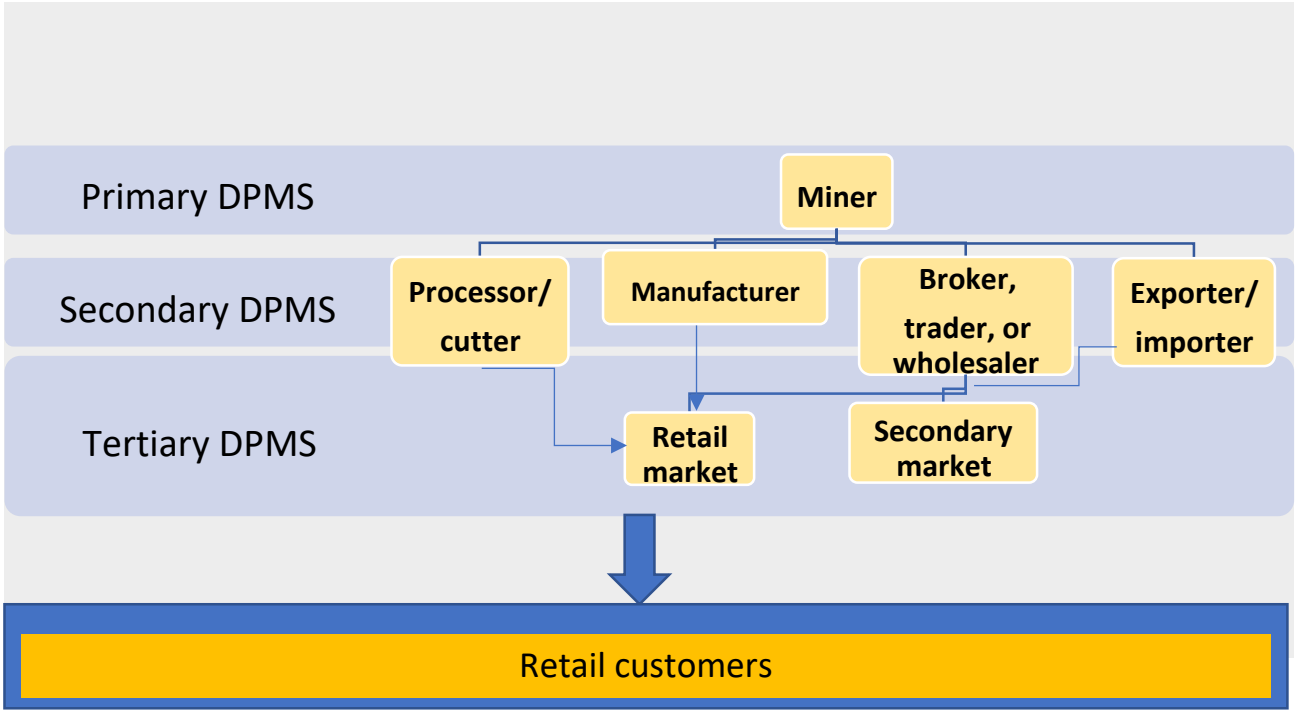
- FBR AML/CFT Regulations for DNFBPs in Section 2.Definitions (1) (k):

"Jeweler" means a person who is a bullion dealer or engaged in sale of jewelry, precious stones and metals including all articles made wholly or mainly of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semi-precious stones or pearls, when they engage in a cash transaction with a customer of a value equivalent to two Million rupees or more.

38. The terms DPMS and jeweller can be considered synonymous. The definition encompasses all stages of the DPMS supply chain, as listed below:

- those who produce precious stones or precious metals at mining operations
- intermediate buyers and brokers
- traders, exporters/importers
- precious stone cutters and polishers and precious metal refiners
- jewellery manufacturers who use precious metals and precious stones
- retail sales to the public, and
- retail secondary markets

39. The diagram below shows the DPMS supply chain:



40. The fact that your business is engaged in the above activities does not automatically mean your business is subject to AML/CFT. Your business also needs to sell or buy items *made **wholly or mainly** of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semi-precious stones or pearls.*

41. Your business also needs to engage in a cash transaction with a customer of a value equivalent to PKR 2 million or more to be subject to AML/CFT, which is the topic of the next sub-section.

4.2 Sales transactions subject to AML/CFT

42. Your business must also be engaged in a covered sales transaction (cash and bearer negotiable instruments) of PKR 2 million or more. This activities based definition means that if you are a retail merchant selling or buying jewellery e.g. rings, bracelets, necklaces and other bodily adornments, you may not be a DPMS in one year or one month, but if you start selling or buying such items over the PKR 2 million threshold, in subsequent years or months, you would be subject to AML/CFT.

43. The interpretation of the PKR 2 million threshold captures a cash transaction below the threshold amount, if the cash transaction is below PKR 2 million but is part of a series of transactions related to the purchase of the same item or items totalling PKR 2 million or above.

44. The following are examples of covered sales transactions subject to the FBR AML/CFT Regulations for DNFBPs.

Examples of covered sales transactions subject to AML/CFT

Example 1- Commercial purchase from another DPMS: A cutting and polishing firm wishes to buy a consignment of gems from a local wholesaler. The two parties arrive at a final negotiated price of PKR 10 million which includes payment in the form of a physical cash deposit of PKR 1 million, with the balance covered through several cheques totalling PKR 9 million. Although the cash deposit is less than the PKR 2 million, the cheques are bearer negotiable instruments which are considered to be cash equivalents. This is a covered transaction.

Example 2- Selling to another DPMS: A jewellery manufacturer sells a finished item worth PKR 3 million to an upmarket retail store for wealthy customers. The manufacturer receives cash payment of PKR 3 million. This is a covered transaction.

Example 3 – Selling to retail customer with linked transactions: A husband and wife come into a store and choose a jewellery set consisting of four items totalling PKR 3 million. The husband wants to pay the amount in cash with a 50% deposit of PKR 1.5 million immediately, and another PKR 1.5 million the next day. While separately the individual cash payments are below the threshold, they are linked to one transaction and therefore subject to AML/CFT. This is a covered transaction.

Example 4 – Selling to retail customer with linked cash transactions: A customer buys five high value goods from you in quick succession (i.e. few days apart) using cash. Each transaction is PKR 0.5 million (below the cash threshold amount) but collectively the transactions equal/exceed the threshold. This is a covered transaction.

Example 5 – Buying from retail customer: Your business is buying and selling second-hand jewellery as a business. A customer would like to sell you their diamond necklace for cash above the threshold. After assessing the necklace, you value it to be worth PKR 2.5 million. The cash transaction has exceeded the threshold of PKR 2 million. This is a covered transaction.

Example 6 – Retail customer transactions with trade-in: A retail dealer accepts a gold ring valued at PKR 1 million from a customer as a trade-in towards partial payment for the purchase of a diamond pendant worth PKR 2.5 million, resulting in a net cash transfer of only PKR1.5 million. Although the cash portion of the payment is below the threshold level of PKR 2 million, the payment-in kind in the form of the traded-in ring is considered to be a cash equivalent. This is a covered transaction.

Note: The definition of "cash" includes both physical cash and bearer negotiable instruments

4.3 Customers subject to AML/CFT

45. The definition of a customer in the FBR AML/CFT Regulations for DNFBPs in Section 2.Definitions (1) (f):

> *"Customer or client" means any natural person, legal person or legal arrangement engaging a Real Estate Agent, Jeweler or Accountant for the purposes of requesting, acquiring, or using any services or carrying out any transaction or business with a Real Estate Agent, **Jeweler** or Accountant;*

46. Based on that definition, the customer of the DPMS is not limited to the buyer, but could also be the seller. Essentially customers can be classified into two groups:

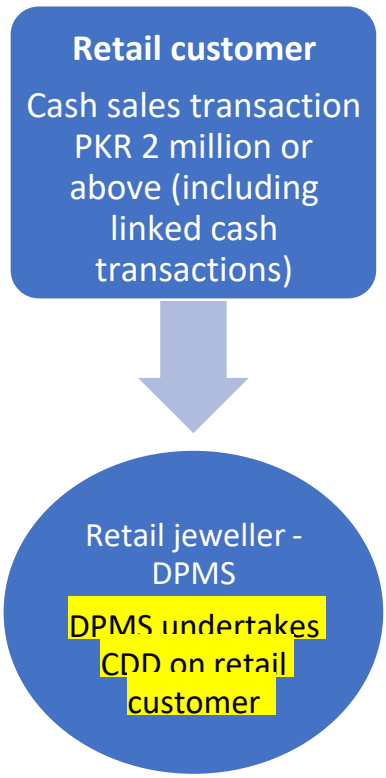
a. A retail customer or from the general public engaged in a sales transaction (buying or selling) with a DPMS.

b. A`DPMS that is engaged in a sales transaction with another DPMS.

(a) Retail customers

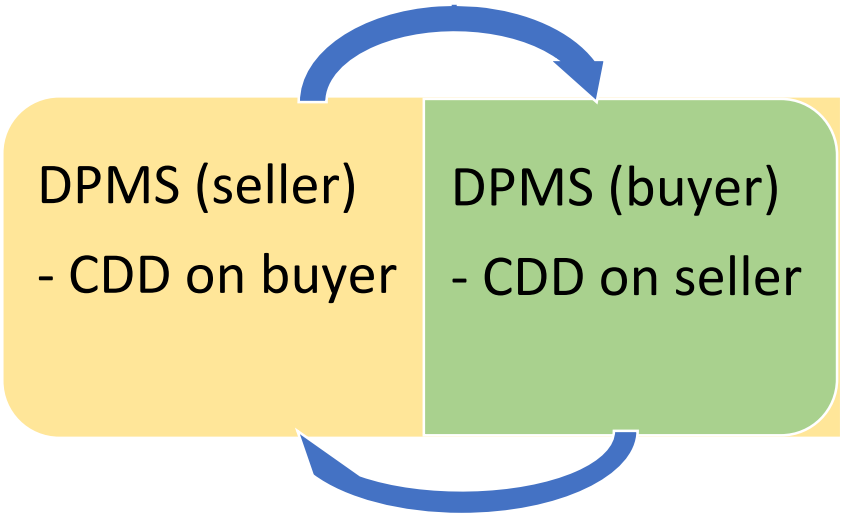
47. For most DPMS, their buyers are retail customers who are individuals i.e. the public. In most instances, these will be walk in customers, although some may have purchased previously. For some retail DPMS merchants, they may also buy from retail customers or as a trade-in for a new

purchase. For commercial transactions, buyers will not, most likely, buy from a retail DPMS to avoid the retail mark-up, but from a wholesale DPMS.



(b) DPMS customers

48. If your business is buying from another DPMS or selling to another DPMS, then most likely your customers will also include companies, and not just individuals as sole traders. If the sales transaction is PKR 2 million or above, both parties would have to conduct CDD on each other. This distinguishes from a retail customer where only one party to the transaction is a DPMS.



49. Examples include the following:

- *Miner (seller/supplier) and processor/cutter, manufacturer or broker (buyer):* Both parties would have to conduct CDD on each other.
- *Broker, manufacturer or processor/cutter (seller/supplier) and retail outlet (buyer):* Both parties would have to conduct CDD on each other.

50. The exception to the above would be a miner, as the only customer would be a buyer.

4.4 Sales transactions not subject to AML/CFT

51. The following are circumstances where DPMS transactions are not subject to the FBR AML/CFT Regulations for DNFBPs.

Transactions not subject to AML/CFT
1) Cash sales transaction involves the buying or selling of high value items not specified or defined as a "*Jeweller*" in the AML/ CFT regulations for DNFBPs. For example, expensive watches and handbags are not normally made "*wholly or mainly*" of precious stones and metals, although they may form part of those consumer goods.
2) An art dealer sells a sculpture, which is comprised of 18K gold, for PKR 2 million in cash. Although the intrinsic value by weight of the gold is worth more than the threshold, the art dealer is not obliged to apply the AML/CFT measures required of DPMS, since the sale of precious metals and stones does not make up a regular component of the business and therefore not considered to be a DPMS.
3) Payment is via credit/debit card or wire transfer. For example, the buyer pays a cash deposit of PKR 500,000 and the balance is paid with a credit card totalling PKR 1.6 million.
4) Cash transaction is below PKR 2 million and not part of a series of related cash transactions totalling PKR 2 million.

4.5 Support and guidance on AML/CFT

52. If your DPMS or you are subject to the obligations, the key requirements and how to implement those requirements are detailed in the remainder of the Guidelines.

53. If, after considering the AML/CFT legislations and the Guidelines, a DPMS is unsure as to whether they are a DPMS or their services are subject to AML/CFT, they should contact the FBR or FMU and/or seek independent professional advice.

54. Where employees of the DPMS have compliance questions, their first reference point should be the DPMS's AML/CFT policies and procedures. The programme documentation should be able to provide answers to basic questions that are likely to arise in the specific business context.

55. Specific questions should be answered by the DPMS's designated compliance officer or senior management.

56. The DPMS can access support from a range of sources:

- 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

57. The Guidelines are not the only source of guidance and information on ML/TF that can be referred. There are other guidance documents issued by the FMU, SECP and SBP that may also be relevant and useful.

58. **Appendix A** to the Guidelines contains a list of some useful and relevant weblinks.

5. Risk Assessment and Mitigation

59. The purpose of the enterprise risk assessment is for your DPMS to identify which customer groups, geographic regions, services and channels 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).

60. 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.

5.1 Statutory requirements under AML/CFT legislations

AMLA: Section 7F requires the DPMS to undertake an enterprise risk assessment for ML/TF.

FBR AM/CFT Regulations for DNFBPs: Section 4 refers to the requirement in the AMLA that DPMS must identify, assess and understand their risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels).

Section also states that DPMS 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 the FBR.

5.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator (e.g. FBR) may impose monetary and administrative penalties for violations of Section 7F.

FBR AM/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 the AMLA.

AML/CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction DPMS for noncompliance with Sections 7 and 7A-7H of the AMLA, and with the 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 risks and DPMS

61. There are many ML or TF risks associated with precious stones and metals, some which are listed below:

General

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

Use of cash

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

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

Gold

- pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily and it can also be used as currency itself e.g. by hawalas.
- gold is available in a variety of forms, e.g. bars, coins, jewellery, or scrap, and trades internationally in all these forms;
- gold has a high actual value and can be found in relatively small sizes, facilitating its transport, purchase and sale in several regions around the world;
- gold also preserves its value regardless of its form whether it comes in the form of bullions, golden articles or is melted;

Diamond

- diamonds are easily portable and traded around the world due to the small size of diamond stones;
- they are unlikely to draw the attention of law enforcement as they are not detected by metal detectors and a very large value can be easily concealed due to their small size;
- all these factors make them at greater risk of being used in cross border money laundering. It has been noted that diamonds have been used by criminals to finance terrorist acts and groups.

5.4 ML/TF enterprise risk assessment

62. 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 DPMS is facing, determining how these risks are mitigated by your DPMS's AML/CFT programme controls, and

establishing the residual risk that remains for the DPMS. The DPMS's AML/CFT programme must be based on your DPMS's risk assessment.

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

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

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

5.5 Difference between an inherent and residual enterprise risk assessment

66. An inherent risk assessment represents your DPMS'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 after the mitigating effects of AML/CFT controls have been accounted for.

67. The primary purpose and benefits of an enterprise risk assessment is to identify the weak spots in your DPMS 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 DPMS to focus more on the remaining vulnerable areas, where despite mitigation measures, they remain at risk. This could be in areas where implementation has been poor e.g. CDD measures for certain categories of customers.

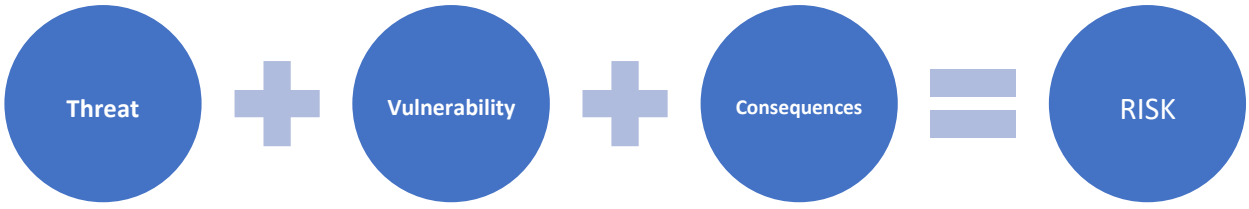
5.6 How to conduct the ML/TF enterprise risk assessment

68. 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 FBR AML/CFT Regulations for DNFBPs, you can choose the method of risk assessment that best suits your DPMS.

69. The following explains the key steps in conducting an enterprise wide risk assessment i.e. identify the risk categories and then assess the risk, including quantitative and qualitative information collection.

(i) Step 1 – What is ML/TF risk

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



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

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

73. ***Consequence:*** A consequence refers to the impact or harm that a threat may cause if eventuated. Determining the impact of ML/TF activity can be challenging but it can also help your DPMS allocate resources more efficiently and effectively in a targeted manner. When determining the impact of ML/TF, the DPMS 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

74. Section 4 in the FBR AML/CFT Regulations for DNFBPs specifies the following four mandatory risk categories:

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

75. ***Customer risk:*** Retail customer of precious metals or precious stones, including jewellery will, in general, not have a business purpose for a purchase of an article of jewellery, a precious stone of a precious metal. A purchase is likely to be made for purely personal and emotional reasons.

76. Give most customers are retail, walk-in customers, the indicators are more related to any unusual patterns in a sale transaction e.g. avoiding PRK 2 million threshold, value of item is beyond the stated occupation or income of customer.

77. As mentioned, a DPMS may sell or buy for another DPMS. In these instances, then there should be an identifiable business reason for the buying or selling of precious stones or metals, or jewellery.

78. ***Product/Service risk:*** All diamonds, jewels, and precious metals can potentially be used for ML and TF, but the utility and consequent level of risk are likely to vary depending on the value of the product. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products.

79. Gold can be higher risk. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself. Gold is available in a variety of forms, e.g. bars, coins, jewellery, or scrap, and trades internationally in all of these forms.

80. The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are

at greater risk of being used in cross border ML. For example, diamonds are small, light in weight, not detected by metal detectors, and a very large value can be easily concealed.

81. Accepting large cash payments increases the risk, especially in large amounts, can be a warning sign, especially if the use of cash is anonymous or intentionally hides an identity.

82. *Geographic risk*: Normally retail purchases are made in person, although the buyer may be a visitor from overseas, particularly wealthier customers who may find the prices less expensive than in their home countries. This in itself is not indicative of higher risk, but the use of large amounts of cash may.

83. For some DPMS, that exports or imports, geographic risk factors would also be important.

84. *Channel of delivery*: Someone buying or paying on behalf of the customer may be indicative of higher risk. However, it is relatively common in jewellery purchases that a woman will select an article of jewellery, and a man will later make payment and direct delivery to the woman. If the person paying is unrelated to the customer (e.g. woman) than the risk is higher.

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

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

Geographic Location (threat and vulnerability)	• FATF listed countries on blacklist or grey list • Offshore tax havens/secrecy jurisdictions • High corruption countries • Countries with high terrorism

86. ***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 DPMS has significant international exposure.

87. ***Other risk categories:*** When conducting your DPMS'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 DPMS deals with e.g. lawyers, other DPMS, banks, service providers etc.

88. ***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 DPMS's business activities i.e. which business lines deliver the specified services subject to AML/CFT, and/or have greater exposure to customer, geographic, products and services, and their delivery channel risks?

89. The DPMS may identify and assess the risk by using risk indicators under each of the four risk categories. The following table contains major risk indicators which are used globally including in FATF guidance documents. For each category, the lower risk indicators are listed and then the higher risk indicators.

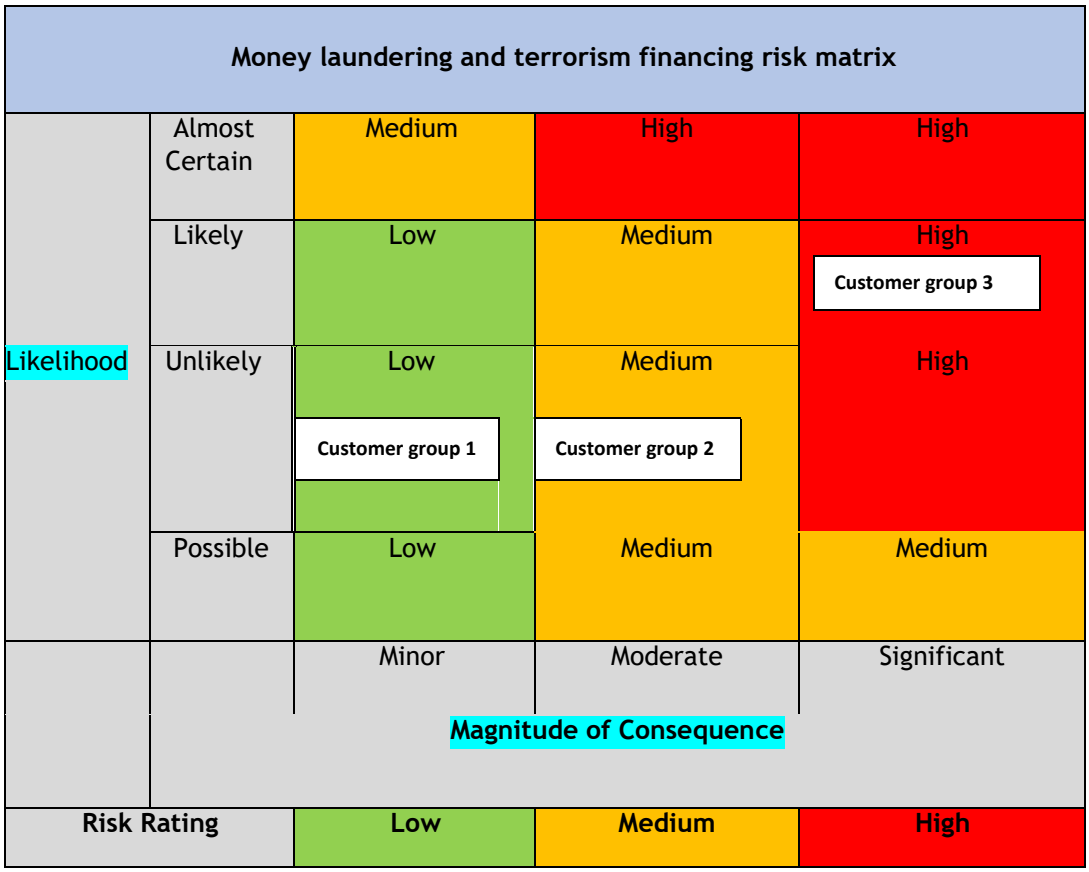
(iii) Step 3- Assess the risk

90. ***Likelihood:*** In order to assess the risk based on the above equation and risk categories 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.

91. 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.

92. When assessing the ML/TF risk, the following matrix, which is commonly referred to as a "heat map", with Likelihood and Consequence scenarios provides a more structure approach.



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

i. ***Customer group 1*** are those that buy items below the threshold in cash or credit card/debit card. It is possible but highly unlikely this group would engage in ML. The consequence may be minor because cash payments are below the threshold specified under the FBR AML/CFT regulations for DNFBPs and out of AML/CFT scope. The inherent risk is therefore low (*refer to above matrix*).

ii. ***Customer group 2*** are regular local customers that pay for expensive items above the threshold. They mostly pay by cheque or physical cash. Overall they are reputable customers e.g. successful doctors, accountants and business people. It is possible but highly unlikely this group would engage in ML. There may be some that are higher risk, and individual customer risk assessment would be required as stated in the FBR AML/CFT Regulations for DNFBPs. The consequence may be moderate, as it would damage the reputation of the DPMS, and the business may be fined by the FBR. The inherent risk is therefore medium (*refer to above matrix)*.

iii. ***Customer group 3*** are politically exposed persons or international visitors. They normally buy very expensive items on a regular basis using physical cash, without regard to their prices. You are aware that some of customers have been accused of corruption. The likelihood that this category of customers 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 your business is providing services knowing that this customer group consist of PEPs and wealthy international buyers. The inherent risk is therefore high (*refer to above matrix*).

5.7 Quantitative and qualitative information for enterprise risk assessment

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

(i) ***Internal Information***: The DPMS's own information about the business – products, prices, customers groups, customers that pay with cash and those who don't etc.

Information from within the DPMS may be collected via a questionnaire or a telephone meeting, or face to face meeting. Depending on how customer records are kept, it may take some time to extract information needed. The DPMS 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 for Pakistan including high risk activities and sectors.

Your DPMS's risk assessment 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 DPMS will have to request a copy from the FBR or the FMU.

(iii) ***Government agencies:*** FMU ML and TF reports (e.g. Strategic Analysis of High Risk Professions), FBR, SRBs, 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 (https://www.transparency.org/en/cpi/2019/results), Basel AML Index (https://www.baselgovernance.org/aml-index) and Tax Justice Network (https://fsi.taxjustice.net/en/).

5.8 Example of an enterprise risk assessment template

95. For a DPMS, conducting the enterprise risk assessment may be divided into two steps:

i. Firstly, reviewing the sales transactions (e.g. last 12 months) to gauge the percentage of transactions conducted via credit/debit/payment card or wire transfer and the percentage using cash. Of those using cash, the percentage over the PKR 2 million threshold, if any.

ii. The second step is undertake a more detailed institutional risk assessment of those customer groups that use cash applying the four major risk categories. You may need to identify the common characteristics of customers paying in cash.

96. This two staged approach is important because if your business rarely have customers that pay in cash PKR 2 million or above, then your DPMS may make a business decision to only allow credit card/debit card/direct wire transfer payments for PKR 2 million or above, rather than invest in AML/CFT procedures for a very small percentage of customers. Conversely, If most of your customers buy goods over the threshold in cash, then your business must invest in AML/CFT processes and controls. It is your DPMS business decision, but an institutional risk assessment is important to provide information on the best risk mitigation strategy.

97. For a DPMS whose customer cash transactions equal or above the threshold of PKR 2 million are limited, the DPMS may decide to consider all such cash transactions as high risk and subject to enhanced due diligence. For another DPMS where this category of customers is a significant component of its customer base, it may need to be more nuanced. For example, it may consider all customer paying in physical cash equal or above the threshold as high risk and subject enhanced due diligence, and those paying by cheque as not automatically high risk.

98. Annex 1 and Table 1 below contain a straightforward risk assessment template. The following provides a case study example on how to use the risk assessment template. It demonstrate how a small DPMS can complete an enterprise risk assessment using a simple template.

Table 1: Risk assessment template

Inherent Risk	Risk rating	Weighting
Inherent Risk Factors **(Using the higher risk indicators)**	**Rating** **High (3)** **Medium (2)** **Low (1)**	**e.g. 25%**
1. **Customers types**		
2. **Geographic location**		
3. **Product / Services**		
4. **Channels of delivery**		
Overall Rating		

99. The above template will be populated using the following case study.

Table 2 Case study

Case Study: DPMS Retailer
The example template has been populated using the following case study. **Case Study: Owner of retail shop in Lahore** - Your retail jewellery shop has 4 shop employees. - The products include gold, precious stones and jewellery made of precious stones and gold. - Customers are mostly walk in, and one off, although there are some repeat longer term customers.
- Most customers pay in cash (or cheque) or credit card below the threshold, although about 20% pay with cash over the threshold. These are your top end customers. These include wealthy international customers.

100. The following provides a relatively straightforward example of an ML/TF enterprise risk assessment using the above case study.

Table 3: Application of risk assessment template using case study

Risk Rating categories	**Low**	**Medium**		**High**	
Customer types	**Local Individual customers**	**International individual customers**		**Risk rating**	**Mitigation measures**
Products/services					
Above PKR 2 million threshold in physical cash (20% of customers)	**High**	**High**		**High**	**Enhanced CDD** **Consider introducing cash maximum e.g. PKR 5 million for all customers** **Training for sales staff**
Geographic location					
80% in Lahore	Medium	N/A		Medium	**Standard CDD**
10% elsewhere in Pakistan (not high risk areas)	Medium	N/A		Medium	**Standard CDD**

10% international	N/A	**High**		**High**	**Enhanced CDD (cash transactions above threshold)** **Training on acceptable ID documents for non-residents**
Channels of delivery					
In person at shop (100%)	Medium	Medium		Medium	
Risk rating	**Over ll risk** Me ium				

Risk conclusions and mitigation measures

The key findings of the enterprise risk assessment are as follows:

- The higher risk categories are customers and those that use cash PKR 2 million or above e.g. PEPs, international visitors.
- Customers from outside of Lahore are not considered higher risk as they are not in geographic regions identified as higher risk in the NRA.
- Overall, the DPMS rated itself as medium risk.

Mitigations measures on higher risk include the following:

- For customers paying by physical cash over the threshold, apply enhanced customer due diligence on purchase.
- Additional training on procedures when dealing with cash payments and acceptable ID verification for international visitors.
- Consider placing a maximum cash threshold. This may be above the PKR 2 million threshold, but will help reduce the risk without impacting on most customers that pay with cash, including those above the threshold.

101. DPMS 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 DPMS, your risk assessment template and risk mitigation measures may be more comprehensive.

6. AML/CFT Programme, Policies and Procedures

102. Your DPMS will need to develop its own comprehensive risk-based AML/CFT compliance programme to comply with the AML/CFT legislations. The basis for this RBA, 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-7H, DPMS 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.

FBR AML/CFT Regulations for DNFBPs: Section 4 (2) on risk based approach states the DNFBPs, including DPMS, must:

(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 7 on compliance programme states that the DPMS 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 7 (1) specifically states that in order to implement compliance programs as set out in 7G of the AMLA, the DPMS 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 DPMS's compliance with these Regulations, the AMLA and other directions and guidelines issued under the aforementioned regulations and laws;
(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; and (d) an independent audit function to test the system.

Section 7 (2) states that for purposes of sub-regulation (1)(d) testing the system includes an assessment of the adequacy and effectiveness of the policies, controls and procedures adopted by the DPMS to comply with the requirements of these regulations; and to make recommendations in relation to those policies, controls and procedures.

Section 7 (3) includes clear powers (e.g. report to board) and 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 (e.g. FBR) may impose monetary and administrative penalties for violations of Section 7G and 7H.

FBR AM/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 the AMLA.

AML/CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction DPMS for noncompliance with Section 7 and sections 7A – 7H of the AMLA, and with the 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

103. The DPMS's senior management must be engaged in decision making on AML/CFT policies, procedures and controls, and take ownership of their risk-based compliance programme. Senior management must encourage a culture of compliance. It must ensure that staff adhere to the DPMS's policies, procedures and processes designed to limit and control risks.

6.4 Compliance officer

104. There must be a person designated as the AML/CFT compliance officer as required under Section 7 (1) (a) of the FBR AML/CFT Regulations for DNFBPs. The compliance officer must be a senior member of the DPMS. 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.

105. Depending on the size of the DPMS, the compliance officer could be:

- The business owner, particularly if a sole proprietorship business; or
- someone from a senior level who has direct access to senior management of the business

106. 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 DPMS, 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 board of directors or chief executive officer or committee;
b) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;
c) be responsible 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 DPMS;
   (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 DPMS may deem necessary in order to ensure compliance with the AML/CFT legislations.

(***Refer Section 7 (3) FBR AM/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

107. An AML/CFT programme sets 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 4 (2) of the FBR AM/CFT Regulations for DNFBPs . These must be approved by senior management.

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

AML/CFT Procedures of DPMS
Table of Contents

i. Enterprise Risk Assessment

ii. Technology Risk Assessment

iii. AML/CFT programme, policies and procedures

iv. Compliance Officer

v. Staff vetting and training

vi. Customer due diligence (CDD)

- Identify and verify customers
- Identify and verify beneficial owners
- Identify and verify any person acting on behalf of the customer, and is so authorised by the customer
- Risk rating of customers – high, medium or low
- Simplified, standard or enhanced customer due diligence
- Delayed verification
- Customer rejection
- CDD and tipping off
- Politically Exposed Persons (PEPs)
- Reliance on third parties

vii. Ongoing CDD, including account monitoring

viii. Targeted financial sanctions

ix. Suspicious transaction report(STR) and currency transaction report (CTR) to FMU x. Record keeping

xi. Independent audit

109. The DPMS has a certain amount of discretion 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

110. 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 DPMS'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

111. If your DPMS 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 Section 7.4-5 of the FBR AM/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 internal 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.

112. 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

113. DPMS must have adequate screening procedures in place to ensure high standards when hiring employees, as required under Section 7 (1) (b) of the FBR AM/CFT Regulations for DNFBPs. If your DPMS already has adequate and effective procedures in place for staff vetting that are also suitable for AML/CFT purposes, your business could include them in your AML/CFT programme and procedures.

114. 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)

115. 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 a new graduate, a reference letter from a university lecturer, university society or from a person of good standing in the community may be sufficient.

116. The employment conditions of staff in the DPMS should include the requirement to comply with AML/CFT legislations and the DPMS's AML/CFT procedures, adding that repeated violations may result in a reduction in sales commission or employment termination.

6.8 AML/CFT training

117. The DPMS must provide its staff with AML/CFT training as required under Section 7 (1) (c) of the FBR AM/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.

118. All sales staff should be made aware of AML/CTF laws 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.

119. The compliance officer will need more specialised external training provided by professional providers, FBR, or by government authorities such as the FMU, SECP, SBP etc.

120. If you are sole proprietor and have no staff, you should attend an external training provided by the FBR or some other provider.

Frequency of AML/CFT training

121. 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.

122. 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

123. While not explicitly stated in the AML/CFT legislations, it is important for the DPMS 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. Given most sales staff are rewarded with bonuses or commission payments, the need to generate sales income need to be balanced against compliance with AML/CFT legislations.

124. 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

125. In addition to regular monitoring by the compliance officer, a regular independent audit is mandatory under Section 7 (1) (d) of the FBR AM/CFT Regulations for DNFBPs. Section 7 (2) states that for purposes of sub-regulation (1)(d) testing the system includes an assessment of the adequacy and effectiveness of the policies, controls and procedures adopted by the DPMS to comply with the requirements of these regulations; and to make recommendations in relation to those policies, controls and procedures.

126. The AML/CFT legislations are silent of the frequency of such an audit; ideally it should be conducted at least once every two years, or as requested by the FBR.

127. The assessment should include a review of the DPMS's AML/CFT procedures so that they cover all the requirements in the FBR AML/CFT Regulations for DNFBPs.

128. The independent audit should undertake a sample of new customers to test whether CDD, targeted financial sanctions and record keeping have been applied in accordance with the FBR AML/CFT Regulations for DNFBPs. This could comprise a review of high risk customers including any PEP customers.

129. Other areas for examination could include whether an institutional risk assessment has been completed, a compliance officer appointed, AML/CFT training conducted for new and existing sales staff and CTRs submitted.

130. The following is a simple template or checklist of areas that the internal audit should cover:

Checklist: Independent Audit		
Areas	**DPMS AML/CFT Procedures**	**Sample testing of implementation**
	Yes/No If no – list gaps	Yes/No If no – list gaps
Institutional Risk Assessment - Money laundering and terrorism financing risks - New technologies		
AML/CFT Programme based on risk assessment		
Compliance officer appointed		
Staff vetting - due diligence checks on new customer facing staff and compliance officer, etc		
AML/CFT training of staff - new staff - existing staff in customer service roles - separate training for designated compliance officer		
AML/CFT procedures adopted by senior management		
Monitoring compliance - identifying violations - staff disciplinary actions		
Group wide compliance (if applicable)		

Risk Based Customer Due Diligence (CDD) - Risk assessment of customer - Simplified CDD - Standard CDD - Enhanced CDD - PEPs - Tipping off - Rejection of new customers, or ceasing relationship with existing customers (both in procedures and actual rejection) - Reliance on third party		
Targeted Financial Sanctions		
- Sanctions lists updated on a timely basis - New customers screening against latest sanctions lists - Existing customers screening against latest sanctions lists - The number of false positives or true positives		
Suspicious Transaction Report (STR) - The number of STRs submitted		
Currency Transaction Report (CTR) - The number of CTRs submitted		
Record Keeping		
Overall conclusion (i) Key findings (ii) Key recommendations		

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

7. Risk Based Customer Due Diligence (CDD)

132. Risk based customer due diligence or CDD is the engine room for effective implementation of AML/CFT. It may require a fundamental change in the DPMS'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 is accepted i.e. engage in a cash transaction equal or above PKR 2 million.

7.1 Statutory requirements under AML/CFT legislations

AMLA: Under Section 7A the AMLA, every reporting entity (including DPMS) with regard to the specified services must conduct CDD on the customer, its beneficial owner and any authorised representative. CDD includes identifying and taking reasonable measures to verify the identity of the beneficial owner. 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.

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 DPMS 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 DPMS 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 DPMS 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 (e.g. FBR) may impose monetary and administrative penalties for violations of Sections 7A to 7H.

FBR AM/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 the AMLA.

AML/CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction DPMS for noncompliance 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

133. Your DPMS 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 (Normally the buyer, but can be the seller)	Means any person engaging a DPMS for the purposes of requesting, acquiring, or using any services or carrying out any transaction or business with a DPMS, but only for specified services and transactions as explained in Section 4 of the Guidelines. • Reference: 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). *(Refer to section 7.8 on Identifying and Verifying Beneficial Ownership below for more detailed explanation)*

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: ▯ The parent who purchases on behalf of the son (with the son's funds) who plans to give it as a gift to his fiancée. ▯ A customer who buys for a friend (funded by the friend) because it is less expensive than in the friend's city. ▯ An employee who has the authority to act on behalf of a company that is your customer.

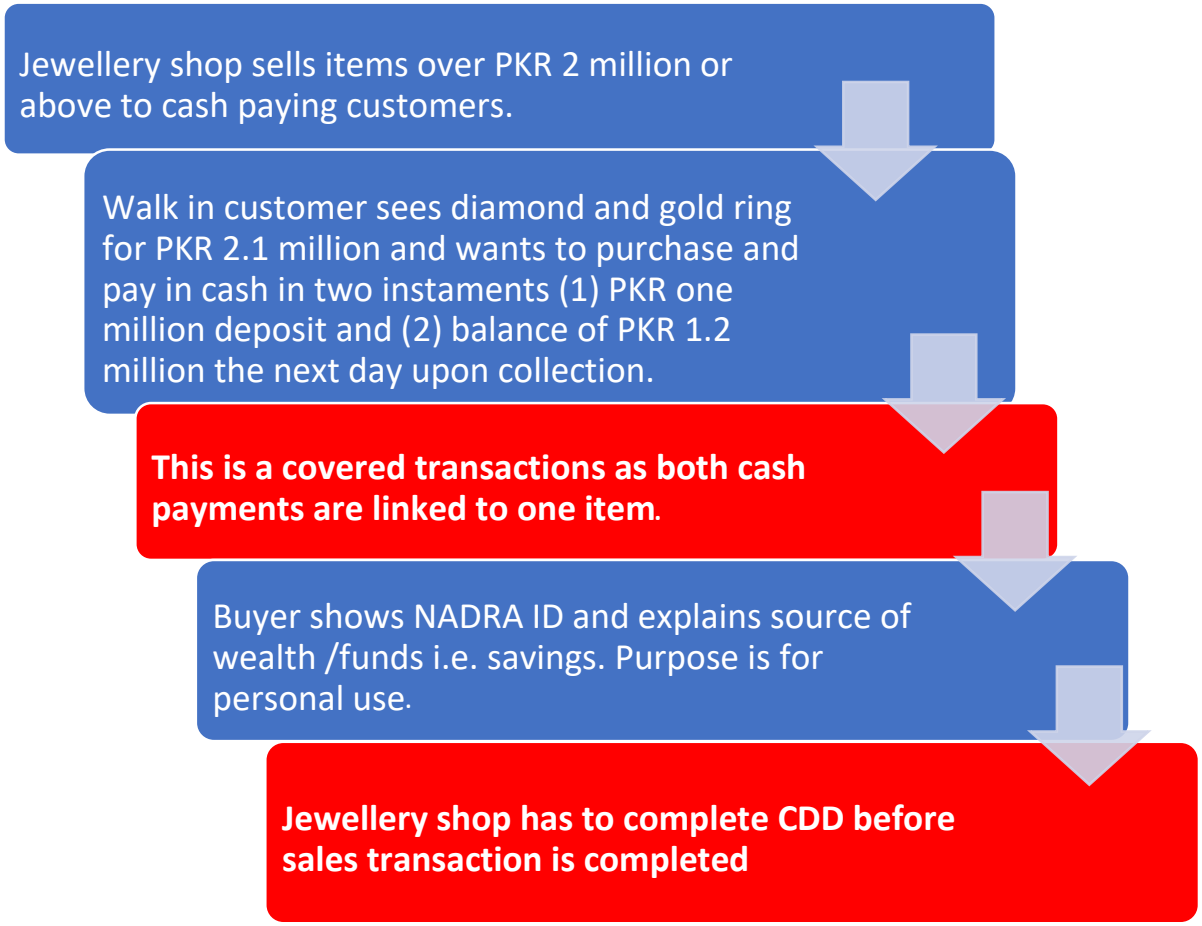
7.4 Timing of CDD

134. The timing of CDD must be undertaken in accordance with Section 7A of the AMLA, as shown in the figure below. The CDD process must be completed before the sales transaction is completed, normally with a buyer but could be a seller.

135. Given most DPMS are retail DPMS e.g. jewellery shop selling to walk in customers, the time available to complete the CDD process is limited if the customers wants to pay in cash, and the sales transaction is PKR 2 million or above.

136. The following examples one for the retailed DPMS and another for a DPMS to DPMS transactions illustrate when CDD must be completed:

Example 1: The retail jewellery shop seller



`

Example 2: DPMS to DPMS

Gem wholesaler sells to jewellery shop items over PKR 2 million or above in cash.

This is a new transaction between the two DPMS as they never traded before with each other. The total value for the cash sales transaction is PKR 3 million.

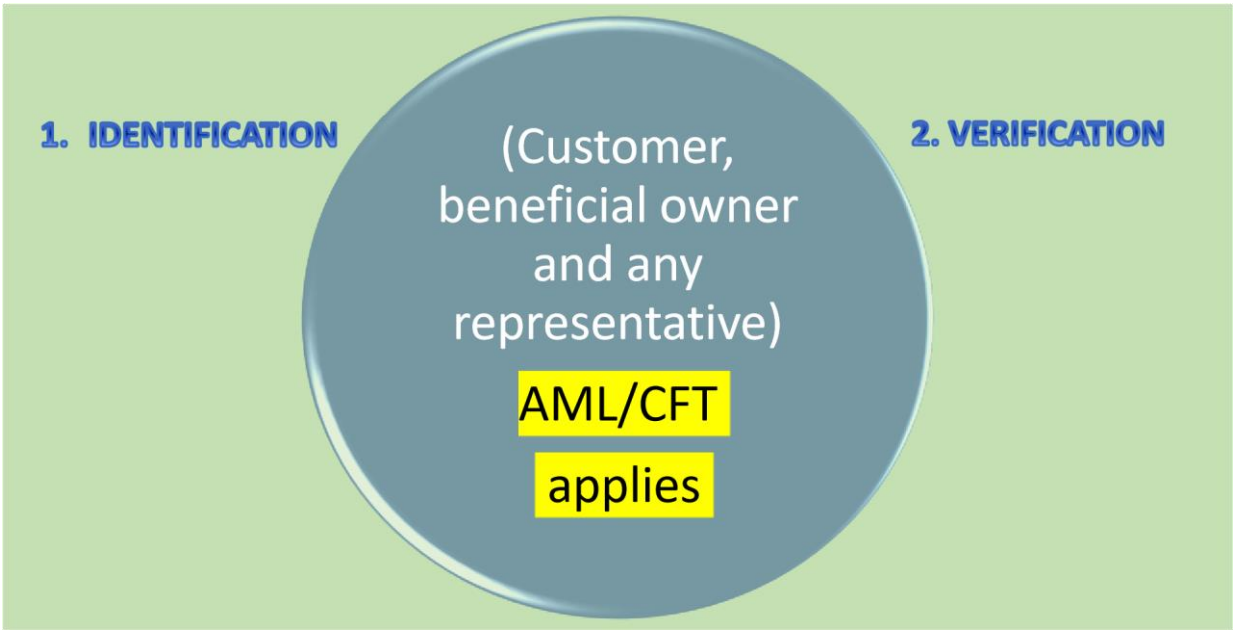
This is covered transactions as both cash payments are linked to one sale.

Both the wholesaler DPMS and jewellery shop DPMS has to conduct CDD on each other.

CDD must be completed on each other before the sales transactions can be completed.

7.5 CDD identification and verification

137. The key CDD requirements are mandated in Section 8 of the FBR AML/CFT Regulations for DNFBPs. The DPMS must not only obtain the required information on the identity of the customer, beneficial owner and any person acting on behalf of the customer, it must also verify the information collected is correct for the customer and any authorised representative, and take reasonable measure to verify the identity of the beneficial owner. CDD therefore involves two interrelated components: identification and verification as shown in the chart below:



138. So, in order to comply with the AML/CFT legislations, the DPMS must verify the ID information with independent and reliable sources that they are true and not false. The following three tables outline the CDD requirements of identification and verification for the three main categories of customers, namely individual/sole proprietor, private company and trust. Beneficial ownership requirements are further explained in the next section.

Table A: CDD Requirements for Individual Customer (or Beneficial Owner or Authorised Representative)*

INFORMATION REQUIRED	DOCUMENTS TO VERIFY INFORMATION Original, or original of certified true copy of document, or electronic verification via NADRA (where applicable)	DATE DOCUMENT SIGHTED/ COPIED/ VERIFIED
Full name:	Resident: NADRA identity card (CNIC) Non-resident: NADRA NICOP or POC, Alien registration card (ARC), or passport https://id.nadra.gov.pk/identitydocuments/verification-services/	
Date of birth:	NADRA identity card, ARC or passport	
Residential address	Recent utility bill	
NADRA identification number/passport	NADRA identity card , ARC or passport https://id.nadra.gov.pk/identitydocuments/verification-services/	
To identify whether customer is acting on own behalf or on behalf of other person	If Yes, and the individual is acting on behalf of another individual (s) – refer to this table (Table A. If the customer is acting on behalf of legal entities – refer to Table B	
Source of wealth or funds (necessary for higher risk customers and PEPs)	Bank statement, accountant's statement, taxation return etc	

Table B: CDD Requirements for Company Customer (and Beneficial Owner and any Authorised Representative)

INFORMATION REQUIRED	DOCUMENTS TO VERIFY INFORMATION	DATE DOCUMENT SIGHTED/COPIED /VERIFIED
Full name of business	Company incorporation certificate	
Registration number	Company incorporation certificate SECP website: https://eservices.secp.gov.pk/eServices/NameSearch.jsp	
Tax payer number	Tax Authority document	

Permanent business address	Company incorporation certificate Utility bill, rental agreement	
Structure of company	Legal documents to establish company/ ownership e.g. Articles and Memorandum , Articles of Association Securities and Exchange Commission of Pakistan (SECP) registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017), as applicable	
Beneficial ownership information	<u>Company</u> Register of Members of a Company Section 119 of the Companies Act, 2017 (Act no. XIX of 2017) Register of Ultimate Beneficial Ownership Information, Section 123A of Companies Act <u>Individuals</u> For all individuals identified as beneficial owners (e.g. major shareholders – 25% and more – verification documents are the same as for individual customers – refer Table A above.	
Source of wealth or funds (necessary for higher risk customers and PEPs)	Bank statement, accountant's statement etc	
Details of individual acting for the company	Same as in Table A for individual customer and official letter from business authorising person to represent the customer	

Table C: CDD Requirements for Trust Customer

INFORMATION REQUIRED	DOCUMENT USED TO VERIFY INFORMATION	DATE DOCUMENT SIGHTED/ COPIED / VERIFIED
Full name of trust (as in trust deed/agreement)	Trust deed/agreement and trust registration certificate	
Registration number (if applicable)	Trust deed/ agreement and trust registration certificate	
Tax payer number	Tax Authority document	
Permanent address	Trust deed/agreement and trust registration certificate	
Type of business / ownership structure	Legal documents to establish business/ Trust deed and trust registration certificate	
Beneficial ownership information		

- Trustee - Protector (if any) - Settlor (or donor) - Beneficiaries Source of wealth or funds (necessary for higher risk customers and PEPs)	Table A information on individuals should be obtained and verified. Table B information on company must be obtained and verified, if any trustee or beneficiaries are companies. Table C on trust if a beneficiary is another trust Bank statement, accountant's statement etc	

7.6 Verification using reliable and independent documents, data or information

139. The above three tables provide examples of reliable and independent documents or information to verify customers that are individuals, companies and trusts. Those verification document, data or information may be in three forms, as outlined in the table below:

Three forms of verification		
Original document	***Certified true copy of original document***	***Electronic/digital verification using data or information***
For purposes of verification, original documents need to be sighted, photocopied and attested by the REA e.g. stamped "Original seen"	Where the customer is unable to produce original documents, the DPMS may consider accepting documents that are certified to be true copies by an independent and qualified person (such as a lawyer , a notary public, etc). The original of the certified true copy must be provided – not just a photocopy of the certified true copy.	Alternatively, if feasible, electronic verification may be undertaken. NADRA is a good source of verification of individuals and SECP for companies and some NPOs. A number of subscription services give access to identity-related information. Many of them can be accessed on-line and are often used to replace or supplement paper-based verification checks. If onboarding is non-face-face and only email copies of documents are provided, in addition to the above 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

140. 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).

141. The AML/CFT legislations state that the DPMS 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".

142. There is a legal definition of the term in the FBR AML/CFT Regulations for DNFBPs, Section 2. Definitions 1) (o). "Reasonable measures" means appropriate measures which are commensurate with the money laundering or terrorist financing risks;" The DPMS has to demonstrate it has taken reasonable measures.

143. The following sub-sections aims to:

a) explain the concept of beneficial ownership for a customer that is an individual, legal persons (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 three categories of customers.

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

144. 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 (Individuals)

145. Most customers of a DPMS are individuals buying for personal reasons and not for business purposes, unless the DPMS is a miner, a wholesaler/trader, importer/exporter or manufacturer of jewellery products. In most instances the individual customer is buying for oneself, so the customer and beneficial owner are the same. However, this may not always be the case and confusion may arise whether the individual customer is also the beneficial customer. This is examined in the Table below:

Customer or authorised representative	Beneficial Owner
1. Customer (e.g. husband) buys a ring (worth PKR 2 million) in cash for his wife as a gift without her knowledge.	If we apply the definition of beneficial ownership in the AMLA (i.e. *a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted),* then the beneficial owner is
	also the customer in this scenario. There is no control by the wife, and he is not conducting it on her behalf. He is conducting the transaction for himself so he can give it as a gift.`

2. Customer X in Karachi buys a necklace for his friend, Mr A in Lahore, as the price is less expensive. Mr A wants to give it as a wedding gift to his daughter . Mr A will wire transfer the money to his friend in Karachi to pay for the necklace (PKR 2.2 million) in cash. The receipt will be in the name of Customer X in Karachi.	The customer is not the beneficial owner. The beneficial owner is Mr A in Lahore. CDD will need to be conducted on both individuals.
3. Husband and wife enters a jewellery shop. The wife selects a bracelet worth PKR2.3 million, and tells his husband to pay for it in cash. He appears reluctant but she insists. When asked by the shop assistant to whom the receipt should be issued, the wife tells the assistant to issue in her husband's name.	Applying the definition of beneficial ownership, the wife has control and the transaction is on her behalf. She is the beneficial owner, even though legally the husband is since the receipt is in his name. He is the customer but not the beneficial owner. CDD will need to be conducted on both individuals.
4. The representative of a wealthy customer wants to buy two diamond necklaces for his employer Mr X. She pays PKR 3 million in cash but wants the receipt issued to her employer Mr X.	The representative is not the customer. The customer is Mr X, who is also the beneficial owner. The DPMS will need to conduct ID verification of the representative including that she is authorised to buy on behalf of Mr X. The DPMS also has to CDD on Mr X.

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

146. 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.

147. 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, a may be specified."***

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

149. 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

TEST 1: The Legal Ownership Test

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

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

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

TEST 2: The Control Test

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

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

2. Majority interest approach: Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity.	– For example, to appoint or remove the majority of the board of directors, or its chair, or CEO of the company. – For example, exercise 25% or more voting rights other than through legal ownership e.g. shareholders agreement to vote collectively to control a company even though individually they do not have 25% or more.

3. ***Connections or contractual relations approach:*** Natural persons who may control the legal person through other means	– For example, the natural person(s) who exerts control of a legal person through other means such as personal connections to persons in positions described above or that possess ownership. – The natural person(s) who exerts control without ownership by participating in the financing of the enterprise, or because of close
	and intimate family relationships, historical or contractual associations, or if a company defaults on certain payments.
4. ***Company director's position approach:*** The natural person(s) responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal person.	The identification of the directors may still provide useful information. However, information on directors may be of limited value if a country allows for nominee directors acting on behalf of unidentified interests.
TEST 3: The Senior Management Test In the event the beneficial owner cannot be identified or verified as above Tests 1 and 2, Section 8 (9) (c) of the FBR AML/CFT Regulations for DNFBPs provide for the use of the senior management approach as the alternative test of beneficial ownership.	
5. ***Senior management approach (alternative test):*** The natural person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position	This is only permitted when the DPMS cannot identify or verify the beneficial owner in limited circumstances, for example: – Dispersed ownership; – Multiple layers of ownership, including in overseas secrecy jurisdiction, or where bearer shares are permitted; The senior management test. for, example, may include the chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president. 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.

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, Section 123A of Companies Act (and the Compliance Certificate) ; and

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

150. Section 119 of the Companies Act provides information on shareholders/members of the company whether natural or legal person. Section 123A relates to the Register of Ultimate Beneficial Ownership which includes ownership beyond the first layer of shareholding of the company.

151. Basically for simple company structures where individuals own the company directly, the DPMS will need the information that the company is required to keep under Section 119 of the Companies Act. Where another company owns your customer (company), then the DPMS 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 (refer to table below for links to SECP documents). Unlike for the Register of Members, however, the actual Register of Ultimate Beneficial Ownership is not provided to the SECP by the company, only the Compliance Certificate. For this reason, the DPMS should also obtain the Compliance Certificate.

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

Summary of information contained in the Register of Beneficial Ownership 123A and Section 119		
	Register of Beneficial Ownership	**Section 119 of the Companies Act**
Applicability	A company shall maintain information of its beneficial owners in such form and manner, within such period and obtain such declaration from its members as may be specified. *Explanation.*- 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 effective control in that company through such other means, as may be specified. (2) Every company shall, in such form and manner as may be specified, maintain a register of its ultimate beneficial owners and shall timely record their accurate and updated particulars, including any change therein, and provide a declaration to this effect to the registrar and where any government is a member of a company such particulars of the relevant government shall be entered in the register of ultimate beneficial owners in the specified manner. The particulars of UBO have been specified through Regulation 19A of the Companies (General Provisions and Forms) Regulations, 2020. The same are available at; https://www.secp.gov.pk/UBO	Every company shall keep a register of iat members. There must be entered in tl register such particulars of each member may be specified. The above specification is contained Regulation 19 of the Companies (Gener Provisions and Forms) Regulations, 2018 which is available https://www.secp.gov.pk/forms
Represents	Ultimate Ownership of the company	Basic/Legal Ownership

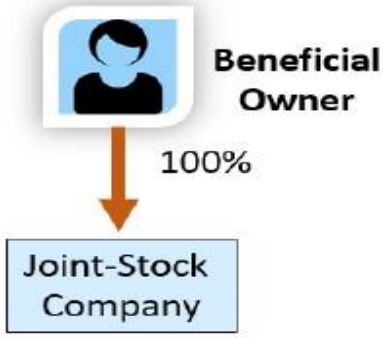
Information to be maintained by the company	Yes	Yes
Information to be notified to the registrar or Commission	No, only Compliance Certificate is provided by the Company	Yes, through FORM A once a year and any Change up to and beyond 25% through Form 3A
Information is publicly available	No	Yes
Penal provision for non-compliance	Yes	Yes

Source: SECP 153. 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)

154. 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



155. 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.

156. For identification and verification purposes, as mentioned earlier, the DPMS needs to collect from the customer the relevant documents, including Register of Ultimate Beneficial Ownership Information by the Company, Section 123A of Companies Act, and the Register of Members of a Company, Section 119, 119A read with section 130 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 the name or names listed are true and correct, and no omission accidently or otherwise.

157. 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 the name or names listed are not false or fictitious because a scanned copy or photocopy can be easily tampered with.

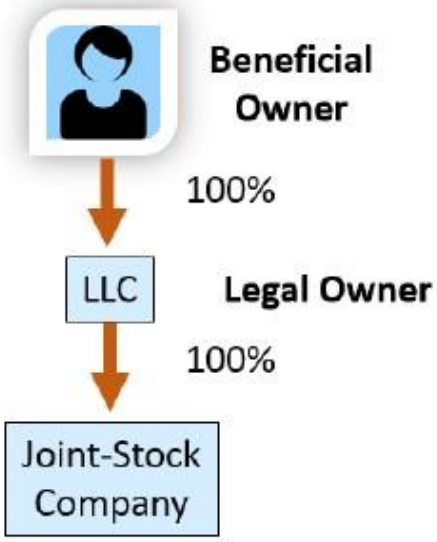
158. If one of the beneficial owner is a non-Pakistani based overseas, the customer should obtain the passport details via email and forward to the DPMS, and a hard copy of the certified true copy sent via mail or courier. Alternatively, if the DPMS has access to an identification verification service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

159. 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.

160. The DPMS will need to complete the above measures to show that it has taken reasonable measures to verify the beneficial owners. The DPMS 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



161. 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.

162. 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 DPMS with information on the beneficial owner.

163. 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 DPMS may need to obtain the LCC company information directly from the SECP or from a company registry overseas, depending on where the LLC is registered or incorporated. Once obtained, the DPMS would then be able to identify the beneficial owner ie. the natural person owner of the LLC company who owns 100% of the customer indirectly.

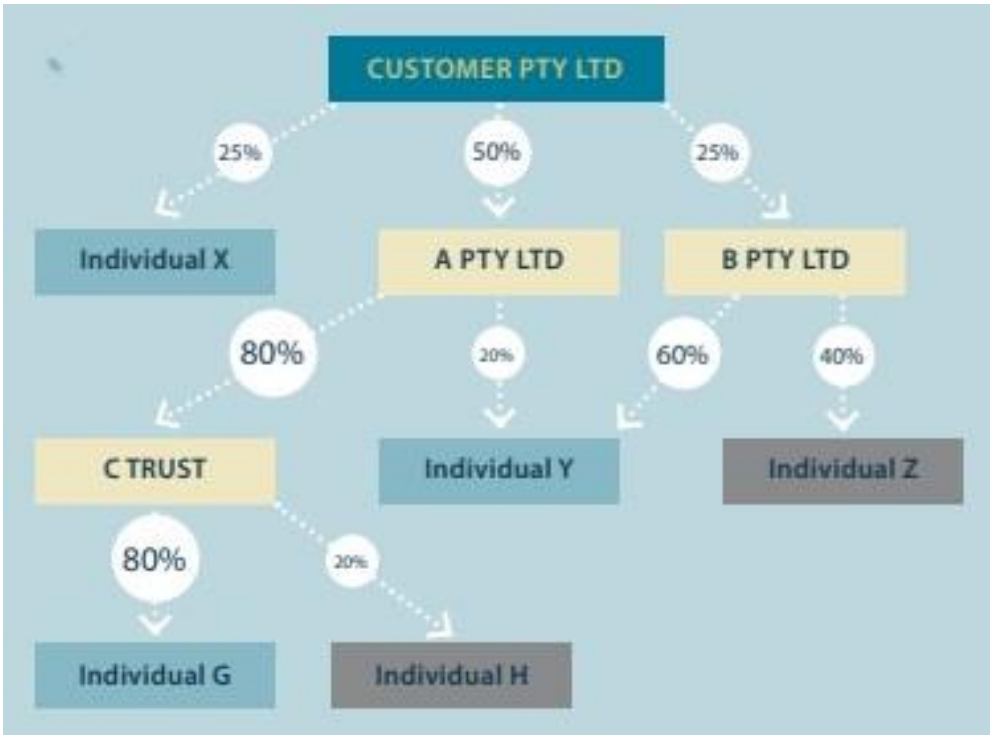
164. CDD also requires the ID documents or information of the individuals who are beneficial owners. The documents need to be original, certified true copy or electronic verification using the NADRA database, If the beneficial owner is a resident. If the beneficial owner is a non-Pakistani resident overseas,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

165. The DPMS will need to complete the above measures to show that it has taken reasonable measures to verify the beneficial owner. The DPMS 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)

166. 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.

Source: AUSTRAC



167. Example 3 above shows the following:

- 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 .8 x .8 x .5 = 32% ownership of CUSTOMER PTY LTD)
- Individual Y is a beneficial owner because they have two interests that collectively amount to an indirect 25% of CUSTOMER PTY LTD:
  - The first is their 20% interest in A PTY LTD, which owns 50% of CUSTOMER PTY LTD (providing an indirect .2 x .5 = 10% ownership of CUSTOMER PTY LTD).
  - The second is their 60% interest in B PTY LTD, which owns 25% of CUSTOMER PTY LTD (providing an indirect .6 x .25 = 15% ownership of CUSTOMER PTY LTD).
  - Adding these together, Individual Y has a 10% + 15% = 25% interest in CUSTOMER PTY LTD

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

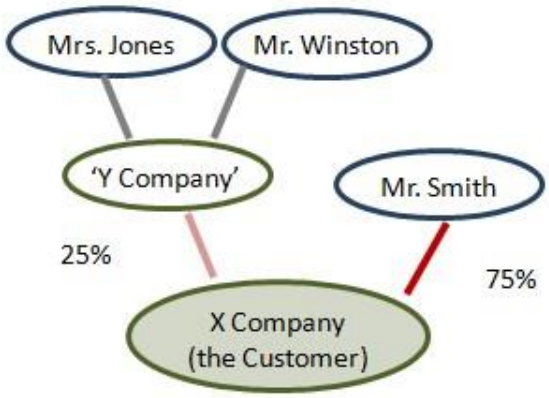
169. If they are not all residents, then the approach will be similar to Examples 1-3 i.e. If one of the beneficial owner is a non-Pakistani based overseas, the customer should obtain the passport details via email and forward to the DPMS, and a hard copy of the certified true copy sent via mail or courier.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

170. The DPMS 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. The DPMS may also experience problems with verifying the ID of Individual Y. However, the customer may need to be classified as higher risk and subject to enhanced due diligence. The DPMS 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)

171. 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

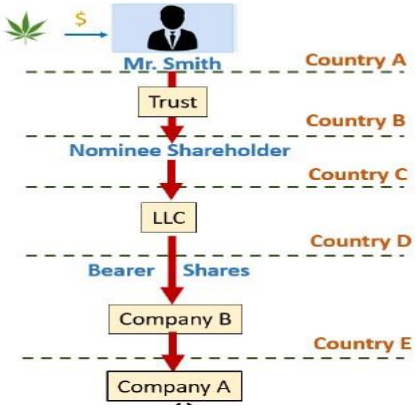


172. However, the DPMS discovers after reviewing the company registration details of Y company that Mrs Jones and Mr Winston both live in the same residential address and are married, but Mrs Jones has kept her maiden name. They could be working collectively to control Y company which in term would exercise 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)

173. 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



174. In this Example 4, neither the Register of Members of a Company (Section 119 of the Companies Act) nor the Registrar of Beneficial Ownership (Section 123A of Companies Act) 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 share certificate has ownership – similar to cash) and a trust.

175. If the beneficial ownership information is not provided, then the DPMS should take measures either 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 nominees shareholders in country C.

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

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

178. 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.

179. If the DPMS determines that the directors are nominee directors and they do not exercise control, then Test 3 may be needed. The DPMS 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.

180. If neither the directors or 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 an STR.

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

181. 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%

182. 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 with equal voting rights. Assuming owners are not forming any alliances or voting blocs, Test 3 on senior management would be the best approach. The DPMS could apply Test 2 and work on the assumption there are 10 individuals that control the customer. This would require verifying the 10 individual directors.

Example 7: Publicly listed company

183. Under Section 10 of the FBR AML/CFT Regulations for DNFBPs, DPMS may apply simplified due diligence. Simplified due diligence for a publicly listed company may include waiving the requirement to identify and verify the beneficial owners. 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.

184. However, consistent with the requirements of simplified due diligence, the DPMS 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.

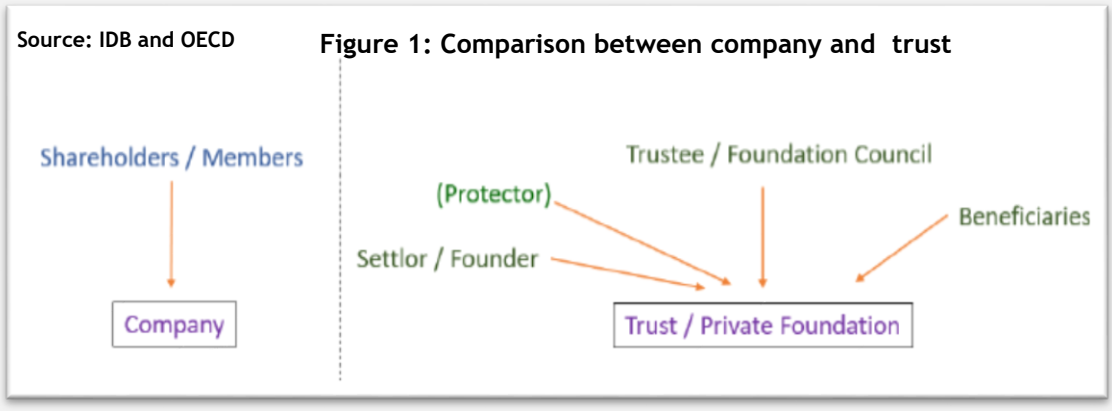
185. It is important to remember, the waving of the beneficial ownership requirement for a publicly listed company is not automatic; it requires a risk assessment. The DPMS will still have to complete other CDD requirements such as verification of the legal status of the company, the ID of the authorised representative and the representative is so authorised by the company (company letter signed by company secretary, director or CEO).

(iv) Legal arrangements (trusts or waqfs)

186. 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

Figure 1: Comparison between company and trust



187. As noted, the definition of beneficial ownership in the AMLA in Section 2 (iv) "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.

188. Section 8 (10) of the FBR AML/CFT Regulations for DNFBPs require the DPMS 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 effective control over the trust (including through a chain of control/ownership);
(b) for waqfs and other types of legal arrangements, the identity of persons in equivalent or similar positions as specified in (a).
(c) Where any of the persons specified in (a) or (b) is a legal person or arrangement, the identity of the beneficial owner of that legal person or arrangement shall be identified.

189. 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 DPMS should identify all parties of the trust as they are all beneficial owners, prima facie, regardless of whether or not any of them exercises control over the trust. The following table shows how to identify beneficial ownership of a trust.

Identifying Beneficial Ownership for Legal Arrangements	
Express trusts/Waqf/or other legal arrangement	
Category	*Identification and verification*
1. *Settlor (or equivalent)* - natural, legal person or arrangement who transfers ownership of their assets to trustee by means of a trust deed or similar 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 DPMS.
2. *Trustee (or equivalent)* - may be professional (e.g. a lawyer, accountant or trust company) if they are paid to act as a trustee in the course of their business, or nonprofessional (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 DPMS. If the trustee is a corporate trustee, the individual authorised to represent the corporate trustee e.g. director needs to be identified and verified.
3. *Protector (or equivalent)* - not all trusts have a protector – protector is a person or group of people (not the settlor, beneficiary, or trustee) who are appointed to exercise one or more powers affecting a trust and the interest of the beneficiaries. The concept of a trust protector is to protect beneficiaries from a rogue trustee.	Once verified based on the trust deed/agreement, the identification and verification is the same as if the person is an individual, legal person or legal arrangement (trust) customer of the DPMS. If the protector is a corporate protector, the individual authorised to represent the corporate e.g. director needs to be identified and verified.

4. *Beneficiaries (or equivalent)* - a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement.	A beneficiary would be a beneficial owner if it has 25% (depending on the threshold used) or more entitlement to the trust distribution. Not all trust specifies a specific unit value e.g. discretionary trust do not, or there are too many potential beneficiaries. In some cases, the beneficiaries are not even born e.g. the children of the son and daughter of X. When it is not possible to identify and verify a beneficiary, the class of beneficiary should be identified e.g. the grandchildren of Mr X, or displaced persons living in region A. Once verified based on the trust deed, the identification and verification are the same as if the person is an individual or legal person customer of the DPMS. If the beneficiary is a corporate beneficiary, then all CDD requirements of a legal person would need to be undertaken. If the beneficial is another trust – then all the CDD requirements of a trust would need to be undertaken.

7.8 Politically Exposed Person (PEP)

(i) *Rule mandated enhanced due diligence*

190. Politically-exposed persons (PEPs) are individuals who, by virtue of their position in public life, may be vulnerable to corruption. While the requirements on enhanced due diligence are further explained in Section 7.15, the requirements of enhanced due diligence for PEPs and their close associates and family members are rule mandated. Under Section 9 (1) of the FBR AML/CFT Regulations for DNFBPs, enhanced due diligence must be applied to all PEPs and their close associates and family members. Unlike for other customers, where enhanced due diligence will depend on whether the customer (and beneficial owner) is rated high risk or not.

(ii) *Who is a PEP?*

191. The definition of PEP is not provided in the AMLA. PEPs are defined in the Definitions sections of the 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.

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

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

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

(iii) *Why are family members and close associates included?*

194. Family members and close associates are included because based on 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.

195. Family members and close associates of a PEP are also defined in the Definitions sections of the 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;

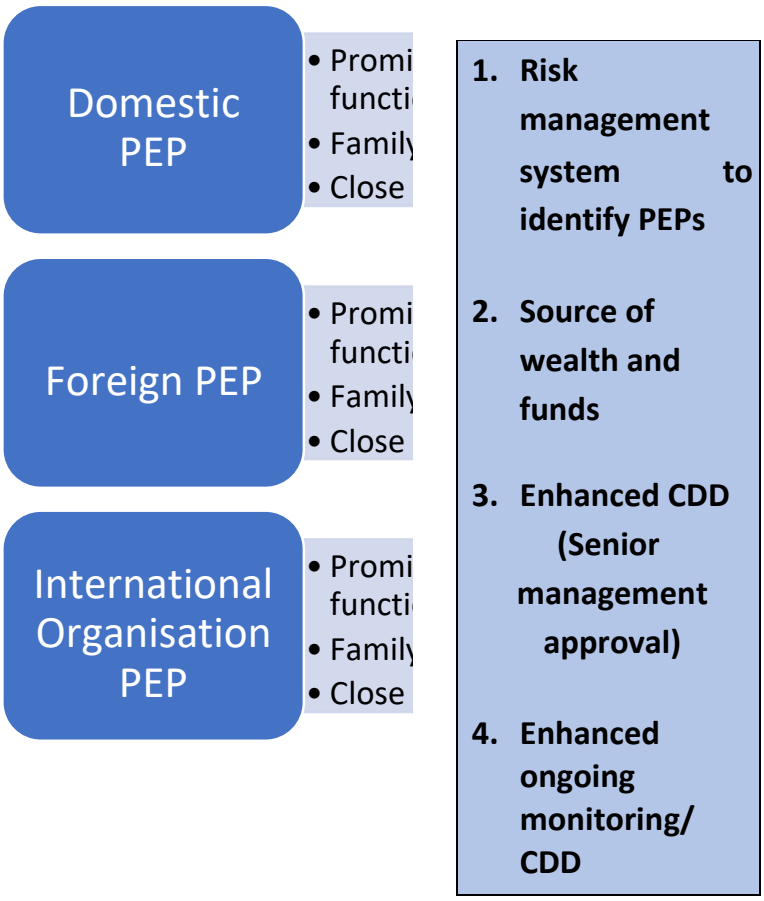
"Close associate" of a PEP means—
(i) an individual known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP;
(ii) any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have 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.

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

196. As noted, Section 9 of the FBR AML/CFT Regulations for DNFBPs state that DPMS 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 below.



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

197. Your DPMS will be required to undertake enhanced due diligence on a customer as described above when providing sales services (buying or selling) 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

198. 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
• For example, authorised representative of a government entity • **Note**: While enhanced due diligence is not required, the REA will still need to identify and verify the identity of the authorised representative, and that the individual is so authorised by his/her organisation.	• The PEP is a director on a board of directors, but there are 9 other directors, and the PEP has only one 1% ownership. • This PEP does not meet the controlling ownership test or the control by other means test. • **Note:** Careful consideration needs to be given to the control test for beneficial ownership. The PEP is still a prominent person, and despite miniscule ownership and limited voting rights, he/she may still influence other directors or senior managament, and thereby control the company.

199. There is nothing precluding a DPMS 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.

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

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

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

202. Firstly, the DPMS 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.

203. Secondly, the DPMS should undertake an independent check. The DPMS's procedures may include:

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

204. 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 DPMS.

205. As explained previously, the above steps are required only if the customer wants to pay in cash (or bearer negotiable instruments) PKR 2 million or above (or below if sales transactions are linked to exceed the threshold amount). If the customers chooses to pay by credit card or wire transfer, for example, the customer is not subject to CDD requirements.

206. Your DPMS 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 a 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

207. 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 DPMS 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

208. 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 DPMS as part of the business relationship.

(iii) Enhanced due diligence

209. 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 9(2) (c) of the FBR AM/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

210. 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 the customer and beneficial owner identified as a PEP, close associate or family member of a PEP under Section 9(3) (b) (ii) of the FBR AM/CFT Regulations for DNFBPs.

211. 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 then one that has no negative news. Also, for the DPMS, establishing the source of wealth or funds will also vary depending on the specified services provided.

212. Further, if the REA 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 DPMS has doubts on the veracity of the documents provided.

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

Information and verification of source of wealth or funds

a) Employment Income • Last month/recent pay slip; • Annual salary and bonuses for the last couple of years; • Confirmation from the employer of annual salary; • Income Tax Returns/ Wealth Statement	**b) Business income/ Profits / Dividends** • Copy of latest audited financial statements; • Rental statements • Dividend statements	**c) Savings / deposits/assets/ property/** • Statement from financial institution • Bank Statement • Taxation returns • Accountant's statements • Property ownership certificate • Share certificates	**d) Inheritance** □ Succession Certificate.
e) Sale of Property/Business □ Copy of sale agreement/Title Deed	**f) Loan** □ Loan agreement	**g) Gift:** • Gift Deed; • Source of donor's wealth; • Certified identification documents of donor.	**h) Other income/wealth sources:** • Nature of income, amount, date received and from whom along with appropriate supporting documentation. • Where there nature of income is such that no supporting documentation is available (for e.g. Agricultural Income) Bank Statement may be obtained.

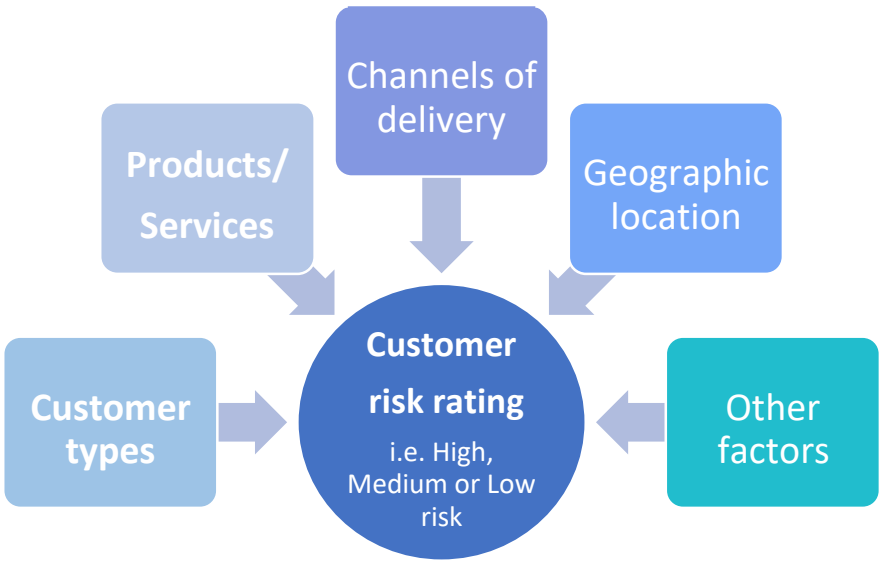
7.10 Enterprise risk assessment and customer risk assessment

214. Section 4 in the FBR AML/CFT Regulations for DNFBPs state that the DPMS must identify and assess the ML/TF risks in relation to its customers, together with other risk categories.

215. The enterprise risk assessment and customer risk assessments are closely linked, but they are not exactly the same. Your DPMS is required to both (i) conduct the enterprise risk assessment and (ii) assess individual customer risk, particularly of new customers. The enterprise risk assessment provides a macro assessment of risk in your DPMS, while the individual customer risk assessment is a micro perspective. Customer risk assessment determines the risk profile of the individual 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.

216. They are different because not all your risks are directly related to your customers, although the customers 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 DPMS 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 rating



217. The customer risk assessment required in Section 4 in the FBR AML/CFT Regulations for must also consider mandatory risk categories are shown in the chart above.

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

Threat + Vulnerabilities (Likelihood and Consequence) = Risk.

219. Similar to the enterprise risk assessment, customer risk can be categorise into three groups, as below:

High risk customer

Medium risk customer

Low risk customer

220. The following table provides a summary of key, higher risk indicators for the four main risk categories.

Indicators for Customer Risk Assessment

Higher risk customers		
1. Politically Exposed Persons (PEP), or a family member or known close associate of a PEP.	2. Customers paying in physical cash significantly above the RKR 2 million threshold	3. Customers wants to make cash payments in instalments with each cash payment below PKR 2 million threshold?
4. Customers wants to trade in of another item so cash payment by customer is below the PKR 2 million threshold for an item that is above this threshold.	5. The business relationship will be conducted in unusual circumstances (e.g. significant unexplained geographic distance between the DPMS and the client)	6. Customers conducting frequent online transactions from locations having tax amnesty to avoid taxes.
7. Customer buying an item that appears to be beyond customer's economic means e.g. stated occupation or business	8. Customer conducts numerous cash transactions over a short period of time without a business purpose, but the cumulative amount is substantial.	9. Discretionary trust (e.g. family trusts).
10. Non-Government Organization (NGO), Not for Profit Organisation (NPO) or charity.	11. Legal persons or arrangements that are personal asset-holding vehicles.	12. Companies that have nominee shareholders or shares in bearer form/ or with complex ownership structures.
Higher risk products/services		
13. Accepting large cash payments from the customer.	14. Higher monetary value items (e.g. diamond) but small in size	15. Conducting transactions for the customer that would involve receipt of funds (cash) from unknown or un-associated third parties
16. Allowing for trade in as partial payment from the customer which results in the cash transaction to be under the threshold of PKR 2 million	17. Allowing for staggered cash payments (separate payments below PKR 2 million)	
Higher risk delivery channels		
18. Services or products provided exclusively via website (online sales), telephone, email, etc, where non face-to-face approach is used?		
Higher risk geographic locations		
19. The jurisdictions which have been identified for inadequate AML/ CFT measures by FATF or called for by FATF for taking counter-measures	20. Countries subject to sanctions, embargos, for example, the United Nations	21. Countries identified by credible sources as having significant levels of corruption, or other criminal activity
22. Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities	23. Locations identified as high risk in NRA (including in Pakistan)	

221. When engaging with the prospective customer, the DPMS will need to gather information about the prospective customer sufficient to undertake the risk assessment.

222. 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.

223. An example of a customer risk assessment template is at **Annex 2.**

7.12 Three categories of CDD

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

225. The figure below highlights the relationship between low, medium and high customer risk, and the required level of CDD.

Relationship between customer risk and level of CDD

7.13 Simplified CDD

226. ***Required information and verification:*** 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 the FBR; and in accordance with the AML/CFT regulations and commensurate with the lower risk factors.

227. Under simplified CDD, verifying the legal identity and beneficial ownership may occur after customer onboarding 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**
- **Take reasonable measures to verify identity of beneficial owner**
- **If necessary, identify and verify natural person representing the customer**
-
- **Scope for delayed verification of customer identity and beneficial ownership**
  Reduce the degree of on-going monitoring and scrutinizing transactions

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

229. There may be lower risk circumstances when one DPMS is conducting a sales transaction with another DPMS. For example, if your supplier of items is a publicly listed company, it may be rated low risk and simplified due diligence may apply. This is subject to a risk assessment confirming low risk (publicly listed companies in Pakistan, FATF member country or a country with equivalent transparency standards on such companies).

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

7.14 Standard CDD

231. The AML/CFT Regulations for DNFBPs is not explicit on the requirements or circumstances where standard due diligence would apply. It is inferred that standard customer due diligence will apply if the customer is not assessed as 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 the identity of the beneficial owner**
- **Ongoing due diligence**

7.15 Enhanced CDD

232. 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. Given the risk associated with cash transactions, a customer paying in physical cash above the threshold or significantly above the threshold may be indicative of higher risk. The possible indicators are detailed in the above table.

233. While there are rule mandated enhanced due diligence scenarios, there will be more instances of enhanced due diligence because of other high risk factors. As indicated earlier in Section 7.11, customers that are discretionary trusts, complex ownership structures (except for publicly listed companies), bearer share ownership (if an owner is another company based overseas), or based offshore in high risk country, are examples of possible higher risk customers.

234. For retail DPMS providers, the customers are most likely individuals. The indicators of higher risk will be different. How a retail customer pays for the jewellery item is an indicator of risk. This could include customers whose economic/financial profile may not match the value of the jewellery item and pay in cash; who wants to make cash payments in instalments with each cash payment below PKR 2 million threshold; or who wants to trade in of another item so cash payment by the customer is below the PKR 2 million threshold for an item that is above the threshold.

235. 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 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

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

Case Study 1: Part 1: Example of Standard Customer Due Diligence on the BUYER: Retail Jeweller B

Customer (Seller)	Jewellery Manufacturer/Supplier A
Customer (Buyer)	Retail Jeweller B
Specified service	Sales
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	**1. Seller (supplier) undertakes CDD on buyer** • Jewellery Manufacturer/Supplier A is selling to Retail Jeweller B. • Retail Jeweller B is sourcing supplies for the retail business. It is a company owned by Mr X. • Buyer (Retail Jeweller B) wants to pay in cash for the first purchase of PKR 4 million in four instalments of PKR one million, but are linked cash transactions totalling PKR 4 million.

2.	Obtain and verify name of customer and address – including all directors, registered and business address	• Certificate of Incorporation • Memorandum of Association • Articles of Association • Register of Members of a Company, Section 119 of the Companies Act, 2017 (Act no. XIX of 2017) • SECP registered declaration for commencement of business as required under Companies Act 2017 • Utility bill for company with physical address • The above information (all originals or certified true copies) verified the name and address of Retail Jeweller B and that Mr. X is listed as the sole director and shareholder of Retail Jeweller B . • Mr. X provides the original of his CNIC ID document. • Original of CNIC is sighted by Jewellery Manufacturer/Supplier A (the seller), photocopied and signed by Mr C the owner.
3.	Obtain and verify names of beneficial owners	• Register of Members of a Company, Section 119 of the Companies Act, 2017 (Act no. XIX of 2017) - lists just Mr X as100% owner and sole director • Memorandum of Association Articles of Association • The natural person owner is also the only beneficial owner.
4.	Assess the ML/TF risk of customer	**Sanctions screening:** Names checked against Ministry of Foreign Affairs and Ministry of Interior lists, and the UNSC website – all okay. The DPMS has consolidated these lists so it is a matter of entering the name and doing a simple search.
		Customer: Simple company structure and beneficial ownership, and no connection to higher risk geographic regions in Pakistan or overseas. **Services:** Sales – standard risk. **Geographic risk**: Standard as in Pakistan and not in areas identified as higher risk. **Channel of delivery**: Standard risk as F2F. **PEP check:** Customer is asked whether PEP or not – answer is negative. Online check confirmed no mention of name. The DPMS 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.

5.	Source of wealth/income Senior management approval Enhanced ongoing CDD/monitoring	□ Information gathered but verification not required, as rated medium risk and not a PEP. □ No need for senior management approval. □ Only standard ongoing CDD.
6.	If the identity information and verification requirements are satisfied, then Jewellery Manufacturer/Supplier A may sell to Retail Jeweller B	□ Completes sales transaction.

Case Study 1: Part 2: **Example of Standard Customer Due Diligence on SELLER:** Jewellery Manufacturer/Supplier A

Customer (Seller)	Jewellery Manufacturer/Supplier A
Customer (Buyer)	Retail Jeweller B
Specified service	Cash sales over PKR 2 million
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	**1. Buyer undertakes CDD on seller (supplier)** • Jewellery Manufacturer/Supplier A is selling to Retail Jeweller B. • Retail Jeweller B is sourcing supplies for the retail business. • Buyer wants to pay in cash for the first purchase of PKR 4 million in four instalments of RPK one million, but are linked cash transactions totalling PKR 4 million. • Because this is a cash transaction, Retail Jeweller B also needs to conduct CDD on Jewellery Manufacturer/Supplier A. • Jewellery Manufacturer/Supplier A is a company owned by Mr and Mrs C.

2.	Obtain and verify name of customer and address – including all directors, registered and business addresses	• Certificate of Incorporation • Memorandum of Association • Articles of Association • Register of Members of a Company, Section 119 of the Companies Act, 2017 (Act no. XIX of 2017) • SECP registered declaration for commencement of business as required under Companies Act 2017 • Utility bill for company with physical address • The above information (all originals or certified true copies) verified the name and address of Jewellery Manufacturer/Supplier A and that Mr and Mrs C are listed as the directors and shareholders. • Mr and Mrs C provides the originals of their CNIC IDs. • Originals of CNICs are sighted by the DPMS (Retail Jeweller B), photocopied and signed by Mr X the owner.
3.	Obtain and verify names of beneficial owners	• Register of Members of a Company, Section 119 of the Companies Act, 2017 (Act no. XIX of 2017) - lists just Mr and Mrs C owners and directors • Memorandum of Association • Articles of Association • The natural person owners are also the only beneficial owners.
4.	Assess the ML/TF risk of customer	• **Sanctions screening**: Names checked against Ministry of Foreign Affairs and Ministry of Interior lists, and the UNSC website – all okay. The DPMS has consolidated these lists so it is a matter of entering the name and doing a simple search. • **Customer**: Simple company structure and beneficial ownership, and no connection to higher risk geographic regions in Pakistan or overseas. • **Services**: Sales – standard risk. • **Geographic risk**: Standard as in Pakistan and not in areas identified as higher risk. • **Channel of delivery**: Standard risk as F2F. • **PEP check:** Customer is asked whether PEP or not – answer is negative. Online check confirmed no mention of name. • The DPMS 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.

5.	Source of wealth/income Senior management approval Ongoing CDD/monitoring	Information gathered but verification not required, as rated medium risk and not a PEP. Note: This is not mandatory as customer is assessed as medium risk, but 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 Retail Jeweller B may complete the sales transaction (buy the items) with Jewellery Manufacturer/Supplier A	Completes sales transaction.

Case Study 2: Example of CDD of Retail Buyer

Customers (Buyer)		Your DPMS, a retail jewellery store, is selling to a walk in customer.
Specified service		Cash sales over PKR 2 million
ML/TF risk		High
Level of CDD required		Enhanced
Steps to complete standard CDD		How this applies to the example
1.	Obtain information about the nature and purpose of the proposed business relationship	Engaged couple comes into store and man wants to buy diamond engagement ring for his girlfriend. Both are working in professional jobs as chartered accountants. He wants to pay in physical cash PKR 200,000 and PKR 1.8 million in a bank cheque.
2.	Obtain and verify names of customer, date of birth and address	The DPMS asks the man to provide identity information (including proof of current address). He provides his original CNIC ID to the DPMS. The DPMS salesperson has a smart phone so he takes a photo of ID placed on top of a piece of paper with his signature and attestation (sighted the original). It is stored onto his phone and he emails it to the administrative person in the office to file. He provides a copy of his utility account for his residential address. The DPMS also uses his smart phone to take a photo of the utility account with the address and emails the photo to his office for filing.

3.	Obtain and verify name of beneficial owner	He is also the beneficial owner as he is controlling the transaction, and it is for himself so he can give it as a gift to his girlfriend.
4.	Assess the ML/TF risk of customer	An assessment is made of customer risk based on the FBR AML/CFT Regulations for DNFBPs and the AML/CFT Guidelines for DPMS. • **Sanctions screening:** The man's names is 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. • **Customer risk:** Higher risk. While the reasons for the purchase and funds are sound, this is still a cash transactions above the threshold. In accordance with the DPMS's procedures, all cash transactions above the PKR 2 million threshold are to be rated higher risk and subject to enhanced CDD.
		• **Geographic risk:** standard risk – he is a resident. • **Services:** standard selling services. • **Delivery channel risk:** standard risk as face to face with buyer. • **PEP check:** Customer is asked whether PEP or not – answer is negative. Online check confirmed no mention of name.
5.	Source of wealth/income	Based on stated profession.
6.	Senior management approval	Senior management approval required as rated higher risk. For a retail jewellery store – this could be the store manager or deputy manager.
7.	Ongoing CDD/monitoring	One off customer. The customer is a buyer. Unlikely to buy another item.
8.	If CDD has been completed satisfactorily, the DPMS may proceed to complete the cash sale.	The DPMS completes the cash sale.

237. Templates for customer onboarding for private companies, individuals and trusts are available at ***Annexes 3-5***. These are for voluntary use, and your DPMS may decide to amend to suit the specific circumstances of your business.

7.17 Prohibited customers and risk screening

238. Section 8 (13) of the FBR AML/CFT Regulations for DNFBP prohibits the DPMS 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. This is covered in detail in the section of the Guidelines on targeted financial sanctions.

239. 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 DPMS cannot accept the new customer as the legal person no longer exists. The DPMS can check online at the SECP website:

https://eservices.secp.gov.pk/eServices/NameSearch.jsp.

240. Once at the portal, just enter the full name of the customer. If it is registered, it will display the company's information.

241. While not mandated in the AML/CFT legislations, the DPMS 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 DPMS 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 higher risk customers such as PEPs.

7.18 Delayed verification

242. Delayed verification is provided in 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.
243. There should be no reason why information on the identity and address of the customer and any authorised representative should be delayed.

244. However, the practicable application of delayed verification for a walk in retail customer may be challenging as once the transaction has been completed, it would be impossible to be revoked.

245. Delayed verification may be more applicable and realistic when one DPMS is conducting a sales transaction with another DPMS e.g. DPMS suppler A is a company, and DPMS buyer B needs to obtain ID verification of beneficial owner residing overseas.

Managing delayed CDD verification

When there is delayed 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 REA shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

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

7.19 Unable to complete CDD

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

(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.

247. The AMLA is very clear that If the DPMS cannot complete the CDD process, even when verification is delayed after the start of the business relationship for whatever reason, the REA 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 DPMS 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 DPMS.

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

7.20 CDD and tipping off

249. As noted above, if continued CDD may tip off a potential customer than, if the DPMS 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 DPMS shall not pursue the CDD process and shall file a STR.

7.21 Ongoing monitoring of new customers

250. Section 8 (6) of the FBR AML/CFT Regulations for DNFBPs requires 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.

251. 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.

252. In most instances, the business relationship is one off and there will not be a need for ongoing CDD. However, there are some customers who may be regular or repeat customers. For example, your customer could be a person who is very wealthy and likes to buy gifts for the extended family on a regular basis. If your customer is another DPMS, then then there is more likely to be an ongoing relationship.

7.22 Existing customers

253. It is important for the DPMS, especially if it is a larger company, 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.

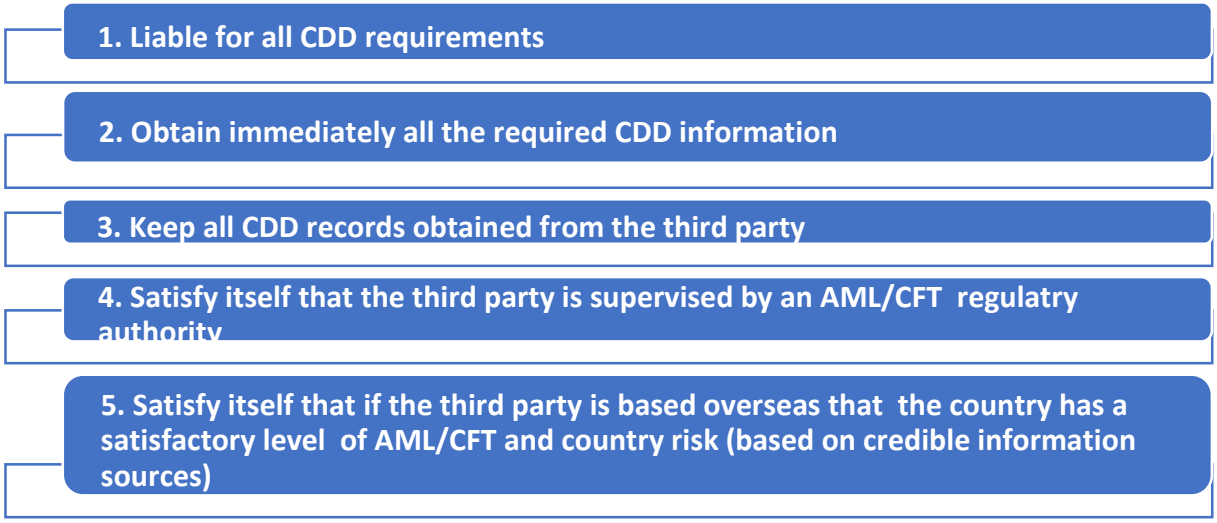
254. Existing customers refer to customers of the DPMS prior to new AML/CFT CDD requirements coming into force and effect. For DPMS, this was up to 28 September 2020, as the FBR AML/CFT Regulations for DNFBPs came into force and effect at once upon promulgation on 29 September.

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**	
No ongoing business relationship or services They will need senior management decision whether they should be treated as new customers, or existing. For example, if dormant for 2-3 years,	**Ongoing services** 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.	**Subject to the full CDD requirements (if paying in cash above the threshold)**
they could be treated as new customers to minimise risk.	There should also be a periodic review of existing customers, particularly those that may be in the higher risk categories e.g. those that are engaging in cash sales transactions over the threshold.	

7.23 Reliance on third party to conduct CDD

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

256. Section 7B of the AMLA provides for reliance on third parties in conducting CDD. This principle is further detailed in Section 12 of the FBR AML/CFT Regulations for DNFBPs. The conditions attached on the DPMS relying on the third party are summarised below:



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

Corporate group complaince	AML/CFT supervision of corporate group	Corporate group mitigation policies for higher country risk
•The corporate group applies CDD and record-keeping requirements in accordance with the AMLA and its associated regulations	•The implementation of the group CDD, record keeping and PEP requirements is supervised by an AML/CFT regulatory authority or an equivalent foreign authority	•The corporate group has adequate measures in place to mitigate any higher country risks

258. For a retail DPMS servicing walk-in customers, reliance on third party may not be practical as these are individual customers. It is easier, for example, for a jewellery store to obtain the NADRA document of a domestic customer, and the passport of a foreign customer then to rely on a third party for CDD.

8. Targeted Financial Sanctions

259. 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:

- UNSC 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 entities including DPMS must have a compliance programme and have AML/CFT policies and procedures, including for targeted financial sanctions.

FBR AML/CFT Regulations for DNFBPs: Section 13 states that the DPMS must undertake the following:

(a) 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.

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

(i) freeze the relevant funds and assets, without delay, in accordance with the respective SRO; (ii) not provide any services, property or funds to the person in question in accordance with the respective SRO; and
(iii) reject the transaction or attempted transaction or the onboarding of the customer, if the relationship has not commenced

(c) In all cases referred in (b) above, the DPMS shall report to the FBR and FMU in mode and manner prescribed by the FBR and/or given in the AMLA.

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

Section 13 (2) further states:

(2) The regulated person [e.g. DPMS) 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.
(3) More

8.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator (e.g. FBR) may impose monetary and administrative penalties for any violations of the provisions of the FBR AML/CFT Regulations pertaining to targeted financial sanctions.

FBR AM/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 the AMLA.

AML/CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction DPMS for noncompliance with Section 7 and sections 7A – 7H of the AMLA, and with the 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 UNSC (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, 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

260. 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.

261. The FBR has issued guidelines and frequently asked questions on targeted financial sanctions under UNSCRs. These are available via the link below:

- https://.fbr.gov.pk/TargetedFinancialSanctionsStatutoryRegulation.pdf

8.4 Screening new and existing customers and their transactions

262. The DPMS must check whether a customer, its beneficial owner and any representative are on the following list.

263. The relevant links to the sanctions lists 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

- Ministry of Interior/NACTA the formal notification of proscription of an organization or person.
  a. https://nacta.gov.pk/proscribed-organizations-3/
  b. https://nacta.gov.pk/pp/
  c. https://nfs.punjab.gov.pk/

- FBR DNFBP Mobile App (IOS & Play store)
- Ministry of Foreign Affairs Strategic Export Control Division (SECDIV) SROs http://www.secdiv.gov.pk/page/sro-unscr-sanctions
- UN Security Council 1718 (North Korea) 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

264. ***Search function on UN Security Council website***: The DPMS may wish to use the search function available at the UN Security Council's website: https://scsanctions.un.org/search/.

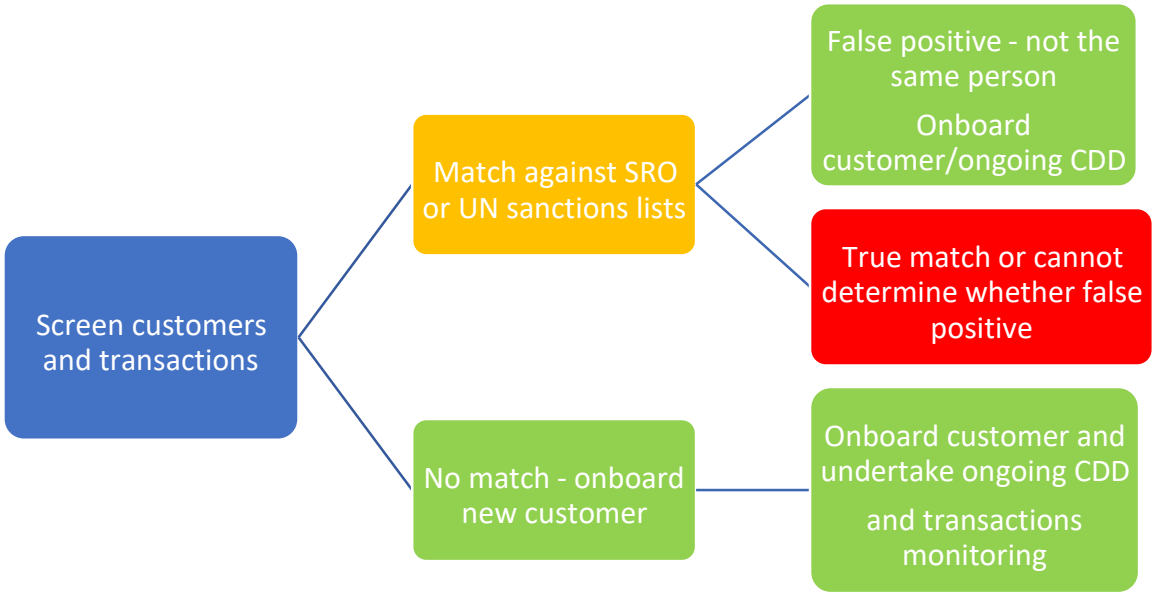
265. There is also a consolidated list of all UN Security Council sanctions available at: https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

266. Please note the search function and consolidated list are not limited to just terrorism and proliferation financing – but also other UN Security Council sanctions. However, they do not include those designated by Federal Government authorities such as the Ministry of Interior/NACTA.

267. ***Delisting:*** The sanctions lists issued by the above bodies are updated whenever there is an addition or removal e.g. delisting. The practical impact of a delisting for a DPMS is if the delisted person was rejected previously as a customer, or had a cash deposit frozen. If a customer (including the beneficial owner or any authorised representative) was previously rejected because of a positive match against a sanctions list, but now delisted, the same customer should not be rejected for that reason again. The DPMS may still reject the customer for other reasons e.g. the risk is still too high. If a cash deposit was frozen, then it should be released.

268. ***New customer screening***: The following is a flowchart of the likely outcomes of the screening:

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



269. ***Existing customer screening***: The DPMS should also conduct screening of existing customers every time there is an update to a sanctions list. This will ensure that no existing customers have been added to one or more of the sanctions lists.

270. ***Consolidated list:*** Given there more than one list, the DPMS should consolidate the lists on a regular basis e.g. download onto a spreadsheet or merged into one PDF document. This will allow for fast name screening by entering a name and searching in the document. For a retail jewellery store, where there are constant walk in customers, completing all the CDD requirements in a timely manner will be important from a business perspective.

271. ***False positives:*** If your DPMS is undertaking the screening on a manual basis, there should be no or very few false positives. If you have a 100% match with name, date of birth and location, then it is a true match from your DPMS'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 e.g. case of mistaken identity.

272. If your DPMS 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 DPMS will need to check manually whether it is a true match or a false match by reviewing all the identifiers.

273. *True match:* If the DPMS identifies a true match – either the customer, beneficial owner or representative, the DPMS must undertake the following:

New customer/updating CDD	New cash transaction with existing customer
1. REJECT the Customer	1. REJECT the cash sales transaction or END the business relationship
2. LODGE a STR with the FMU (refer to section on STR)	
And	
3. REPORT to the FBR **Note:** This is not the STR report, but a report of a match against a name on a sanctions list.	

274. The DPMS must not give prior notice of the above actions to the customer, as this would be tipping off and contravene the AML/CFT legislations.

275. There is also the obligation to freeze funds, however, in a typical cash sales over the threshold amount, it is unlikely the rejected customer would have handed over the cash without receipt of the good as the sale has not been completed. The exception is if the customer is paying in cash instalments (with total PKR 2 million or above), and the match was identified after the first instalment, but not the final instalment to complete the cash transaction.

8.5 Ministry of Foreign Affairs Updates

276. To ensure prompt transmission of SROs issued by MOFA to relevant stakeholders, including DPMS, the MOFA has put in place an email subscription service. DPMS are required to sign up for this service. For those needing to subscribe – the link to the MOFA's website is: http://202.83.172.66/app/signup/.

9. Suspicious Transaction Report (STR)

277. 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

AMLA: Under Section 7 (1) of the AMLA, the reporting entity which includes the DPMS (as per Section 2 (xxxiv) and 2 (xii) of AMLA) must file an STR to the FMU promptly for a conducted or attempted transaction if the DPMS 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 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.

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

9.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator (e.g. FBR, FMU) 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 willfully 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 FBR to sanction DPMS for noncompliance with Section 7 and sections 7A – 7H of the AMLA, and with the 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.

FBR AM/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 the AMLA.

278. 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/wpcontent/uploads/2020/05/Guidelines-on-filing-of-Suspicious-Transaction-Reports-for-theReporting-Entities.pdf.

279. 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

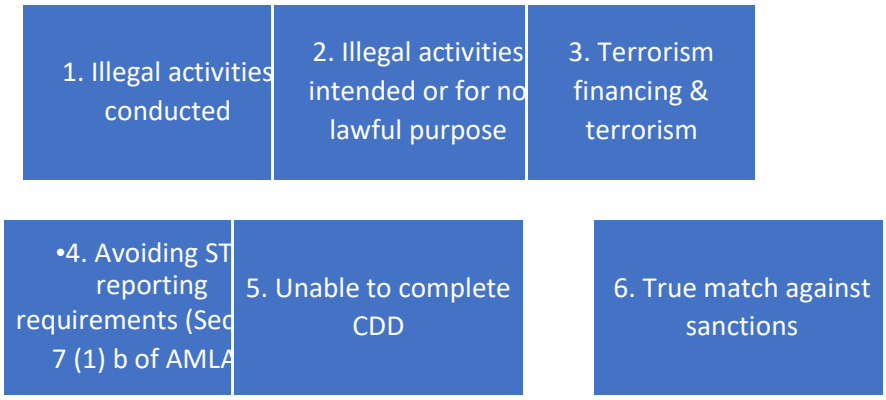
280. Section 7 (1) of the AMLA is quite broad – not just in the coverage of ML and TF, and conducted or attempted, but also on both transactions and activities. According to Section 7, if the DPMS knows, suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, 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**

To know is a higher threshold for reporting. To know is to have objective evidence of ML or TF. Known or knowledge means actually knowing something to be true. The knowledge must have come to the DPMS (or to its staff) in the course of business. 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.	**Reasons to suspect are an objective test** to submit an STR and is a step above suspicion, meaning that there is likelihood that an 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 an STR should be submitted This could be based on matches against AML/CFT red flags or suspicious indicators issued by the FMU.	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.

9.4 Scope of STR reporting

281. Under Section 7 of the AMLA , the DPMS must file an STR when one or more of the following six activities have been identified (refer to Table on Reporting above) when dealing with a customer:



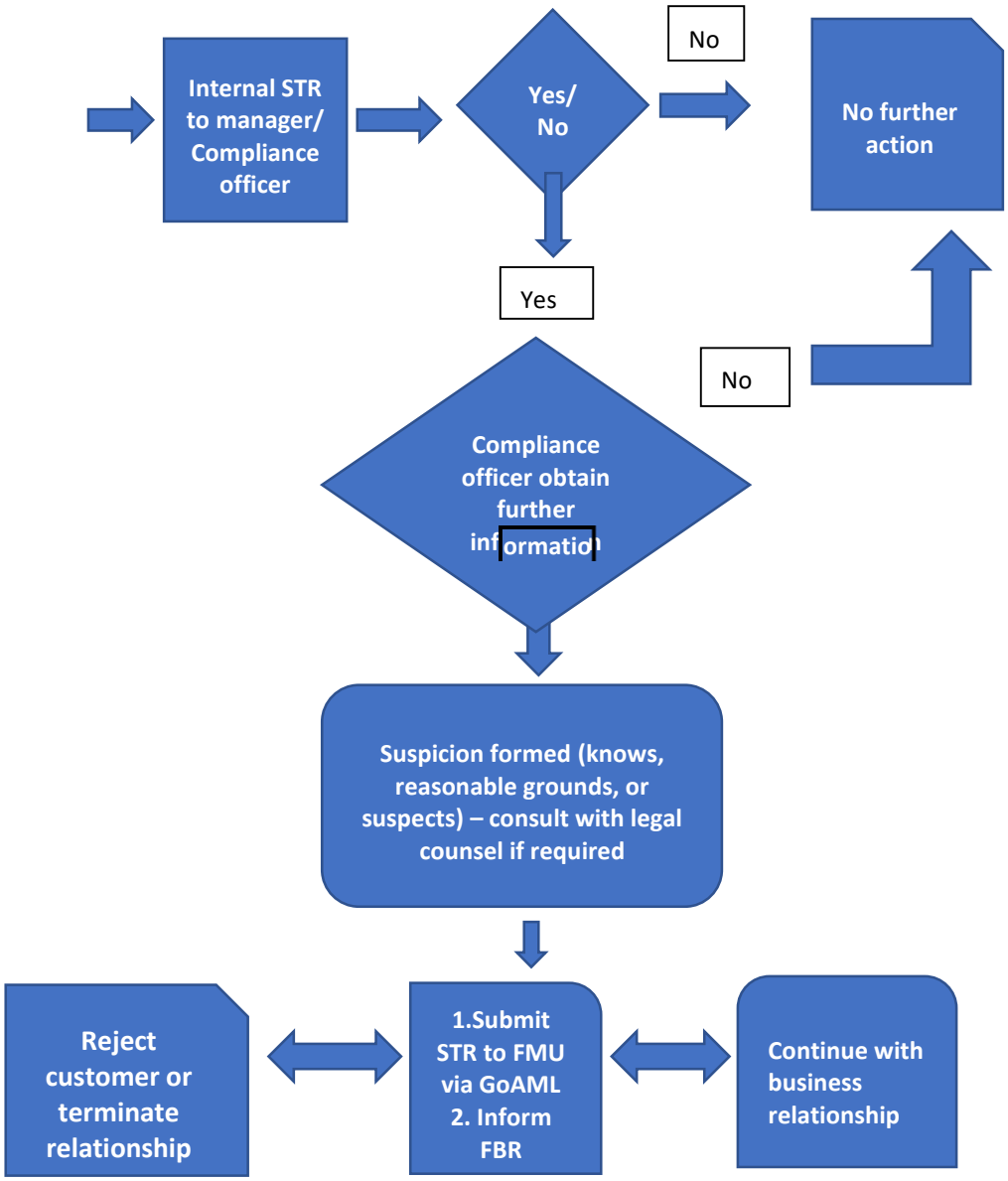
9.5 AML/CFT red flag indicators for DPMS

282. In addition to the guidelines on STR reporting, the FMU has also issued a Circular No.05/2020 :Red Flag Indicators for DPMS: https://www.fmu.gov.pk/Red-Flag-Indicators-for-Jewelers-andPrecious-Stones-or-Metal-Dealers-Final.pdf. Please also see Annex-6 for Red Flag Indicator for Countering Proliferation Financing.

283. 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 DPMS 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 DPMS knows, has reasonable grounds to suspect or suspects.

9.6 Internal reporting procedures

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



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

286. 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.

287. 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 an STR.

288. 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.

289. The compliance officer may also consult on a confidential basis with the DPMS'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

290. 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

291. 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.

292. DPMS are recommended to report STRs via goAML Web Form instead of developing XML extractor through their system.

293. In order to report STR, reporting entities (including DPMS) are firstly 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.

294. The designated compliance officer is responsible for registering with the FMU and submitting any STRs. It is highly recommended that the designated compliance officer register with goAML as soon as possible, and understand how to use the system prior to any need to submit an 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-Updated2020.pdf.

9.8 Content of STR

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

Reason for Reporting of STR

296. 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

297. The DPMS is required to provide detail of any action already taken by the DPMS 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

298. There are varieties of indicators in goAML and the DPMS 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 DPMS can select one or more indicators while reporting the STR.

299. 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:

- From (Source) and To (Destination) party information which include multiple details,
- Three parties (i.e. Person, Account and Entity) will be shown on each side (from & to). One party must be selected based on the movement of funds.
- Fund types to be selected on both From & To Side separately.
- Transaction details (multiple fields).

9.9 Types of STRs

300. There are two types of suspicious reports which can be submitted by the DPMS to FMU.

Report Parties (STR-A):

301. 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.

302. 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):

303. 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.

304. 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

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

10. Currency Transaction Report (CTR)

306. The purpose of Currency Transaction Report (CTR) is to identify cash transactions with the financial system, either directly or via designated non businesses and professions (DNFBPs), including DPMS. 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 DPMS 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.

FBR AM/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 the AMLA.

10.2 Sanctions for non-compliance

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

Under Section 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 FBR to sanction DPMS for noncompliance 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.

FBR AM/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 the AMLA.

10.3 Currency threshold for CTR

307. According to the Ministry of Finance SRO issued in January 2015, all cash-based transactions PKR 2.0 million or above or equivalent foreign currency are required to be reported to the 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.

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

10.4 When are DPMS required to submit CTR?

309. Given the AML/CFT requirements only apply to cash transactions PKR 2 million or over, every time you complete a cash sale transaction over the threshold, your DPMS is required to file a CTR. This includes cash sales transactions below the threshold which are linked and totals above the threshold as described in Section 4 of the Guidelines.

310. Your DPMS would not be required to file any CTR if the sales transaction is via wire transfer or credit/debit card. If your DPMS pays cash to sales staff as renumeration over the threshold, or purchase an asset such as a computer, it would not be subject to CTR filing. They would not be considered as a cash sales transactions.

311. However, if your supplier or buyer is another DPMS, and the item sold or purchased with cash is wholly or mostly made of precious stones and metals, then CTR filing obligations apply.

10.5 Reporting to FMU via goAML

312. Similar to STR reporting to the FMU, all CTR reporting is via the FMU's online goAML system – refer: www.fmu.gov.pk/goaml.

313. 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.

10.6 Contents of CTR

314. As per the standardized CTR format the information relates to the:

- From (Source) and To (Destination) party information which include multiple details, Three parties (i.e. Person, Account and Entity) will be shown on each side (from & to). One party must be selected based on the movement of funds.
- Fund types to be selected on both From & To Side separately.
- Transaction details (Amount in PKR, Reference Number (auto generated) and City Name).

Parties Details:

Following details of parties required when selected on either from or to side:

Person Involved:

- Name (First Name and Last Name)
- Father / Husband Name
- CNIC or Passport Number
- Address

- Contact Number (without + & 0 at the start)

Bank Account Involved:

- Account Number
- Bank Name
- Account Title

Entity Involved:

- Entity Name
- Incorporation Number
- Legal form of the Entity (Proprietorship, Partnership, etc.)

Funds Type Selection for CTRs:

For Purchase Transaction:

- From Funds Type: Purchase from Customer
- To Funds Type: Cash
- **For Sale Transaction:** From Funds Type: Cash
- To Funds Type: Sale to Customer

Person involved in transaction	Other individual conducting the transaction	Transactions Details	DPMS where transaction takes place
•Name, address, other contact information •CNIC, NTN number •Nationality •Occupation /		•Date of transaction • Name of City Transaction Reference Number (can be used goAML's auto generated reference number	•Name •Address

10.7 Timeline for CTR reporting

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

10.8 No tipping off to customer

316. The DPMS 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

317. DPMS are required to maintain records either in hard or digital form. The purpose are multiple, including for the DPMS's own benefit, as evidence to authorities that the DPMS 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.

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)."

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

11.2 Sanctions for non-compliance

AMLA: Section 7I AMLA provides that a regulator (e.g. FBR) 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.

AML/CFT Sanction Rules: Section 3 provides the powers for the FBR to sanction DPMS for noncompliance 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.

FBR AM/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

318. The following Table summarises the key requirements.

Record keeping requirements	
Record Type	Retention period
1. CDD documents (Section 7C of AMLA) (Sections 6 of the FBR AM/CFT Regulations for DNFBPs)	5 years after the end of the customer relationship.
2. Transaction records (Section 7C of AMLA) (Section 6 of the FBR AM/CFT Regulations for DNFBPs)	5 years after completion of transaction.
3. STR and CTR filed records – including CDD and transaction records related to the STR or CTR (Section 7 (4) of AMLA)	10 years after submission

319. While not explicitly stated, the DPMS should keep records for 5 years of enterprise risk assessments, procedures, AML/CFT training records including staff attendance, and independent audit.

320. Section 6 (7) of the FBR AM/CFT Regulations for DNFBPs requires DPMS to keep a list of all customers where the business transaction was refused (e.g. new customer) or needed to be closed on account of failure of the customer to provide the relevant CDD documents.

11.4 Table on how to maintain records

321. As mentioned in Section 6 (2) of the FBR AML/CFT Regulations for DNFBPs, record of CDD and other AML/CFT documents as described above may be maintained in paper or electronic form. The following Table provides guidance on how records could be maintained:

Three forms of verification and record keeping

Original document	*Certified true copy of original document*	*Electronic/ digital verification using data or information*
If original documents were collected e.g. certificate of incorporation, bank statement, then they could be filed either physically, electronically or both. If the original documents were only sighted e.g. NADRA ID or passport, then the DPMS's photocopy of the ID documents should be clearly marked e.g. "Sighted by X staff member on X date, and then signed and dated by X staff member". If electronic files are used as the primary method of record keeping, it may be useful to note on the electronic copy that the original document was collected, and date of collection (if not already noted). This will assist in demonstrating that while the record is electronically	The same approach as for record keeping of original documents. If electronic files are the primary method of record keeping, then similar to original documents, the electronic copy should note that the original document of the certified true copy (not a photocopy of the certified true copy) was collected, and date of collection.	If an ID is verified electronically by using NADRA: (https://id.nadra.gov.pk/identity verification-services) or the SECP portal: **https://eservices.secp.gov.pk** then a verification screenshot or a PDF print of the verification notice should be filed either physically or electronically as evidence of verification. If verification is through a third party service provider, the service provider's system should have digital records of all verifications completed or not completed e.g. name, date of verification and evidence of verification, which can be extracted and printed via a management report.
stored, there is also an original hard copy. For example, during an onsite inspection by the FBR on compliance with the regulations.		

Annex 1 – Enterprise Risk Assessment Template

Risk assessment template

Inherent Risk	Risk rating	Weighting
Inherent Risk Factors **(Using the higher risk indicators)**	**Rating** **High (3)** **Medium (2)** **Low (1)**	
1. **Customers types**		
2. **Geographic location**		
3. **Product / Services**		
4. **Channels of delivery**		
Overall Rating		

Annex 2 – Customer Risk Assessment Template

CUSTOMER RISK ASSESSMENT TEMPLATE (Note: For internal use by DPMS only)

Explanatory Notes:

1. This is an example template for customer risk assessment for voluntary use, or the DPMS may wish to amend this template to suit its own circumstances.

2. The following factors should be considered by the DPMS in carrying out its risk assessment for new customers. The list is not exhaustive, and the DPMS may consider additional factors relevant to their working environment.

3. If the response to any of the questions listed in Section 1.1 (i.e. prohibited persons/organisations) is ***"YES"***, this means that the DPMS 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 PEP, the DPMS is required to conduct enhanced customer due diligence which involves approval by senior management of the DPMS prior to accepting the new customer. The concerned staff member should also consult with the designated Compliance Officer with regards to the risk factors identified. If the DPMS is a sole trader, then senior management approval would be by the sole proprietor.

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 DPMS can then decide whether to accept the new customer or not.

SECTION 1.1: PROHIBITED PERSONS/ORGANISATIONS SCREENING *(refer point # 3 of the explanatory notes)*	
	Response

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

SECTION 1.2: CUSTOMER'S RISK FACTORS

(refer point # 4 of the explanatory notes)

	Response	
Is the customer or its beneficial owner a Politically Exposed Person (PEP), family member of a PEP or close associate of a PEP? *Note: "Politically exposed persons" or "PEPs" - means any person entrusted with a prominent public function by the State of Pakistan, a foreign country or an international organization and includes Heads of state or government, and 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
Customers wants to pay in physical cash for item that is significantly above the PKR 2 million threshold?	YES	NO
Customers wants to make cash payments in instalments with each cash payment below PKR 2 million threshold?	YES	NO
Customer buying an item in cash that appears to be beyond customer's economic means e.g. stated occupation or business?	YES	NO
Customer conducts numerous cash transactions over a short period of time without a business purpose, but the cumulative amount is substantial?	YES	NO
The customer is non-resident in Pakistan?	YES	NO

The customer or potential customer is a Non-Government Organization (NGO), Not for Profit Organisation (NPO) or charity? *Note: The list of registered charitable organizations / NGOs / NPOs can be obtained from* *http://pcp.org.pk/pagestyle.php*	YES	NO
Is the customer in a high – risk industry? *Note: High risk industry includes (but not limited to) following businesses;* *- Businesses dealing with precious metals (gold, 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
Is the customer a shell company, especially in cases where there is foreign ownership which is spread across jurisdictions? *Note: Shell Company means an inactive company used as a vehicle for various financial manoeuvres or kept dormant for future use in some other capacity.*	YES	NO
Does the customer have unusual or complex shareholding structure (e.g. involving 3 layers or more of ownership structure, different jurisdictions, trusts), given the nature of its business? Note: *The above excludes publicly listed companies in Pakistan and FATF member countries, or other countries with equivalent transparency standards for such countries.*	YES	NO

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

SECTION 1.3: COUNTRY / GEOGRAPHICAL RISK FACTORS

(refer point # 4 of the explanatory notes)

	Response	
Countries identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering/terrorism financing or subject to a FATF statement? *Note:* *- For countries in black list, please refer* *https://www.fatfgafi.org/countries/#high-risk* *- For countries in grey list, please refer* *https://www.fatfgafi.org/countries/#other-monitored-jurisdictions*	YES	NO
Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations? United Nations: https://scsanctions.un.org/search/	YES	NO
Countries identified by credible sources as having significant levels of corruption or other criminal activity? Transparency International: https://www.transparency.org/en/cpi/2019/results	YES	NO

Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country? Institute of Economics and Peace: http://economicsandpeace.org/Global Terrorism Index	YES	NO
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? *Note: The high risk areas / jurisdictions includes western borders / FATA / Southern Punjab and the eastern border.*	YES	NO
Countries known for high levels of financial secrecy or with low tax rates? Tax Justice Network: https://fsi.taxjustice.net/en/		

SECTION 1.4: SERVICES / PRODUCTS RISK FACTORS

(refer point # 4 of the explanatory notes)

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

SECTION 1.5: DELIVERY CHANNEL RISK FACTORS

(refer point # 4 of the explanatory notes)

	Response	
Will services or products be exclusively via internet (website online sales) telephone, email, etc, where non face–to–face approach is used?	YES	NO

SECTION 1.6: REPUTATIONAL RISK SCREENING

(refer point # 4 of the explanatory notes)

	Response	
Has the DPMS performed 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? Are there adverse news or information arising?	YES	NO

CUSTOMER RISK RATING

☐	Low Risk → Simplified Due Diligence
☐	Medium Risk → Standard Due Diligence
☐	High Risk → Enhanced Due Diligence

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

Customer Acceptance Recommendation:

☐ Accept

☐ Reject

Assessed by:

Name: _____

Designation: _____

Date: _____

Signature: _____

Approved by:

Name: _____

Designation: _____

Date: _____

Signature: _____

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 Act
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

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

PART 1. BASIC IDENTIFCATION INFORMATION	**VERIFICATION DOCUMENTS**
Full Legal Name (as per ID document):	**Residents**: CNICs/ Smart National Identity Card (SNIC) issued by NADRA **Non Residents:** National Identity Card for Overseas Pakistanis (NICOP) and/or Passport issued by NADRA for Non-resident / overseas Pakistanis or those who have dual nationality; or Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistanis who have given up Pakistan nationality; or Form B or Juvenile card issued by NADRA to children under the age of 18 years; or Where the natural person is a foreign national, either an Alien registration card (ARC) issued by NADRA or a Passport having valid visa on it or any other proof of legal stay along with passport. **Note**: If only photocopies and not originals or certified true copies provided of the above, electronic verification is required of the authenticity and information contained in the photocopies. https://id.nadra.gov.pk/identity-documents/verification-services/
Date of Birth:	As above
Place of Birth:	As above
Gender M/F	
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 **Note: Only complete if the customer is a sole trader/proprietor. If not, then Part 3 is not applicable.**	**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	
Occupation or business	
What is the main source of income or wealth of the customer?	
Note: For customer subject to enhanced due diligence.	

PART 5: ARE YOU ACTING FOR SOMEONE ELSE?

If No, just marked as Not Applicable (N/A) **If yes, please provide details below**	
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:	Utility or telephone bill with physical address; or Other document with evidence of physical address
Relationship to customer: e.g. lawyer/accountant.	**Attach original of official company letter** authorising individual to enter into contractual relations with DPMS on behalf of the customer e.g. from the governing body/board if not a company director. .

PART 6: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION
Certificate of Registration, if sole trader/proprietor
Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA
If non-resident, Original or certified true copy of National Identity Card for Overseas Pakistanis (NICOP), Pakistan Origin Card, Alien Registration Card or foreign passport
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 (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 Act
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

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

PART 1. IDENTIFCATION INFORMATION	**VERIFICATION DOCUMENTS**
Full Legal Name:	Certificate of Incorporation Check online: https://eservices.secp.gov.pk/eServices/NameSearch.jsp
Director name (s):	CNICs/ Smart National Identity Card (SNIC) issued by NADRA of all directors Foreign passport
Company information (ownership and control)	Article of Association Memorandum of Association
Registration Number:	Certificate of Incorporation
Country of Incorporation:	Certificate of Incorporation
Date of Incorporation:	Certificate of Incorporation
Registered Address:	Certificate of Incorporation
Physical Address:	Certificate of Incorporation, Utility statement with address, telephone account statement with address, etc
Landline Number:	N/A
Email Address:	N/A

PART 2. BENEFICIAL OWNERSHIP INFORMATION	**VERIFICATION DOCUMENTS**

<table>
<tr>
<td>1. Shareholders:

e.g. Names of individuals (natural persons) shareholders holding 25% or above ownership

Note: This includes where the customer is owned by one or more companies.</td>
<td rowspan="4">Details of company:

1. SECP website to confirm registration: https://eservices.secp.gov.pk/eServices/NameSearch.js p

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

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

4. Register of beneficial Ownership maintained by the Company and Compliance Certificate, as required under Section 123A of the Companies Act

5. Articles of Association/Memorandum of Association

Details of individuals (beneficial owners):

Originals or certified true copies of:

1. Residents: CNICs/ Smart National Identity Card (SNIC) issued by NADRA

2. Non Residents:

National Identity Card for Overseas Pakistanis (NICOP) and/or Passport issued by NADRA for Non-resident / overseas Pakistanis or those who have dual nationality; or

Pakistan Origin Card (POC) issued by NADRA and/or Passport for Pakistanis who have given up Pakistan nationality; or

Form B or Juvenile card issued by NADRA to children under the age of 18
years; or

Where the natural person is a foreign national, either an Alien registration card (ARC) issued by NADRA or a Passport having valid visa on it or any other proof of legal residence together 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.

https://id.nadra.gov.pk/identity-documents/verificationservices/</td>
</tr>
<tr>
<td>2. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g.

- appoint or remove the majority of the board of directors, or its chair, or CEO of the company:</td>
</tr>
<tr>
<td>3. Name (s) of any other individual (s) with control, either direct or indirect over the company e.g.

- personal connections to persons in positions described above or that possess ownership
- close and intimate family relationships
- historical or contractual associations if a company defaults on certain payments</td>
</tr>
<tr>
<td>4. Senior managing official: Where no natural person is identified under 1 to 3 above after reasonable measures have been made

- the identity of the relevant natural person who holds the position of senior managing official.</td>
</tr>
</table>

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 4: DETAILS ON THE BUSINESS

1. Please provide details of the industry and business (e.g. products / services)	
2. Number of staff/employees?	
3. Does the company have operations in other geographic regions in Pakistan? 4. If the above is "Yes", please provide the names of those regions?	
5. Which are the primary countries in which the company has dealings with, if any?	
6. Does the company deal with any individual or entity from countries that are subject to UN sanctions or embargoes?;	
7. If the above is "Yes", please indicate the specific countries and the nature of those dealings?	

PART 5: SOURCE OF FUNDS OR WEALTH

4. What is the main source of funds or wealth of the business?	
5. Income last financial year?	
6. Assets held by the customer?	

Note: For customer subject to enhanced due diligence.

PART 6: INDIVDIUAL ACTING ON BEHALF OF COMPANY

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

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

PART 7: CHECKLIST OF DOCUMENTS TO BE ATTACHED, IF PAPER BASED VERIFICATION
1. Certificate of Incorporation
2. SECP registered declaration for commencement of business as required under the Companies Act, 2017 (XIX of 2017)
3. Register of Members of a Company, Section 119 of the Companies Act, 2017 (Act no. XIX of 2017)
4. Register of Beneficial Ownership Information, Section 123A of Companies Act and Compliance Certificate
5. Article of Association, Memorandum of Association
6. Original or certified true copy CNICs/ Smart National Identity Card (SNIC) issued by NADRA of all directors and beneficial owners
7. Original or certified true copy of National Identity Card for Overseas Pakistanis (NICOP), Pakistan Origin Card, Alien Registration Card or foreign passport of director and beneficial owner
8. Utility statement, telephone account statement etc with physical address
9. Letter authorising individual to act on behalf of the customer
Note: If only photocopies and not originals provided of the above, electronic verification is required of the authenticity and information contained in the photocopies.

DECLARATION BY PERSON AUTHORISED TO ACT ON BEHALF OF COMPANY:

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

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

Annex 5 - 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 Act
- Federal Board of Revenue Anti-Money Laundering and Combating Financing of Terrorism Regulations for Designated Non-Financial Businesses and Professions.

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

PART 1. BASIC IDENTIFCATION 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 CNIC/ Smart National Identity Card (SNIC) issued by NADRA
If non-resident, original or certified true copy of foreign passport
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:

Annex 6 – Red Flag Indicators for Proliferation Financing

Financial Monitoring Unit (FMU)
Government of Pakistan
2nd Floor, SBP Main Building, I.I Chundrigar Road, Karachi

RED FLAG INDICATORS FOR PROLIFERATION FINANCING (2020)

1. WHAT IS PROLIFERATION?

The definition of "Proliferation" provided in the FATF's 2008 Proliferation Financing Report [1]is: "Proliferation has many appearances but ultimately involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weaponrelated programs, including delivery systems; it poses a significant threat to global security." The Report, which identifies a link between proliferation of Weapons of Mass Destruction (WMD) and terrorism, states that: "If appropriate safeguards are not established, maintained and enforced for sensitive materials, technology, services and expertise, they can become accessible to individuals and entities seeking to profit from the acquisition and resale, or for intended use in WMD programs".

2. WHAT IS PROLIFERATION FINANCING (PF)?

The 2010 FATF's Guidance on Counter Proliferation Financing [2] defines "Proliferation Financing" as:

"the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".

The said report further adds that:

"PF facilitates the movement and development of proliferation-sensitive items and can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction (WMD) are developed and deployed".

3. INTERNATIONAL STANDARDS AND OBLIGATIONS TO COUNTER PROLIFERATION FINANCING RISKS

- The United Nation Security Council's Resolution (UNSCR 1540)

  On April 28, 2004 the UN Security Council adopted UNSCR 1540, which was established to prevent non-state actors from acquiring nuclear, biological, and chemical weapons, their means of delivery, and related materials. The resolution filled a gap in international law by addressing the risk that terrorists might obtain, proliferate, or use WMDs. The UNSCR 1540 imposed the following three (3) primary obligations upon its UN membership (including Pakistan) to restrict proliferation financing. The financial provisions of the Resolution require that all States:

  a. abstain from supporting non-State actors seeking WMDs and their means of delivery;

  b. adopt and implement effective laws (i.e. criminal or civil penalties for violations of export control laws) to prohibit non-State actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their means of delivery; and

[1] FATF PROLIFERATION FINANCING REPORT
https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

[2] FATF GUIDANCE ON COUNTER PROLIFERATION FINANCING
http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf

c. establish and enforce effective measures and domestic controls (i.e. export and transhipment controls) to prevent the proliferation of nuclear, chemical, or biological weapons, their means of delivery and related materials.

- The Financial Action Task Force (FATF) Recommendations & Immediate Outcomes

Recommendation 7 of the FATF Standards requires countries to implement proliferation financingrelated Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs or resolutions). Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD). Immediate Outcome 11 and certain elements of Immediate Outcome 1 relating to national cooperation and coordination aim to measure how effective countries are implementing these Recommendations.

4. Pakistan's Regulatory Framework for Combating Proliferation Financing

To address the risk of proliferation financing and to comply with the above requirements of UNSCR 1540 and FATF's Recommendations and Immediate Outcomes, Pakistan has established relevant legislations, regulations and guidelines which include but not limited to following:

- Anti-Money Laundering Act 2010 (as amended up to Sep 2020);
- Anti-Terrorism Act 1997;
- United Nations (Security Council) Act, I948;
- State Bank of Pakistan's AML/ CFT/ CPF Regulations (Issued on 30 Sep 2020);
- AML / CFT Regulations Issued by SECP;
- Federal Board of Revenue AML/CFT Regulations for DNFBPs, 2020;
- National Savings (AML and CFT) Regulations, 2020;
- ICAP's AML / CFT Regulations for Chartered Accountants Reporting Firms; and ICMAP's AML / CFT Regulations for Cost Accountants Reporting Firms.
- Guidelines on TFS and UNSC Resolutions by AML / CFT Regulatory Bodies.

Moreover, Strategic Export Control Division (SECDIV), Ministry of Foreign Affairs of Pakistan has also issued detailed guidance document namely "Guidelines on the Implementation of the UN Security Council Resolutions Concerning Targeted Financial Sanctions on Proliferation Financing"[3].

5. Red Flags Indicators for Proliferation Financing

To identify a suspicion that could be indicative of proliferation financing activity, FMU has prepared the red flags indicators that are specially intended as an aid for the reporting entities. These red flags may appear suspicious on their own; however, it may be considered that a single red flag would not be a clear indicator of potential proliferation financing activity. A combination of these red flags, in addition to analysis of expected overall financial activity, business profile may indicate towards potential proliferation financing activity.

Customer Behavior:

1. When customer is involved in the supply, sale, delivery or purchase of dual-use, proliferationsensitive or military goods, particularly to higher risk jurisdictions.
2. When customer or counter-party, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.
3. The customer is a research body connected with a higher risk jurisdiction of proliferation concern.
4. When customer's activities do not match with the business profile provided to the reporting entity.
5. When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.

[3] GUIDELINES ON THE IMPLEMENTATION OF THE UN SECURITY COUNCIL RESOLUTIONS CONCERNING TARGETED
FINANCIAL SANCTIONS ON PROLIFERATION FINANCING
http://secdiv.gov.pk/uploads/CRMC_Guidelines_on_TFS_for_PF-38da.pdf

6. When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
7. When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
8. When final destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.

Transactional Patterns:

1. Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
2. The transaction(s) involve an individual or entity in any country of proliferation concern.
3. The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
4. The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
5. Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
6. When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.

Disclaimer:

These red flags are developed for guidance purpose and may appear suspicious on their own; however, it may be considered that a single red flag would not be a clear indicator of potential PF activity. However, a combination of these red flags, in addition to analysis of overall financial activity and client profile may indicate a potential PF activity. While every effort has been made to ensure the accuracy and check all relevant references/ resources, errors and omissions are possible and are expected. Financial Monitoring Unit (FMU), its officers and its stakeholders are not responsible for any mistakes and/or misinterpretation.

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

Document	Weblink
1. AMLA 2010	http://www.fmu.gov.pk/Anti-Money- Laundering-Act-2010-asamended-upto-Feb.-2020.pdf
2. ATA	http://www.fmu.gov.pk/wp-content/uploads/2020/04/The-AntiTerrorism-Act-1997-as-amended-upto-Feb-2017-1.pdf
3. AML Regulations 2015	http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf
4. FBR AML/CFT Regulations for DNFBPs	http:FBR AML/CFT Regulations for DNFBPs.pdf
5. AML/CFT Sanction Rules	https://AML-CFT-Sanction-Rules-2020-SRO-NO-950I-2020.pdf
6. Circular for DPMS – Red Flags	https://www.fmu.gov.pk/docs/Red-Flag-Indicators-for-Jewelersand-Precious-Stones-or-Metal-Dealers-Final.pdf
7. Guidelines on filing of Suspicious Transaction Reports for the Reporting Entities	http://www.fmu.gov.pk/wp-content/uploads/2020/05/Circular02-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/wpcontent/uploads/2020/05/Guidelines-on-Reporting-of-SuspiciousTransaction-Reports-STRs-on-Designated-Proscribed-IndividualsEntities-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-StakeholdersLEAs-Updated-Version.pdf
10. FMU reporting forms	http://www.fmu.gov.pk/reporting-forms/
11. Introducing Guidelines for DNFBPs on Targeted Financial Sanctions under UN Security Council Resolutions - FBR	https://download1.fbr.gov.pk/Docs/20201021610362290TargetedFinancialSanctionsStatutoryRegulation.pdf
12. SECP Beneficial Ownership Guidelines	https://www.secp.gov.pk/UBO

13. FATF	http://www.fatf-gafi.org/.
14. APG	http://www.apgml.org/
15. Responsible Jewellery Council	https://www.responsiblejewellery.com/