Government of Pakistan
Finance Division
(CDNS Section)
***

SUBJECT: **GUIDELINES AND TEMPLATE FOR CDNS IN IDENTIFICATION, ASSESSING AND UNDERSTANDING ITS MONEY LAUNDERING (ML), TERRORISM FINANCING (TF) AND PROLIFERATION FINANCING (PF) RISKS**

Reference to the subject noted above.

2. Supervisory Board has [illegible] approved the Guidelines and Template for CDNS on Money Laundering (ML), Terrorism Financing (TF) and Proliferation (PF) RISKS Assessment **(Annexed)**

3. CDNS is requested to take further necessary action, accordingly, please.

Encl: As above.

DIRECTOR GENERAL
925
3.12.2020

(Fahad Ahmed)
Section Officer (CDNS)
051-9204799

Director General, CDNS, Islamabad.

Fin. Div. U.O. No.F.16 (1)-GS-I/2019-1492 Dated: 02.12.2020

National Savings (AML-CFT) Supervisory Board

Islamabad

Guidelines and Template for CDNS

on

ML / TF / PF Risk Assessment

Table of Contents

1 Introduction and Background

1.1 Background

In line with Section 7F of Anti-Money Laundering Act 2010 and Chapter II (Risk Assessment and Mitigation) of National Savings (AML and CFT) Regulations 2020, the National Savings (AML and CFT) Supervisory Board is pleased to share following guidelines and template for CDNS in identification, assessing and understanding its Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF) Risks.

Under Section 3 of National Savings (AML and CFT) Regulations 2020 the CDNS shall document its risk assessment considering all relevant risk factors and provide risk assessment information to National Savings AML and CFT Supervisory Board.

The internal ML/TF/PF risk assessment is not a one-time exercise and must be kept up to date. CDNS updates its internal risk assessment on yearly basis. CDNS conducted its last internal risk assessment in 2019 in light of ML/TF NRA 2019 update.

In order to document the identified ML/ TF/ PF risks, CDNS shall prepare Internal Risk Assessment Report which shall cover ML/ TF/ PF risks and other emerging risks to and from CDNS. The report shall identify, assess, and understand ML/ TF/ PF risks at entity level for customers, products, services, delivery channels, technologies, and their Geographies of Operations.

The ultimate responsibility of ensuring effective AML/ CFT/ CPF controls rests with CDNS. Therefore, CDNS shall ensure adequate, reliable, periodic management information system, from senior management, for ensuring effective oversight, monitoring and accountability. CDNS shall ensure adequate monitoring mechanism to assess ML/ TF/ PF risks and adequacy of AML/ CFT/ CPF controls including STR/ CTR and TFS through internal audit, transaction monitoring and name screening etc.

1.2 Risk Based Approach

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

1.3 Internal Risk Assessment

The key purpose of CDNS internal ML/TF/PF risk assessment is to drive improvements in risk management through identifying the general and specific ML, TF and PF risks CDNS is facing, determining how these risks are mitigated by CDNS AML/CFT programme controls, and

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

The CDNS Internal Risk Assessment Report will take into account results of National Risk Assessment (NRA) and its subsequent updates shared with CDNS, major international/ domestic financial crimes and terrorism incidents that have probability of posing ML/ TF/ PF risks to the entity itself, to other entities and to the Pakistan's financial sector. Further, feedback from National Savings (AML and CFT) Supervisory Board, FMU, LEAs, and other related stakeholders should be taken into account.

The CDNS Internal Risk Assessment Report will also assess effectiveness of existing Anti Money Laundering (AML), Combating Financing of Terrorism (CFT) and Countering Proliferation Financing (CPF) policies/ controls/ obligations/ preventive measures.

The CDNS Internal Risk Assessment Report will be presented to the by National Savings (AML and CFT) Supervisory Board. It will include recommendations for the CDNS along with a time bound action plan for mitigation of ML/ TF/ PF risks and ensuring effective AML/ CFT/ CPF policies/ procedures/ controls/ obligations/ preventive measures. Further, the recommendations in CDNS Risk Assessment Report should cover measures for improvement in understanding of ML/ TF/ PF risks of employees, senior management and adequacy of resources i.e. systems and human resource etc.

CDNS will formulate policy for application of SDD, CDD and EDD in light of levels of ML/ TF/ PF risks identified as low, medium, or high in their internal Risk Assessment Report, and as prescribed by National Savings (AML and CFT) Supervisory Board from time to time.

1.4 Difference between an inherent and residual risk assessment

An inherent risk assessment represents CDNS's exposure to ML, TF and PF risks in the absence of any mitigation measures, namely no AML/CFT procedures or controls. A residual risk assessment is done after the mitigating effects of AML/CFT controls have been accounted for.

While not explicitly stated in the AML/CFT legislations, the expectation is that an inherent enterprise risk assessment should be conducted. CDNS may choose to undertake a residual risk assessment, but the inherent risks must be clearly identified.

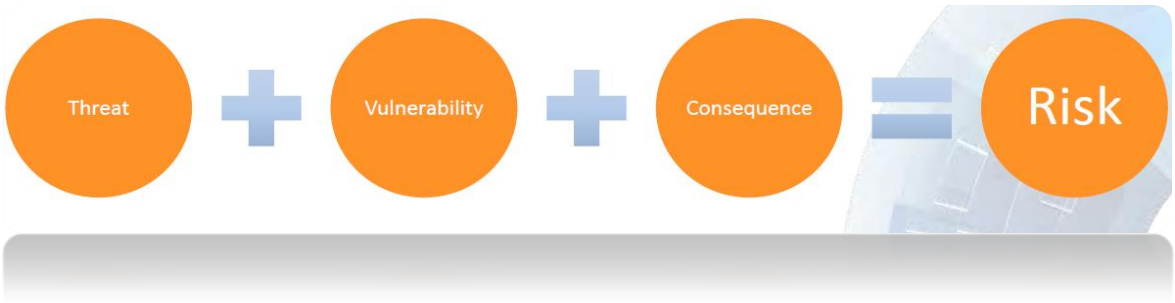
2 Risk assessment Guidelines

2.1 How to conduct risk assessment on ML/TF/PF

The following explains the key steps in conducting an internal risk assessment i.e. understand the meaning of ML/TF/PF risks, identify the risk categories and then assess the risk.

2.1.1 Step 1 – What is ML/TF/PF Risk

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



Threat: A threat is usually an external element. A threat can be a walk in customer of CDNS i.e. person or a legal person with the intention or potential to cause harm by ML,TF or PF.

Vulnerability: A vulnerability is usually an internal element. A vulnerability can be a CDNS product that can be exploited by the threat, or a delivery channel that may support or facilitate a threat.

Consequence: A consequence refers to the impact or harm that a threat may cause to CDNS or financial sector or Pakistan. When determining impact of ML/TF/PF, the CDNS may consider a number of factors, including:

- Nature, size or branch network of CDNS;
- Potential criminal, financial and reputational consequences to CDNS;
- Terrorism-related impacts;
- Wider criminal activity and social harm;
- Political impact;
- Negative media.

2.1.2 Step 2 – Identify the Risks

Section 3 in the National Savings AML/CFT Regulations 2020 specifies the following four mandatory risk categories:

- Customer risk
- Countries or geographic risk
- Products and services risk
- Transaction or delivery channel risk

Weighting: The above risk categories may be weighted, or you may decide to assign equal weighting to each e.g. 25%. For example, as CDNS has no international exposure and all its products, branch network is based in in Pakistan that is not higher risk, then geographic risk may not be a significant risk category.

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

Customer with intention or potential to cause harm by ML/TF/PF

CDNS should consider the following questions;

- Does the customer or its beneficial owners have characteristics known to be frequently used by money launderers or terrorist financiers?
- Are they involved in occasional or one-off activities / transactions above a certain reasonable threshold?
- Do your customers use complex business structures that offer no apparent financial benefits?
- Are they politically exposed person (PEP) or their close relative or associate?
- Are your customer involved in cash-intensive business?
- Are they involved in businesses associated with high levels of corruption?
- Do they have unexplained or hard to verify source of wealth and / or source of funds?
- Do they conduct business through, or are they introduced by, gatekeepers such as accountants, lawyers, or other professionals?
- Are they a non-profit organisation?

A ‘Yes’ or ‘Don’t know’ answer will show higher risk of ML/TF/ PF risk.

Certain customer types or legal persons present more ML/TF risk than others. These are also pointed out in **FATF material** and **ML/TF NRA and its Updates**.

Geographical Vulnerabilities to ML/TF/PF

CDNS should consider the following question; Are our customers established in countries or regions (including within Pakistan) that are known to be used by money launderers or terrorist financiers?

Certain geographies present more ML/TF risk than others. These are also pointed out in **FATF material** and **ML/TF NRA and its Updates**. Though it should be borne in mind that lower risk and legitimate customers may be located in high risk countries.

Products and Services Vulnerable to ML/TF/PF

The products CDNS offers are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF or PF. CDNS should consider the following question; Do any of our Products have attributes known to be used by money launderers or terrorist financiers or proliferation financiers?

There are certain specific factors that increase risk such as cash, cross border transfers etc. Some of the main ones are as follows:

- Is the product bearer in nature and allows for anonymity i.e. is bearer in nature?
- Can the product disguise or conceal the beneficial owner of your customer?
- Can the product disguise or conceal the source of wealth or funds of your customer?
- Does the product allow payments to third parties?
- Does the product commonly involve receipt or payment in cash?
- Has the product been identified in the **ML/TF NRA and it's Updates** as presenting a higher ML/TF risk?
- Does the product allow for the movement of funds across borders?

A 'Yes' or 'Don't know' answer will show higher vulnerability to ML/TF/ PF risk.

Transaction or Delivery Channels Vulnerable to ML/TF/PF

How CDNS delivers products and services to its customers are also vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF or PF. CDNS should consider the following question; Does the fact that I am dealing with the customer non face to face pose a greater ML/TF risk?

There are certain specific factors that increase risk. The higher risk factors could include the following:
Can your business / product / service have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
Do you provide your products / services via the internet?
Do you provide your products / services via agents or intermediaries?
Can you provide your products / services to overseas Customers or in Overseas Jurisdictions?
Can your delivery channel / transaction method allow for anonymity?
Can your delivery channel / transaction method disguise or conceal the beneficial owner of your customer?

2.1.3 Step 3- Assess the Risk

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

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

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

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

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

i. ***Customer 1*** is a Pensioner. In this scenario, it is possible but highly unlikely the Pensioner would engage in ML. The consequence may be minor because of the limited products on offer for Term Deposit used to invest his or her Pension or Savings. The inherent risk is therefore low (*refer to above matrix*).

ii. ***Customer 2*** is a well-known company in educational services which is customer of CDNS or the last 10 years. In this scenario, it is unlikely that such a company would try to launder funds, as it would damage the reputation of the well reputed company. But the consequence may still be moderate as the amount invested may be high and CDNS may be heavily penalized by the Supervisory Board. The inherent risk is therefore medium (*refer to above matrix).*

iii. ***Customer 3*** is a politically exposed person who has been alleged to be engaged in corruption who has invested high amounts in terms deposits of purchase of Prize Bonds. The likelihood that he/she may be engaged in ML is likely - highly probable. The consequence is significant because of the negative reputational damage (e.g. extensive media coverage) and possible severe penalties – because CDNS is providing higher risk products knowing that the customer is a PEP. The inherent risk is therefore high (*refer to above matrix*).

CDNS does not need to risk rate each individual customer and may group customers with similar characteristics or risks for the efficient and broad base risk assessment.

3 CDNS Risk Assessment Template

Risk Assessment Template with mitigation measures					
Customer - *types of customers we deal with*	**Are any of my CDNS's customers a higher or lower threat for ML/TF/PF?**	**Likelihood rating of ML/FT/PF *(refer table)***	**Consequence rating of ML/TF/PF - minor, moderate, significant, severe *(refer table)***	**ML/TF/PF Risk level High, Medium, or Low *(refer table)***	**Risk Mitigation Measures**
Pensioner	Yes, lower risk	Unlikely	Minor	Low	Simplified CDD
Sole Proprietorship	Overall, medium risk. Business not in higher risk sector and is not cash intensive	Unlikely overall, although some may be higher risk	Minor/ Moderate	Medium	Standard CDD
Associate of PEP	**May be related to PEP**	**Likely**	**Significant**	**High**	**Enhanced CDD**
Businessman or Business in High Risk Sector	**Jeweller or real estate business. Higher risk business and sectors – cash intensive.**	**Likely**	**Significant**	**High**	**Enhanced CDD** **Specialised training on beneficial ownership and ML/TF risks**
Customer in news being audited by FBR	**Yes, as source of funds not totally clear**	**Likely**	**Moderate**	**Standard**	**Review transactions**

Geographic locations/ *countries or region we deal with*	**Is it considered higher risk? Why?**	**Likelihood rating of ML/FT**	**Consequence rating of ML/TF**	**Risk level High, Medium, or Low**	**Risk Mitigation Measures**
Pakistani National based overseas in FATF countries with family in Pakistan	Standard risk because of geography	Unlikely	Moderate	Medium	Standard CDD
Pakistani National based in FATF Black Listed Country	**Yes FATF Black List country**	**Likely**	**Moderate/ Significant**	**High**	**Enhanced CDD on source of funds** **Transaction monitoring** **Regular update of EDD**
Products and Services Risk - *types of products and services we offer*	**Are my services/ product at higher risk of abuse?**	**Likelihood rating of ML/FT**	**Consequence rating of ML/TF**	**Risk level High, Medium, or Low**	**Risk Mitigation Measures**
Receipts or Payments in Cash	**Yes, higher risk based on indicators**	**Likely**	**Significant**	**High**	**Enhanced CDD** **Regular reviews of transactions** **Adopt policy of no cash payments or impose threshold**
Sale and Purchase of Unregistered Prize Bonds	**Yes, risk of abuse for ML or TF**	**Likely**	**Significant**	**High**	**Enhanced CDD on source of funds** **Regular reviews**

					of transactions
Deposit Certificates for General Public	No	Unlikely	Moderate	Medium	Standard CDD
Deposit Certificates available for Pensioners only	Yes, lower risk	Unlikely	Minor	Low	Simplified CDD
Delivery Channels - *how we deliver our services*	**Are my delivery channels more vulnerable to potential abuse?**	**Likelihood rating of ML/FT**	**Consequence rating of ML/TF**	**Risk level High, Medium, or Low**	**Risk Mitigation Measures**
Face-to-face	No, standard risk	Unlikely/ likely	Moderate	Medium	Standard CDD
Through Internet or other Non-face-to-face delivery channel for non-resident customers/ counter parties	**Yes, as they are also based overseas**	**Likely**	**Significant**	**High**	**Enhanced CDD** **Electronic verification** **Regular account monitoring**