Risk Assessment Guideline for Banking Sector

Chapter: One
Overview of AML/CFT Risk

1. Introduction

As a lead agency for prevention of money laundering and combating financing of terrorism, Bangladesh Financial Intelligence Unit (BFIU) is very keen to achieve highest success in this regard. The success of AML/CFT program highly depends on efficient assessment of related risk/vulnerability/threat and placing combating tools as per the result of assessed risk/vulnerability/threat.

The purpose of this guideline is to:

- provide general information about risks related with the products, services, delivery channels, and geographical locations;
- assist reporting entities to assess their risks efficiently;
- enable reporting entities in implementing an AML/CFT program appropriate to their business having regard to the business size, nature and complexity; and
- provide a broad risk management framework based on high-level principles and procedures that a reporting entity may wish to consider when developing and implementing a risk-based approach to identify, mitigate and manage ML/TF risks.

1.2 What are the obligation for such Risk Assessment and Management?

As per the first Recommendation of Financial Action Task Force (FATF) revised 40 Recommendations, each country should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

BFIU is the lead agency for AML/CFT issues in Bangladesh. Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML/CFT regime. Every reporting agency has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act, 2012 and Anti Terrorism Act, 2009. This Guideline has been issued through BFIU circular aiming to strengthen AML/CFT regime in Bangladesh. Therefore, it is obligatory for all reporting entities to comply with this Guideline.

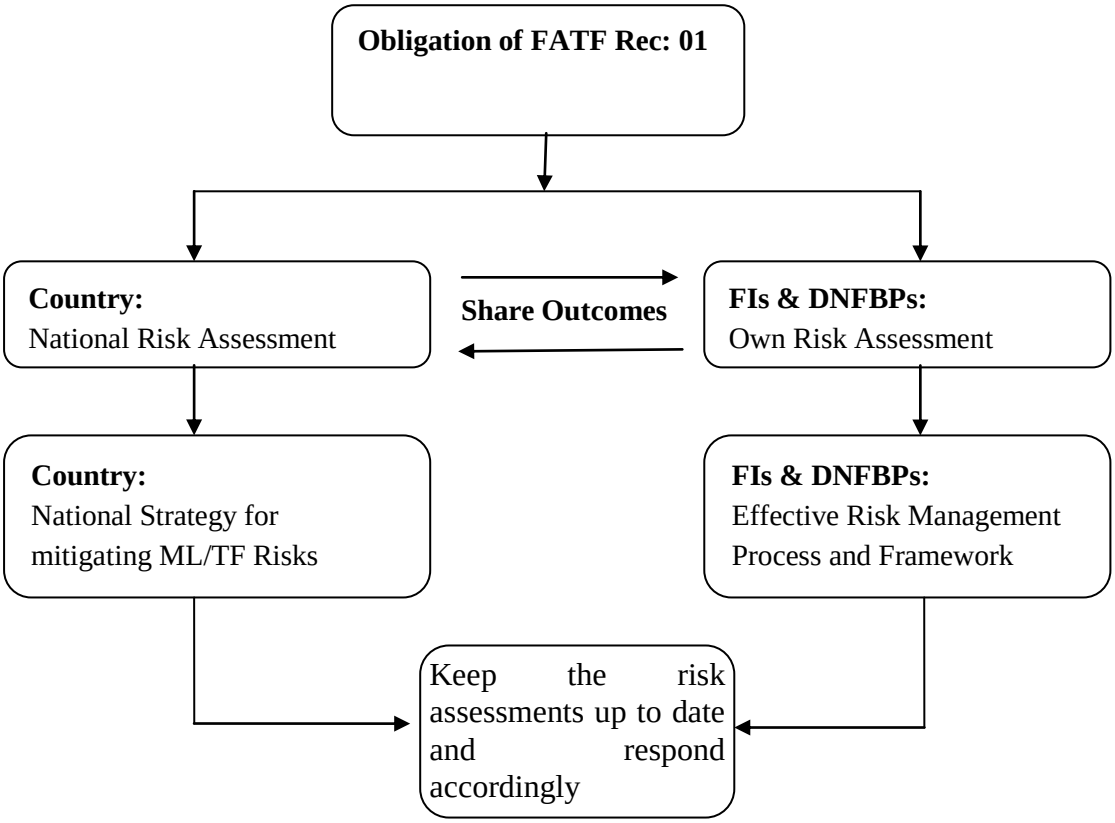
1.3 Assessing risk:

Financial institutions should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and self regulatory bodies (SRBs).

1.4 Risk management and mitigation:

Financial institutions should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

The obligation of FATF Recommendation-1 may be shown as follows:



1.5 What is risk?

Risk can be defined as the combination of the probability of an event and its consequences. In simple terms risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

1.6 What is risk management?

Risk management is the process of recognizing risk and developing methods to both minimize and manage the risk. This requires the development of a method to identify, prioritize, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

1.7 Which risks do you need to manage?

For the ML/TF environment, BFIU generally expects a business's risk management practice to address two main risks: business risk and regulatory risk.

Business risk is the risk that your business may be used for ML/TF. Businesses must assess the following risks in particular:

- customer risks
- products or services risks
- business practices and/or delivery method risks
- country or jurisdictional risks.

Regulatory risk is associated with not meeting all obligations of reporting entity under the Money Laundering Prevention Act, 2012 and Anti Terrorism Act, 2009 (including all amendments) and the respective Rules issued under these two acts. Examples of regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML/CFT program (how a business identifies and manages the ML/TF risk it may face) etc.

It is unrealistic that a business would operate in a completely risk-free environment in terms of ML/TF. Therefore, it is suggested that a business identifies the ML/TF risk it faces, and then works out the best ways to reduce and manage that risk. In doing this, it is necessary to balance the costs to the business and customers against the risk of the business being used for ML/TF. This should be in proportion to the size of the business and the availability of the resources.

Chapter: Two

Risk Management Framework

2.1 Introduction

The reporting entities will have flexibility to construct and tailor their risk management framework for the purpose of developing risk-based systems and controls and mitigation strategies in the manner most appropriate to their business structure (including financial resources and staff), their products and/or the services they provide. Such risk-based systems and controls should be proportionate to the ML/TF risk(s) a reporting entity reasonably faces.

The risk management framework discussed in this guideline aims to assist reporting entities to develop and implement their AML/CFT programs in compliance with the local laws and international standards and best practices.

Generally, BFIU expects reporting entities to develop and maintain logical, comprehensive and systematic methods to address each of the components referred to in this Guideline and that such methods and the entities' approach to ML/TF risk are understood, implemented and maintained, to some appropriate extent, within their organizations.

Reporting entities would be expected to demonstrate to BFIU (for example, when an BFIU audit is being conducted) that their risk based systems and controls are suitable to their particular businesses and consistent with prudent and good practices.

A risk management framework would consist of:

(a) establishing the internal and external context within which the designated service is, or is to be, provided (that is, the customer types, types of services, delivery methods and any dealings with foreign jurisdictions);

(b) identifying risks;

(c) evaluating or assessing risks; and

(d) treating risks (mitigating, managing, control, monitoring and periodic reviews).

Figure 1: The risk management framework at a glance

- **Risk identification:**

Identify the main ML/TF risks:
• customers
• products & services
• business practices/delivery methods
• country/jurisdiction

Identify the main regulatory risks:

- Failure to report STRs/SARs
- Inappropriate customer verification
- Lack of AML/CFT program

- **Risk assessment/measurement**

Measure the size & importance of risk:
• likelihood – chance of the risk happening
• impact – the amount of loss or damage if the risk happened
• likelihood X impact = level of risk (risk score)

- **Risk treatment**

Manage the business risks:
• minimize and manage the risks
• apply strategies, policies and procedures

Manage the regulatory risks:
• put in place systems and controls
• carry out the risk plan & AML/CFT program

- **Risk monitoring and review**

Monitor & review the risk plan:
• develop and carry out monitoring process
• keep necessary records
• review risk plan and AML/CFT program
• do internal audit or assessment
• do AML/CFT compliance report

2.2 The risk management process

2.2.1 Risk identification:

Identify the main ML/TF risks:
• customers
• products & services
• business practices/delivery methods
• country/jurisdiction

Identify the main regulatory risks:

- Failure to report STRs/SARs
- Inappropriate customer verification
- Lack of AML/CFT program

The first step is to identify what ML/TF risks exist in a business when providing designated services. As previously discussed, there are two risk types: **business risk and regulatory risk.**

- **Business risk**

A reporting entity must consider the risk posed by any element or any combination of the elements listed below:

- Customers
- Products and services
- Business practices/delivery methods (channels)
- Countries it does business in/with (jurisdictions).

Under these four groups, individual risks to a business can be determined. While not an exhaustive list, some of these individual risks may include:

- **Customers:**
  - a new customer
  - a new customer who wants to carry out a large transaction
  - a customer or a group of customers making lots of transactions to the same individual or group

- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- a customer who brings in large amounts of used notes and/or small denominations.
- a customer who has relationship with unusual circumstances.
- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex.

➢ **Products and services:**

- private banking
- credit card
- anonymous transaction
- non face to face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed.

➢ **Business practice/delivery method (channels):**

- direct to the customer
- online/internet
- phone
- fax
- email
- third-party agent or broker.

➢ **Country/jurisdiction:**

- any country which is unidentified by credible sources as having significant level of corruption and criminal activity;
- any country subject to trade sanctions

- any country known to be a tax haven and unidentified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country.
- any country unidentified by credible sources as not having adequate AML/CFT system.

- **Regulatory risk**

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012 and Anti Terrorism Act, 2009 (including all amendments). Examples of some of these risks are:

- customer identification and verification not done properly
- failure to scrutinize staffs properly
- ~~not having data in relation to customer adequately~~
- failure to train staff adequately
- not having an AML/CFT program
- failure to report suspicious matters
- not submitting an AML/CFT compliance report
- not having an AML/CFT Compliance Officer

2.2.2. Risk assessment:

For assessing risk, in this chapter we have used, the Table -1, which is a simple & generic table with Risk Score and Treatment. Risk Score can be found by blending likelihood and impact; the details will be explained later on. Table -1 is used, only the examples of customer risk assessment and developed phase by phase so that user can have a good idea of risk assessment.

Table 1: Risk Management Worksheet – risk

Risk group:	**Customers**			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
New customer *(example only)*				
Customer who brings in large amounts of used notes and/or small denominations *(example only)*				
Customer whose business address and registered office are in different geographic locations *(example only)*				

A table similar to *Table 1* shown above - *Risk management worksheet* - could be used for each risk group in preparation for assessing and managing those risks: customers, products and services, business practices/delivery methods, country/jurisdiction and the regulatory risks.

2.2.3. Calculation of Risk Score:

Measure the size & importance of risk:
- likelihood – chance of the risk happening
- impact – the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)

Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

Therefore each risk element can be rated by:

- the chance of the risk happening – **'likelihood'**
- the amount of loss or damage if the risk happened – **'impact' (consequence)**.

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood *(Table 2) on page 13* and impact *(Table 3) on page 14* and from these get a level of risk or risk score using the risk matrix *(Figure 2) on page 14*.

LIKELIHOOD	**X**	**IMPACT**	=	**RISK LEVEL/SCORE**

- **Likelihood scale**

A likelihood scale refers to the potential of an ML/TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in Table 2, but the entity can have as many as they believe are necessary.

Table 2: Likelihood scale

Frequency	Likelihood of an ML/TF risk
Very likely	**Almost certain: it will probably occur several times a year**
Likely	**High probability it will happen once a year**
Unlikely	**Unlikely, but not impossible**

- **Impact scale**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. It does not cover everything and it is not prescriptive. Impact of an ML/TF risk could, depending on individual business circumstances, be rated or looked at from the point of view of:

- how it may affect the business (if through not dealing with risks properly the entity suffer a financial loss from either a crime or through fines from the regulator)
- the risk that a particular transaction may result in the loss of life or property through a terrorist act
- the risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud
- the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- reputational risk – how it may affect the business if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers
- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

Three levels of risk are shown in Table 3, but the entity can have as many as they believe are necessary.

Table 3: Impact scale

Consequence	Impact – of an ML/TF risk
Major	**Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**
Moderate	**Moderate level of money laundering or terrorism financing impact.**
Minor	**Minor or negligible consequences or effects.**

- **Risk matrix and risk score**

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix *(Figure 2)* and risk score table *(Table 4)* shown below. Four levels of risk or score are shown in Figure 2 and Table 4, but the entity can have as many as they believe are necessary.

Figure 2: Risk matrix

Threat level for ML/TF risk

LIKELIHOOD

Very Likely	**Medium 2**	**High 3**	**Extreme 4**
Likely	**Low 1**	**Medium 2**	**High 3**
Unlikely	**Low 1**	**Low 1**	**Medium 2**
	Minor	**Moderate**	**Major**

What is the chance it will happen?

How serious is the risk?

IMPACT

Table 4: Risk score table

Rating	Impact – of an ML/TF risk
4 Extreme	**Risk almost sure to happen and/or to have very serious consequences.** **Response:** **Do not allow transaction to occur or reduce the risk to acceptable level.**
3 High	**Risk likely to happen and/or to have serious consequences.** **Response:** **Do not allow transaction until risk reduced.**
2 Medium	**Possible this could happen and/or have moderate consequences.** **Response:** **May go ahead but preferably reduce risk.**
1 Low	**Unlikely to happen and/or have minor or negligible consequences.** **Response:** **Okay to go ahead.**

- **Risk Assessment and Management Exercise:**

From the above discussion, the entity will have an idea to calculate risk score by blending likelihood and impact, risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet (Table-01). It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the reporting agencies would be called together **"Risk Registrar"** and this **"Risk Registrar"** is under the authority or control of BFIU.

Once threat levels and risk scores have been allocated the entity can be entered in the risk management worksheet *(Table 5)* next to the risk.

Table 5: Risk management worksheet – threat level and risk score

Risk group:	**Customers**			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
New customer *(example only)*	**Likely *(example only)***	**Moderate *(example only)***	**2 *(example only)***	
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	**Likely *(example only)***	**Major *(example only)***	**3 *(example only)***	
Customer whose business address and registered office are in the different geographic location *(example only)*	**Very likely *(example only)***	**Major *(example only)***	**5 *(example only)***	

2.2.4 Risk treatment

Manage the business risks:
- minimize and manage the risks
- apply strategies, policies and procedures

Manage the regulatory risks:
- put in place systems and controls
- carry out the risk plan & AML/CFT program

This stage is about identifying and testing methods to manage the risks the entity may have identified and assessed in the previous process. In doing this they will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment step are:

- setting transaction limits for high-risk products
- having a management approval process for higher-risk products
- process to place customers in different risk categories and apply different identification and verification methods
- not accepting customers who wish to transact with a high-risk country.

Table 6: Risk management worksheet – risk treatment or action

Risk group:	**Customers**			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
New customer *(example only)*	Likely *(example only)*	Moderate *(example only)*	2 *(example only)*	**Standard ID check**
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	Likely *(example only)*	Major *(example only)*	3 *(example only)*	**Standard + additional ID check**
Customer whose business address and registered office are in the different geographic location *(example only)*	Very likely *(example only)*	Major *(example only)*	5 *(example only)*	**Do not accept as customer**

Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. The entity may choose to use a combination of customer, product/service and country risk to modify an overall risk. For example, in the case of a remitter, for a low-risk customer, the entity may decide to use a bank account-to-bank account service only (assessed as low risk by them) to a certain city/province (assessed as a high risk area by them) in a certain country (assessed as low risk by them).

It is important to remember that identifying, for example, a customer, transaction or country as high risk does not necessarily mean that money laundering or terrorism financing is involved. The opposite is also true: just because a customer or transaction is seen as low risk does not mean the customer or transaction is not involved in money laundering or terrorism financing. Experience and common sense should be applied to the risk management process of an entity.

2.2.4 Monitor and review

Monitor & review the risk plan:
- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML/CFT program
- do internal audit or assessment
- do AML/CFT compliance report

Keeping records and regular evaluation of the risk plan and AML/CFT program is essential. The risk management plan and AML/CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law.

Once documented, the entity should develop a method to check regularly on whether AML/CFT program is working correctly and well. If not, the entity needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML/CFT Act and respective Rules.

2.2.5 Additional tools to help risk assessment

The following tools or ideas can be useful in helping to manage risk. It can be included in the previous risk assessment process so that the decisions are to be better informed.

2.2.6 Applying risk appetite to risk assessment

Risk appetite is the amount of risk a business is prepared to accept in pursuit of its business goals. Risk appetite can be an extra guide to the risk management strategy and can also help deal with risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

- What risks will the business accept?
- What risks will the business not accept?
- What risks will the business treat on a case by case basis?
- What risks will the business send to a higher level for a decision?

The risk matrix can be used to show the risk appetite of the business.

In a risk-based approach to AML/CFT the assessment of risk appetite is a judgment that must be made by the reporting business. It will be based on its business goals and strategies, and an assessment of the ML/TF risks it faces in providing the designated services to its chosen markets.

Figure 3: Sample risk matrix showing risk appetite

LIKELIHOOD			
Very Likely	**Acceptable Risk** Medium 2	**Unacceptable Risk** High 3	**Unacceptable Risk** Extreme 4
Likely	**Acceptable Risk** Low 1	**Acceptable Risk** Medium 2	**Unacceptable Risk** High 3
Unlikely	**Acceptable Risk** Low 1	**Acceptable Risk** Low 1	**Acceptable Risk** Medium 2
What is the chance it will happen?	**Minor**	**Moderate**	**Major**

How serious is the risk? IMPACT

2.2.7 Risk tolerance

In addition to defining business's risk appetite, the entity can also define a level of variation to how it manages that risk. This is called risk tolerance, and it provides some flexibility whilst still keeping to the risk framework that has been developed.

An example showing how risk appetite and risk tolerance interact follows:

A remitter business has decided that generally the risk is unacceptable to remit money to a particular country. However, the remitter does have some risk tolerance. In this case the business will remit to this region provided that it is a bank to bank transaction only, the customer provides three verifiable customer identification documents and the transaction is signed off by a senior manager.

Chapter: Three

Risk management: some important issues

3.1 Risk Management Strategies:

The reporting entity may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

a) reviews at senior management level of the reporting entity's progress towards implementing stated ML/TF risk management objectives

b) clearly defined management responsibilities and accountabilities regarding ML/TF risk management

c) adequate staff resources to undertake functions associated with ML/TF risk management

d) specified staff reporting lines from ML/TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system

e) procedural controls relevant to particular designated services

f) documentation of all ML/TF risk management policies

g) a system, whether technology based or manual, for monitoring the reporting entity's compliance with relevant controls

h) policies to resolve identified non-compliance

i) appropriate training program(s) for staff to develop expertise in the identification of ML/TF risk(s) across the reporting entity's designated services

j) an effective information management system which should:

   i) produce detailed and accurate financial, operational and compliance data relevant to ML/TF risk management

   ii) incorporate market information relevant to the global AML/CFT environment which may assist the reporting entity to make decisions regarding its risk management strategy

   iii) enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML/CFT Compliance Officer) within the reporting entity

   iv) allow the reporting entity to identify, quantify, assess and monitor business activities relevant to ML/TF risk(s)

v) allow the reporting entity to monitor the effectiveness of and compliance with its internal AML/CFT systems and procedures

vi) allow the reporting entity to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

It should be noted that a reporting entity can adopt other strategies in addition to taking into account of any of the above factors (where relevant), if it considers this approach is appropriate in accordance with its risk management framework.

3.2 Ongoing Risk Monitoring

A reporting entity's ongoing monitoring of its risk management procedures and controls may also alert the entity to any potential failures including (but not limited to):

a) failure to include all mandatory legislative components

b) failure to gain board and/or executive approval of the AML/CFT program

c) insufficient or inappropriate employee due diligence

d) frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s)

e) changes in business functions which are not reflected in the AML/CFT program (for example, the introduction of a new product or distribution channel)

f) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML/CFT program

g) legislation incorrectly interpreted and applied in relation to a customer identification procedure

h) customer identification and monitoring systems, policies and procedures that fail to:

i) prompt, if appropriate, for further identification and/or verification when the ML/TF risk posed by a customer increases

ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service

iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check

iv) take appropriate action where the identification document provided is neither an original nor a certified copy

v) recognize foreign identification documentation issued by a high risk jurisdiction

vi) record comprehensive details of identification documents, for example, the date of issue

vii) consult appropriate resources in order to identify high-risk customers

viii) identify when an expired or old identification document (for example, a driver's license) has been used

ix) collect any other name(s) by which the customer is known

i) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers

j) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

i) customer identification policies, procedures and systems

ii) identifying potential ML/TF risks

k) acceptance of documentation that may not be readily verifiable.

3.3 Higher risk scenario

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer)
- Non-resident customers
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Business that are cash-intensive
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business

b) Country or geographic risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country

c) Product, service, transaction or delivery channel risk factors:

- Private banking
- Anonymous transactions (which may include cash)
- Non-face-to-face business relationships or transactions
- Payment received from unknown or un-associated third parties.

3.4 Lower risks Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable

means), which impose requirements to ensure adequate transparency of beneficial ownership

- Public administrations or enterprises.

b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is very low
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems
- Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

3.5 Risk variables

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or

delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship.

3.6 Counter Measures for Risk:

3.6.1 Enhanced CDD measures

Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

3.6.2 Simplified CDD measures

Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established. Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

3.7 Ongoing due diligence

Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.