ཨོཾ ། རྒྱལ་གཞུང་དངུལ་ལས་དབང་འཛིན།།

ROYAL MONETARY AUTHORITY OF BHUTAN

AML/CFT RISK BASED FRAMEWORK FOR BANKS
2019

AML/CFT Riske Based Framework for Banks

Contents

Chapter 1: Overview of ML/TF Risk

Introduction

The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. The focus on risk is intended to ensure a bank is able to identify, assess and understand the ML/TF risks to which it is exposed to and take the necessary AML/CFT control measures to mitigate them.

The RBA serves as a useful means to understand the risk areas where related risks are relatively high in order to allocate resources in the most effective way. The RBA:
(a) recognizes that the ML/TF threats to a bank vary across customers, geographic, products and services, transactions and distribution channels;
(b) allows the bank to apply procedures, systems and controls to manage and mitigate the ML/TF risks identified; and
(c) facilitates the bank to allocate its resources and internal structures to manage and mitigate the ML/TF risk identified.

The RBA provides an assessment of the threats and vulnerabilities of the bank from being used as a conduit for ML/TF. By regularly assessing the bank's ML/TF risks, it allows the bank to protect and maintain the integrity of its business and the financial system as a whole.

Banks applying a risk-based approach need to be proactive in seeking out information about money-laundering trends and threats from external sources, such as law enforcement, as well as relying on their own experiences and observations. This allows banks to effectively review and revise their use of AML tools to fit the specific risks that they face

Accordingly, this framework is aimed at:

i) Assisting the banks to design and implement AML/CFT control measures by providing a common understanding of what the RBA encompasses;
ii) Outlining the recommended steps involved in applying the RBA. In the event a bank has developed its own RBA, the adopted RBA must be able to achieve the outcomes intended under this framework;
iii) Providing general information about risks related with the customers, products, services, delivery channels and geographical locations.

Risk management and mitigation

Banks are required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They are required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by the Board, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with AML/CFT Act and Rules and Regulations and other AML/CFT requirements.

What is risk?

Risk can be defined as the combination of the probability of an event and its consequences. In simple term, 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.

What is risk management?

Risk management is a systematic 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.

Which risks do banks need to manage?

For the ML&TF aspects, FID expects a 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. The banks 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 banks under the AML/CFT Act of Bhutan 2018, AML/CFT Rules and Regulation 2018 (including all amendments), the other relevant Rules issued under the Act and instructions issued by FID. Examples of regulatory obligations that may be breached includes reporting of STR, verifying the identity of your customer, and having an AML&CFT program (showing how a business identifies and manages the ML&TF risk it may face) etc.

It is unrealistic that a bank would operate in a completely ML&TF risk-free environment. Therefore, it is suggested that a bank shall identify the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

Banks 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 a manner that is 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 bank reasonably faces.

For effective risk management, banks should at all levels follow the principles below:

1) Risk management contributes to the demonstrable achievement of objectives and improvement of performance, governance and reputation.
2) Risk management is not a stand-alone activity that is separate from the main activities and processes of the bank. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning.
3) Risk management helps decision makers to make informed choices, prioritize actions and distinguish among alternative courses of action.
4) Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
5) A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
6) Risk management is based on the best available information.
7) Risk management is aligned with the bank's external and internal context and risk profile.
8) Risk management is transparent and inclusive.
9) Risk management is dynamic, iterative and responsive to change. It must iteratively seek to collect and update data related to identified risks and to review mitigation plans accordingly.

Following the above-mentioned principles, banks are expected to develop and maintain logical, comprehensive and systematic methods to address each of the components referred to in this framework and that such methods and the banks' approach to ML&TF risk are understood, implemented and maintained, to some appropriate extent, within their organizations.

Banks would be expected to demonstrate to FID and DFRS (for example, when an inspection is being conducted) that their risk based systems and controls are suitable to their particular businesses and consistent with prudent and good practices. In assessing and mitigating ML&TF

risk, the banks should consider a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

1) *Retail banking*: where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
2) *Corporate and investment banking*: where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
3) *Investment services*: where banks provide products and services to manage their customers' wealth (sometimes referred to as privileged or priority banking); and
4) *Correspondent services*: where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank"). Banks should be mindful of those differences when assessing and mitigating the ML/TF risk to which they are exposed.

Chapter 2: Risk Management Framework, Process and Calculation

Risk Management Framework

Risk management framework is the process used to identify the potential threats to an organization and to define the policies and procedures to eliminate or minimize the threats, as well as developing a strategy or guideline to monitor and review of those identified risk. Framework consists of:

a) Establishing the internal and external context within which the designated service is, provided or to provide. These may include:

   i. the types of customers,
   ii. the nature, scale, diversity and complexity of their business,
   iii. their target markets,
   iv. the number of customers already identified as high risk,
   v. the jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with having high level of deficiencies in AML/CFT controls and listed by FATF,
   vi. the distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies on third parties to conduct CDD and the use of technology,
   vii. the internal audit and regulatory findings, and
   viii. the volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

b) Risk identification,
c) Risk assessment or evaluation, and
d) Risk treatment (mitigating, managing, control, monitoring and periodic reviews).

In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include:

Figure 1: The risk management framework

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:

- minimise 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/CTF program

Risk monitoring and review

Monitor & review the risk plan:

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML/CTF program
- do internal audit or assessment
- do AML/CTF compliance report

The risk management process

Risk identification

Identify the main business ML&TF risks relating to:

- customers
- products & services
- business practices/delivery methods or channels
- country/jurisdiction

Identify the main regulatory risks:

- failure to report STRs/SARs
- inappropriate customer verification
- inappropriate record keeping
- lack of AML&CFT program

The first step is to identify what ML&TF risks exist in a bank when providing designated services.

Some examples of ML&TF risk associated with different banking activities

Retail Banking	• Provision of services to cash incentive business, • Volume of transactions, • High-value transactions, and • Diversity of services.
Wealth Management	• Culture of confidentiality, • Difficulty to identify beneficial owners, • Concealment (use of offshore trusts), • Banking secrecy, • Complexity of financial services and products, • PEPs, • High value transaction, and • Multiple jurisdictions.
Investment Banking	• Layering and integration, • Transfer of assets between parties in exchange for cash or other assets, and • Global nature of markets.
Correspondent Banking	• High value transactions,

	• Limited information about the remitter and source of funds especially when executing transaction with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, and • The possibility that PEPs are involved regarding the ownership of the banks.

As previously discussed, there are two risk types: **Business risk and Regulatory risk**.

Business risk

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

i. Customers,
ii. Products and services,
iii. Business practices/delivery methods or channels, and
iv. Country or jurisdiction risks.

Under the elements of the business risk, individual risk to a bank can be determined. Some of these individual risks may include:

a) Customers: followings are some indicators to identify ML&TF risk arises from different customers of a bank.

i. a new customer,
ii. a new customer who wants to carry out a large transaction,
iii. a customer or a group of customers making lots of transactions to the same individual or group,
iv. a customer who has a business which involves large amounts of cash,
v. a customer whose identification is difficult to check,
vi. a customer who brings in large amounts of used notes and/or small denominations,
vii. customers conducting their business relationship or transactions in unusual circumstances, such as, significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations,
viii. a non- resident customer,
ix. a corporate customer whose ownership structure is unusual and excessively complex,
x. customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates,
xi. customers submit account documentation showing an unclear ownership structure, and
xii. customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

b) Products and services:

i. credit card,
ii. anonymous transaction,
iii. non face to face business relationship or transaction,
iv. payment received from unknown or unrelated third parties,
v. any new product & service developed,
vi. service to walk-in customers, and
vii. mobile banking.

c) Business practice/delivery methods or channels:

i. direct to the customer,
ii. online/internet,
iii. phone,
iv. fax,
v. email, and
vi. third-party agent or broker.

d) Country/jurisdiction:

i. any country subject to economic or trade sanctions,
ii. any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country,
iii. any country identified by FATF as not having adequate AML&CFT system, and
iv. any country identified as destination of illicit financial flow and having significant level of corruption and criminal activity.

Regulatory risk

This risk is associated with not meeting the requirements of the AML/CFT Act of Bhutan 2018 and AML/CFT Rules and Regulation 2018 (including all amendments) and instructions issued by FID. Examples of some of these risks are:

i. identification and verification not done properly on customer/beneficial owner
ii. failure to keep record properly,
iii. failure to scrutinize staffs properly,
iv. failure to train staff adequately,
v. not having an adequate AML&CFT program,
vi. failure to detect and report suspicious transactions,
vii. not submitting required report to FID regularly,
viii. not having an AML&CFT Compliance Officer,
ix. failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs),
x. not complying with any order for freezing or suspension of transaction issued by FID, and
xi. not submitting accurate information or statement requested by FID.

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 making significant wire transfer (example only)				
Customer whose business address and registered office are in different geographic locations (example only)				
Customers opens account for pension deposit (example only)				

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

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, the risk 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:

a) **'Likelihood'** - the chance of the risk happening
b) **'Impact' (consequence)** - the amount of loss or damage if the risk happened.

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

LIKELIHOOD	X	IMPACT	=	RISK LEVEL/SCORE

a) 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 banks 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

b) 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 bank and its business circumstances, be rated or looked at from the point of view of:

i. how it may affect the business (if risks are not dealt properly the bank may suffers a financial loss from either a crime or through fines from regulator).
ii. the risk that a particular transaction may result in the loss of life or property through a terrorist act,
iii. the risk that a particular transaction may result in funds being used for any of the predicate offence like, corruption and bribery, counterfeiting currency, counterfeiting deeds and documents, human trafficking, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency and black marketing,
iv. the risk that a particular transaction may cause suffering due to the financing of illegal drugs,
v. reputational risk, how it may affect the bank 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, and
vi. 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 impact are shown in Table 3, but the bank 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 score are shown in Table 4, but the bank can have as many as they believe are necessary.

Figure 2: Risk Matrix

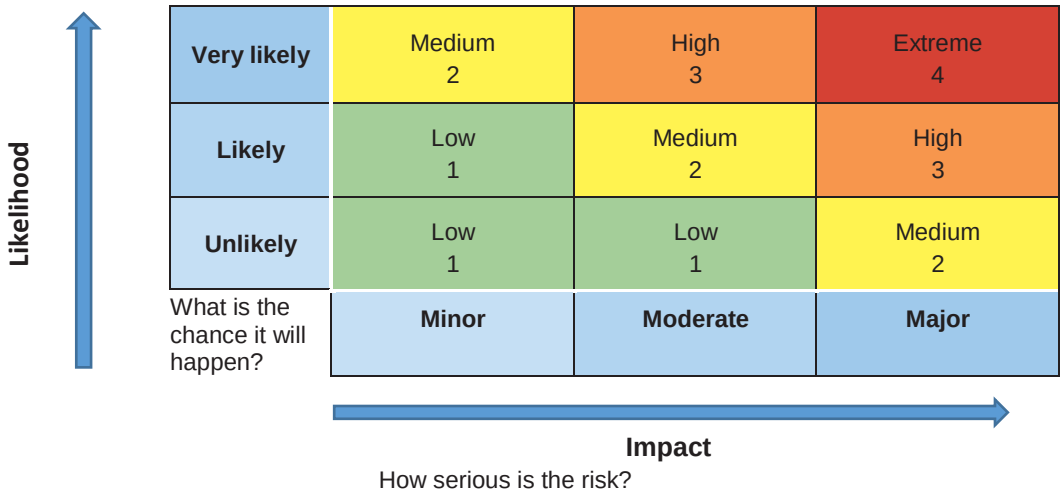


Table 4. Risk Score

Rating	**Impact – of an ML/TF risk**
4 Extreme	Risk almost sure to happen and/or to have very dire 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 banks will have an idea to calculate risk score by blending likelihood and impact, the risk matrix and risk score 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 1). It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the banks would be called together ***"Risk Register".***

Once threat levels and risk scores have been allocated banks can enter in the risk management worksheet (Table 1) 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 making significant wire transfer (example only)	likely *(example only)*	Major *(example only)*	3 *(example only)*	
Customer whose business address and registered office are in different geographic locations (example only)	Very likely *(example only)*	Major *(example only)*	4 *(example only)*	
Customers opens account for pension deposit (example only)	Unlikely *(example only)*	Minor *(example only)*	1 *(example only)*	

Risk Treatment

Manage the business risks:

- minimise 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/CTF program

This stage is about identifying and testing methods to manage the risks the bank 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 the risk. Examples of a risk reduction or treatment step are:

i. setting transaction limits for high-risk products,
ii. having management approval to process higher-risk products,
iii. process to place customers in different risk categories and apply different level of customer due diligence, and
iv. 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)*	**Conduct standard Customer Due Diligence**
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	Likely *(example only)*	Major *(example only)*	3 *(example only)*	**Conduct Enhanced Customer Due Diligence and ask the source of fund and wealth.**
Customer making significant wire transfer (example only)	likely *(example only)*	Major *(example only)*	3 *(example only)*	**Conduct enhanced Customer Due Diligence and collect the details of both the originator and beneficiary, verify source of funds…**
Customer whose business address and registered office are in different geographic locations (example only)	Very likely *(example only)*	Major *(example only)*	4 *(example only)*	**Do not accept or established the relationship with such customer.**

Customers opens account for pension deposit (example only)	Unlikely *(example only)*	Minor *(example only)*	1 *(example only)*	**Conduct simplified customer Due Diligence upon Supervisor's approval**

Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. The bank may choose to use a combination of customer, product/service and country risk to modify an overall risk.

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 should be applied to the risk management process of a bank.

Monitor and review

Monitor & review the risk plan:

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML/CTF program
- do internal audit or assessment
- do AML/CTF 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 bank should develop a method to check regularly on whether AML/CFT program is working correctly and well. If not, the bank 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 Acts and respective Rules.

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.

a) Applying risk appetite to risk assessment

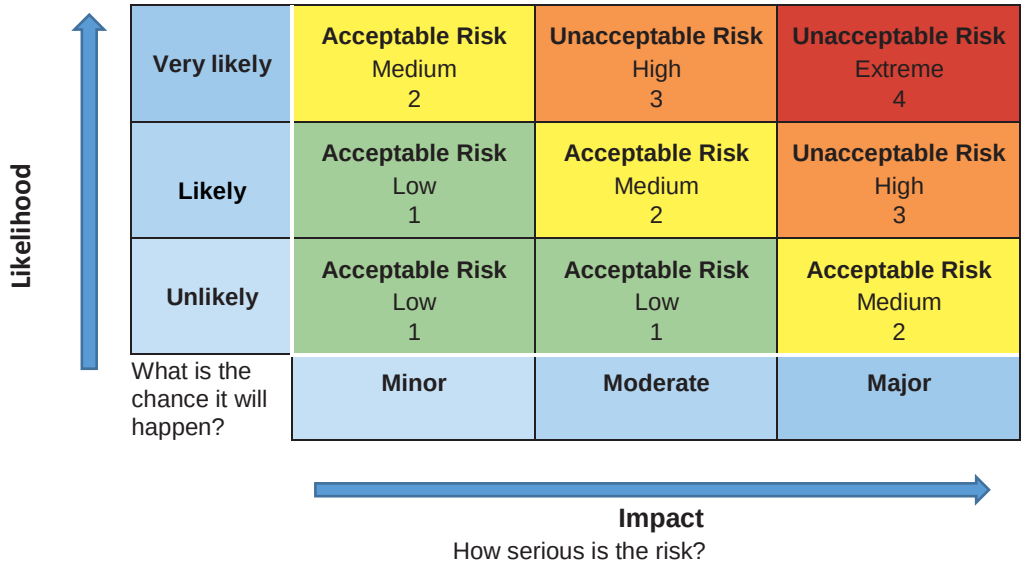
Risk appetite is the amount of risk, that a bank is prepared to accept in relation to its business goals. Risk appetite can be an extra guide to the risk management strategy and can also help in dealing with those identified risks. It is usually expressed as an acceptable/unacceptable level of risk.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

i. What risks will the bank accept?
ii. What risks will the bank not accept?
iii. What risks will the bank treat on a case by case basis?
iv. What risks will the bank send to a higher level for a decision?

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

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

Figure 3: Risk matrix showing risk Appetite



b) Risk tolerance

In addition to defining bank's risk appetite, the bank 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.

Chapter 3: Risk management and mitigation control measures

Risk Management Strategies

The banks 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:

1) reviews at senior management level of the bank's progress towards implementing stated ML&TF risk management objectives.
2) clearly defined management responsibilities and accountabilities regarding ML&TF risk management.
3) adequate staff resources to undertake functions associated with ML&TF risk management.
4) 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.
5) procedural controls relevant to particular designated services.
6) documentation of all ML&TF risk management policies.
7) a system, whether technology based or manual, for monitoring the bank's compliance with relevant controls.
8) policies to resolve identified non-compliance
9) appropriate training program(s) for staff to develop expertise in the identification of ML&TF risk(s) across the bank's designated services.
10) 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 banks 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 banks.
    iv) allow the banks to identify, quantify, assess and monitor business activities relevant to ML&TF risk(s).
    v) allow the banks to monitor the effectiveness of and compliance with its internal AML&CFT systems and procedures.
    vi) allow the banks to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

It should be noted that a bank 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.

Ongoing Risk Monitoring

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

1) failure to include all mandatory legislative components.
2) failure to gain board and/or executive approval of the AML&CFT program.
3) insufficient or inappropriate employee due diligence.
4) frequency and level of risk awareness training not aligned with potential exposure to ML&TF risk(s).
5) changes in business functions which are not reflected in the AML&CFT program (for example, the introduction of a new product or distribution channel).
6) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML&CFT program.
7) legislation incorrectly interpreted and applied in relation to a customer identification procedure.
8) 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.
9) 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.
10) 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.

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**

1) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
2) Non-resident customers.
3) Correspondent banks' accounts
4) Customers with links to offshore tax havens.
5) High net worth customers with no clearly identifiable source of income.
6) Legal persons or arrangements that are personal asset-holding vehicles.
7) Companies that have nominee shareholders or shares in bearer form.
8) Business that are cash-intensive.
9) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
10) Customer who are in sanction list.

b) Country or geographic risk factors

1) The jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called for by FATF for taking counter-measures.
2) 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.
3) Countries subject to sanctions, embargos or similar measures for example, the United Nations.
4) Countries identified by credible sources as having significant levels of corruption or other criminal activity.
5) 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**

1) Private banking.
2) Cash intensive or other forms of anonymous transactions.
3) Non-face-to-face business relationships or transactions.
4) Payment received from unknown or un-associated third parties.
5) Payment received/sent from/to a sanctioned individual or entity

Lower risks Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower, for example where information on the identity of the customer and the beneficial ownership is publicly available. 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

1) Banks that are subject to requirements of combat money laundering and terrorist financing consistent with the FATF Recommendations, having effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
2) 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.
3) Public administrations or enterprises.
4) A government entity.

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

1) Low value accounts
2) Salary accounts of individual's subject to the condition that account is not used for other than salary purposes.
3) Pension accounts for direct credit of pensions.
4) 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**

1) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as adequately complying with and having effectively implemented the FATF Recommendations.
2) 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.

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 bank 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:

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

Counter Measures for Risk

a) Enhanced due diligence measures

Banks 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, banks should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships include:

1) Obtaining and verifying 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.
2) Obtaining and verifying additional information on the intended nature of the business relationship.
3) Obtaining and verifying information on the source of funds or source of wealth of the customer.
4) Obtaining and verifying information on the reasons for intended or performed transactions.
5) Obtaining and verifying the approval of senior management to commence or continue the business relationship.
6) 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.
7) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

b) Simplified CDD measures

Where the risks of money laundering or terrorist financing are lower, the banks are 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:

1) 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).
2) Reducing the frequency of customer identification updates.
3) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
4) 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.

c) Ongoing due diligence

Banks 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.

Continuous application of RBA

The application of RBA is a continuous process to ensure that RBA processes for managing and mitigating ML/TF risks are kept under regular review.

For the purpose of risk assessment, banks should conduct periodic assessment of its ML/TF risks (minimum every two years or sooner if there are any changes to the reporting institution's business model) taking into account the growth of the business, nature of new products/services and latest trends and typologies in the sector.

Banks must review its risk assessment to:

- ensure it remains current at all times
- identify any deficiencies in its effectiveness
- make any changes that are identified as being necessary in this process.

A bank must take appropriate measures to ensure that its policies and procedures are updated in light of the continuous risk assessments and ongoing monitoring of its customers.

Documentation of the RBA process

Banks must ensure the RBA process is properly documented. Documentation by the banks should include–

1) Process and procedures of the Risk Assessment;
2) Information that demonstrates higher risk indicators have been considered, and where they have been considered and discarded, reasonable rationale for such decision;
3) Analysis of the ML/TF risks and conclusions of the ML/TF threats and vulnerabilities to which the reporting institution is exposed to;
4) Measures put in place for higher risk indicators and to ensure that these measures commensurate with the higher risks identified.

In addition, on a case-by-case basis, banks should document the rationale for any additional due diligence measures it has undertaken (or any which it has waived) compared to the standard CDD approach.