GUIDELINES ON

RISK-BASED APPROACH (RBA) FOR THE PURPOSE OF ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT)

Contents

1.0 Relationship with Existing Policies

1.1 The requirements aim to provide explanation on the existing requirements and detail guidance with reference of implementation under Part B of AML/CFT requirements for "**Risk-Based Approach (RBA) Application"** and shall be read together with the reporting institutions existing AML/CFT Guidelines as per each sector below:

- Guidelines on AML/CFT– Banking Sector (Paragraph 12.1-12.5)
- Guidelines on AML/CFT–Trust Company Sector (Paragraph 12.1-12.5.2)
- Guidelines on AML/CFT– Insurance and Takaful Sectors (Paragraph 12.1- 12.5.2)
- Guidelines on AML/CFT– Capital Market and Other Business Services (Paragraph 12.1- 12.5.2)

1.2 This guidance also shall be read together with other relevant policy documents, circulars and directives issued by Labuan FSA relating to the compliance with AML/CFT requirement from time to time unless it was stated otherwise.

2.0 Non Compliance

2.1 Any person who fails to comply with the Guidelines may be guilty of an offence punishable under Section 4B of the Labuan Financial Services Authority Act 1996.

3.0 Compliance Date

3.1 Compliance to the requirements outlined in this guideline shall take effect immediately, unless otherwise specified by the Labuan FSA.

4.0 General

4.1 The RBA is central to the effective implementation of the FATF Recommendations. The focus on risk is intended to ensure a reporting institution 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.

4.2 This Guidance seeks to:

a. assist the reporting institution to design and implement AML/CFT control measures by providing a common understanding of what the RBA encompasses; and

b. outline the recommended steps involved in applying the RBA. In the event a reporting institution has developed its own RBA, the adopted RBA must be able to achieve the outcomes intended under this Guidance.

4.3 For entities under a group structure, this Guidance shall apply to each reporting institution that falls under First Schedule of the AMLA, whether as a holding or subsidiary entity.

4.4 The RBA–

(a) recognises that the ML/TF threats to a reporting institution vary across customers, geographic, products and services, transactions and distribution channels;

(b) allows the reporting institution to apply procedures, systems and controls to manage and mitigate the ML/TF risks identified; and

(c) facilitates the reporting institution to allocate its resources and internal structures to manage and mitigate the ML/TF risk identified.

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

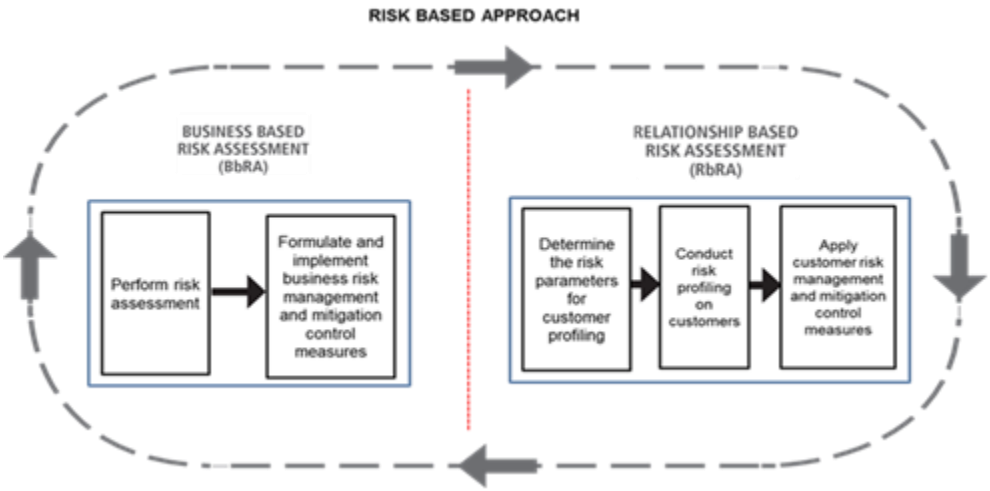
5.0 General: RBA Steps

5.1 The RBA entails two (2) assessments:

(a) **Business-based Risk Assessment (BbRA);** and

(b) **Relationship-based Risk Assessment (RbRA)**

5.2 The RBA steps above are illustrated in the diagram below:



A. Business-based Risk Assessment (BbRA)

In a BbRA, a reporting institution must identify ML/TF risk factors that affect its business and address the impact on the reporting institution's overall ML/TF risks.

I. ***Perform risk assessment -*** A reporting institution shall perform an assessment on the degree of ML/TF risks that the reporting institution's business is exposed to and determine its risk appetite level. To this end, a reporting institution should formulate specific parameters of the ML/TF risk factors considered.

II. ***Formulate and implement business risk management and mitigation control measures -*** A reporting institution must formulate procedures, systems and controls designed to manage and mitigate the identified ML/TF risks. These risk control measures should manage and mitigate the ML/TF risks identified as well as be proportionate to the risks recognised.

B. Relationship-based Risk Assessment (RbRA)

In a RbRA, a reporting institution must consider types of products, services, distribution channels, etc. that the customers are using and mitigate the risks identified.

I. ***Determine the risk parameters for customer profiling*** - A reporting institution must identify specific risk factors and parameters for customers' profiling. Where relevant, the reporting institution may adopt similar parameters that have been used for the assessment of the ML/TF risk factors considered under the BbRA.

II. ***Conduct risk profiling on customers*** – Based on the CDD information or ongoing CDD information, as the case maybe, a reporting institution must determine the risk profiling of each customer e.g. high, medium or low, to determine the CDD measures (standard or enhanced) applicable in respect of each customer.

III. ***Apply customer risk management and mitigation control measures –*** A reporting institution must apply the necessary risk management and mitigation procedures, systems and controls, that commensurate with the risk profile of each customer, to effectively manage and mitigate the ML/TF risks.

5.3 The RBA must be tailored to the reporting institution's business, size, structure and activities.

5.4 The RBA must be reflected in the reporting institution's policies and procedures. All steps and processes in relation to the RBA must be documented and supported by appropriate rationale.

5.5 Recognising that ML/TF risks may change and evolve over time with new threats, products/services, new technologies, etc., the reporting institution must understand that assessing and mitigating ML/TF risks is not a static exercise. Therefore a reporting institution must periodically review, evaluate and update the RBA accordingly.

5.6 The outcome of the BbRA and RbRA complement each other. Therefore, to effectively implement the RBA–

(a) a reporting institution must determine reasonable risk factors and parameters for the BbRA and RbRA ; and

(b) over a period of time, data from the RbRA may also be useful in updating the parameters of the BbRA.

6.0 Business-based Risk Assessment (BbRA)

A: Perform Risk Assessment

6.1 While there is no prescribed methodology, the risk assessment should reflect the threats and vulnerabilities of the reporting institution's business against ML/TF risks. Hence a reporting institution may formulate either a manual or automated system in performing its risk assessment.

6.2 The reporting institution should evaluate the extent of its ML/TF risks at a macro level. When assessing the ML/TF risks, a reporting institution should consider all relevant risk factors that affect their business and operations which may include the following:

(a) Reporting institution's customers;

(b) Geographic location of the reporting institution;

(c) Transactions and distribution channels offered by the reporting institution;

(d) Products and services offered by the reporting institution;

(e) Structure of the reporting institution;

(f) Findings of the National Risk Assessment (NRA); and

(g) Other specific risk factors that the reporting institution may consider for the purpose of identifying its ML/TF risks.

6.3 The ML/TF risks may be measured based on a number of factors. The weight or materiality given to these factors (individually or in combination) when assessing the overall risks of potential ML/TF may vary from one reporting institution to another, depending on their respective circumstances. Consequently, the reporting institution has to make its own determination as to the risk weightage or materiality. These factors either individually or in combination, may increase or decrease potential ML/TF risks posed to the reporting institution.

6.4 To assist a reporting institution in assessing the extent of its ML/TF risks, the reporting institution may consider the following examples under the risk factors mentioned below for guidance:

(a) ***Customers –*** in conducting business transactions, the reporting institution is exposed to various types of customers that may pose ML/TF risks. In analysing its customers' risk, a reporting institution may consider the non-exhaustive examples below:

- *Percentage of high-net-worth customers within the reporting institution;*
- *Nature / type of business of the customers;*
- *The complexity of the customers' legal structures;*
- *Exposure to PEP customers;*
- *Whether the reporting institution has a significant number of legal arrangement and legal person as its customers;*
- *Likelihood of the customers' transactions originating from FATF black or grey list countries, tax havens;*
- *Exposure to customers from jurisdiction known with higher levels of corruption, organised crimes or drug production/distribution; and*
- *Exposure to customers that are mostly domicile in, or conducting business in or through, countries that are listed by FATF on its Public Statement or the Government of Malaysia.*

(b) ***Countries or geographic*** – a reporting institution should take into account factors including the location of the reporting institution's branches and subsidiaries and whether its holding company is located within a jurisdiction with full AML/CFT compliance as identified by a credible source. Further non- exhaustive examples are as below:

- *Location of its branches and subsidiaries in tourist hotspots, crime hotspots, country's border and entry-points; and*
- *Location of its branches and subsidiaries in high risk jurisdictions e.g. countries identified by FATF and the Government of Malaysia, countries subjected to sanctions by UN, etc.*

(c) ***Transactions and distribution channels –*** a reporting institution has various modes of transaction and distribution of its products and services. Some of the modes of transaction and distribution channels may be more susceptible to ML/TF risks. In this regard, a reporting institution must consider the appropriate ML/TF risks attributed to these modes including the following examples:

- *Mode of distribution primarily via agents;*
- *Online or technology based transaction;*
- *Non face-to face business relationship; and*
- *Cash-based transactions.*

(d) ***Products and services –*** given the variety of financial products in the market, a reporting institution must identify the appropriate level of ML/TF risks attached to the types of products and services offered. Some of the non- exhaustive examples that the reporting institution may take into account are as follows:

- *Nature of the products i.e. transferability/liquidity of the products;*

- *Level of complexity of the products and services;*
- *Bearer instruments; and*
- *New technologies.*

(e) ***Reporting institution's structure*** – the ML/TF risk of a reporting institution may differ according to its size, structure and nature of business. Appropriate assessment of its business model and structure may assist a reporting institution to identify the level of ML/TF risks that it is exposed to. In this regard, a reporting institution may take into account the following non- exhaustive examples:

- *Number of branches and subsidiaries;*
- *Size of the reporting institution;*
- *Number of employees;*
- *Degree of dependency on technology; and*
- *Size against industry.*

(f) ***Findings of the National Risk Assessment (NRA) or any other risk assessments issued by relevant authorities*** – in identifying, assessing and understanding the ML/TF risks, a reporting institution must fully consider the outcome of the NRA or any other equivalent risk assessments by relevant authorities:

Under the NRA, a reporting institution should take into account the following:

- *Sectors identified as highly vulnerable to ML/TF risks;*
- *Crimes identified as high risk or susceptible to money laundering; and*
- *Terrorism Financing and/or Proliferation Financing risks.*

(g) ***Other factors –*** *a reporting institution may also take into account other factors in determining its risk assessment such as:*

- *Trends and typologies for a particular sector;*
- *The internal audit and regulatory findings;*
- *The number of suspicious transaction reports it has filed with the FIED; and*
- *Whether the reporting institution has been subjected to service any freeze or seize order by any law enforcement agencies pursuant to the AMLA, Dangerous Drugs (Forfeiture of Property) Act 1988, Malaysian Anti-Corruption Commission Act 2009, etc.*

6.5 In considering each risk factor mentioned above, a reporting institution must formulate parameters that indicate their risk appetite to the potential ML/TF risks it may be exposed to. The reporting institution should set the parameters according to the size and complexity of its business. Refer Example 1 below for illustration purposes:

Example 1

Risk Factor	Examples	Formulated Parameters
Customer	Percentage of high- net-worth customers within the reporting institution	Customers with high-net-worth of RM5 million (USD2 million)
Transactions and Distribution Channels	Number of cash or remittance – amount based transaction	Cash or remittance transaction amounted above RM50,000 or any transaction amounted above RM50,000 / USD30,000
Findings of the NRA	Sectors identified as	Number of customers

	highly vulnerable to ML/TF risks	with occupation or nature of business from highly vulnerable sectors identified under the NRA

6.6 By applying all the risk factors and parameters in performing its risk assessment, the reporting institution would be able to determine the extent of ML/TF risks that it is exposed to, on a quantitative and/or qualitative basis.

6.7 The outcome of the risk assessment will determine the level of risk the reporting institution is willing to accept i.e. the reporting institution's risk appetite and its appropriate risk rating. The risk appetite and risk rating will have a direct impact on the proposed risk management and mitigation procedures, systems and controls adopted by the reporting institution.

6.8 Apart from ensuring that the risk assessment is reflected in the policies and procedures, a reporting institution must also be able to justify the outcome of the risk assessment conducted.

B: Formulate and implement business risk management and mitigation control measures

6.9 Once the reporting institution has identified and assessed the ML/TF risks it faces upon performing its risk assessment under paragraph 6.1-6.9 above, a reporting institution must ensure that appropriate risk control measures are formulated and implemented in order to manage and mitigate these risks.

6.10 The overall expectation is that the mitigation measures and controls must commensurate with the ML/TF risks that have been identified.

6.11 The type and extent of the AML/CFT controls will depend on a number of factors, including–

a. nature, scale and complexity of the reporting institution's operating structure;

b. diversity of the reporting institution's operations, including geographical locations;

c. types of customers;

d. products or services offered;

e. distribution channels used either directly, through third parties or agents or on non face-to-face basis;

f. volume and size of transactions; and degree to which the reporting institution has outsourced its operation to other entities (Group).

6.12 The following are non-exhaustive examples of the risk controls that a reporting institution may adopt–

a. restrict or limit financial transactions;

b. require additional internal approvals for certain transactions and products or services;

c. conduct regular training programmes for directors and employees or increase resources where applicable;

d. employ technology based screening or system-based monitoring of transactions; and

e. employ biometric system for better customer verification

7.0 Relationship-based Risk Assessment (RbRA)

A. Determine the risk parameters for customer profiling

7.1 A reporting institution should determine the appropriate risk parameters when considering the risk factors such as customer, country or geographic, product or service and transaction or distribution channel. These risk parameters will assist the reporting institution in identifying the ML/TF risk factors for customers for the purpose of risk profiling. Refer to Example 2 below for illustration purposes:

Example 2

Risk Factor	Parameters determined for risk profiling		Risk Rating
Customer	Type	Individual	Low
		Legal Person	Medium
		Legal Arrangement	High
	Net Worth	Less than RM500,000	Low
		Less than RM500,000 – RM3 million	Medium
		Above RM3 million	High
Transaction or Distribution Channel	Over the Counter		Low
	On behalf		Medium
	Non Face-to-face		High

7.2 Where relevant, a reporting institution may adopt similar risk parameters that have been used for the assessment of the ML/TF risks considered under the BbRA.

7.3 The different parameters considered within the customer, country or geographic, product or service and transaction or distribution channel risk factors, may either individually or in combination impact the level of risk posed by each customer.

7.4 Identifying one high risk indicator for a customer does not necessarily mean that the customer is high risk[1]. The RbRA ultimately requires the reporting institution to draw together all risk factors, parameters considered, including patterns of transaction and activity to determine how best to assess the risk of such customer on an ongoing basis.

7.5 Therefore, a reporting institution must ensure that the onboarding and ongoing CDD information obtained is accurate and up to date.

B. Conduct risk profiling on customers

7.6 Based on the processes under paragraph 5 above, a reporting institution must formulate its own risk scoring mechanism for the purpose of risk profiling its customers, e.g. high, medium or low. This will assist the reporting institution to determine whether to apply standard or enhanced CDD measures in respect of each customer.

7.7 A reporting institution is expected to document, the reason and basis for each risk profiling and risk scoring assigned to its customers.

7.8 Accurate risk profiling of its customers is crucial for the purpose of applying effective control measures. Customers who are profiled as high risk should be subjected to more stringent control measures including frequent monitoring compared to customers rated as low risk.

7.9 While CDD measures and risk profiling of customers are performed at the inception of the business relationship, the risk profile of a customer may change once the customer has commenced transactions. Ongoing monitoring determines whether the transactions are consistent with the customer's last known information.

[1] Except for high risk customer relationship that have already been prescribed, example Foreign PEP, customers from high risk jurisdiction identified by FATF.

C: Apply customer risk management and mitigation control measures

7.10 Based on the risk profiling conducted on customers, a reporting institution must apply the risk management and mitigation procedures, systems and control measures proportionate to the customers' profiles to effectively manage and mitigate such ML/TF risks.

7.11 Non-exhaustive examples of risk management and mitigation control measures for RbRA include:

a. *Develop and implement clear customer acceptance policies and procedures;*

b. *Obtain, and where appropriate, verify additional information on the customer;*

c. *Update regularly the identification of the customer and beneficial owners, if any;*

d. *Obtain additional information on the intended nature of the business relationship;*

e. *Obtain information on the source of funds or source of wealth of the customer;*

f. *Obtain information on the reasons for the intended or performed transactions;*

g. *Obtain the approval of senior management to commence or continue business relationship;*

h. *Conduct appropriate level and frequency of ongoing monitoring;*

i. *Scrutinise transactions based on a reasonable monetary threshold and/or prescribed transaction patterns; and*

j. *Impose transaction limit or set a certain threshold.*

8.0 Continuous application of RBA

8.1 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.

8.2 For the purpose of risk assessment, a reporting institution 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.

8.3 Through the periodic assessment, a reporting institution may be required to update or review either its BbRA or RbRA.

8.4 A reporting institution 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.

9.0 Documentation of the RBA process

9.1 Reporting institution must ensure the RBA process is properly documented.

9.2 Documentation by the reporting institution should include–

I. Process and procedures of the Risk Assessment;

II. Information that demonstrates higher risk indicators have been considered, and where they have been considered and discarded, reasonable rationale for such decision;

III. Analysis of the ML/TF risks and conclusions of the ML/TF threats and vulnerabilities to which the reporting institution is exposed to;

IV. Measures put in place for higher risk indicators and to ensure that these measures commensurate with the higher risks identified.

9.3 In addition, on a case-by-case basis, a reporting institution 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.

Labuan Financial Services Authority
17th July 2017 (Monday)