1.0 Introduction

1.1 The risk-based approach (RBA) is central to the effective implementation of the anti-money laundering and countering financing of terrorism (AML/CFT) preventive requirements and the FATF Recommendations. The focus on risk is intended to ensure a reporting institution is able to identify, assess and understand the money laundering and terrorism financing (ML/TF) risks to which it is exposed to and take the necessary AML/CFT control measures to mitigate them.

1.2 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) clarify the policy expectations in relation to the assessment of business-based and customer-based ML/TF risk in applying the RBA. In the event a reporting institution has developed its own RBA, the reporting institution is expected to ensure its RBA achieves the outcomes as specified in the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs and NBFIs policy document) as further clarified in this Guidance.

1.3 This Guidance is **not** intended to supersede or replace any of the existing mandatory requirements on RBA that are provided in Paragraph 10 of the AML/CFT and TFS for DNFBPs and NBFIs policy document.

1.4 The RBA–

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

(b) allows the reporting institution to apply appropriate policies, procedures, systems and controls to manage and mitigate the ML/TF risks identified based on the nature, scale and complexity of the reporting institution's business and ML/TF risk profile; and

(c) facilitates more effective allocation of the reporting institution's resources and internal structures to manage and mitigate the ML/TF risk identified.

1.5 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.

2.0 Institutional Risk Assessment and Customer Risk Profiling

2.1 The RBA entails two (2) assessments:

Institutional Risk Assessment (IRA)

A reporting institution is expected to identify ML/TF risk factors that affect its business and address the impact on the reporting institution's overall ML/TF risks.

- ***Refer to requirements in paragraphs 10.2 and 10.3 in the AML/CFT and TFS for DNFBPs and NBFIs policy document***

I. ***Perform risk assessment -*** A reporting institution is expected to 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 is expected to formulate specific parameters of the ML/TF risk factors considered.

II. ***Formulate and implement business risk management and mitigation control measures -*** A reporting institution is expected to establish and implement policies, controls and procedures to manage and mitigate the identified ML/TF risks. Such measures should be sufficiently adequate to manage and mitigate the ML/TF risks identified.

Customer Risk Profiling (CRP)

For CRP, a reporting institution is expected to consider the inherent risks arising from the types of products, services, distribution channels, etc. that the customers are using and implement appropriate measures to manage and mitigate the ML/TF risks identified therein.

- ***Refer to requirements in paragraph 10.4 in the AML/CFT and TFS for DNFBPs and NBFIs policy document***

I. ***Determine the risk parameters for customer risk profiling*** - A reporting institution is expected to identify specific ML/TF 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 IRA.

II. ***Conduct risk profiling on customers*** – Based on the Customer Due Diligence (CDD) information obtained at point of on-boarding new customers, or ongoing CDD information obtained from existing customers, as the case may be, a reporting institution is expected to determine the ML/TF risk profile of each customer (e.g. high, medium or low) by applying the risk parameters determined above, in order to determine the appropriate level of CDD (i.e. standard or enhanced) that is applicable in respect of each customer. The resulting ML/TF risk profile may also have a bearing on the frequency and intensity of on-going CDD that is applicable throughout the duration of the business relationship with the customer.

III. ***Apply customer risk management and mitigation control measures*** – A reporting institution is expected to apply the necessary risk management and mitigation policies, controls and procedures that are commensurate with the ML/TF risk profile of each customer, to effectively manage and mitigate the ML/TF risks identified. For example, customers assessed as having higher ML/TF risks should be subject to enhanced CDD procedures, senior management's approval should be obtained before offering or continuing to transact or provide professional services and the customer should be subject to more frequent and intense on-going CDD procedures throughout the duration of the business relationship with the customer.

2.2 The RBA is expected to be tailored to the nature, scale and complexity of the reporting institution's business, size, structure and activities.

2.3 A reporting institution is expected to incorporate the RBA into its existing policies and procedures. All steps and processes in relation to the RBA for purpose of IRA and CRP are expected to be documented and supported by appropriate rationale and be subject to approval by senior management and/or the Board of Directors, as appropriate.

2.4 Recognising that ML/TF risks evolve and are subject to change over time (arising from the emergence of new threats, introduction of new products/services, new technologies, expansion to new customer base etc.) a reporting institution is expected to understand that assessing and mitigating ML/TF risks is not a static exercise. Therefore, a reporting institution is expected to periodically review, evaluate and update the RBA accordingly.

2.5 The outcome of the IRA and CRP complement each other. Therefore, to effectively implement the RBA–

(a) a reporting institution is expected to determine reasonable risk factors and parameters for the IRA and CRP; and

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

3.0 Institutional Risk Assessment (IRA)

A. Perform Risk Assessment

3.1 While there is no prescribed methodology, the IRA is expected to reflect material and foreseeable ML/TF threats and vulnerabilities which a reporting institution is exposed to for the period under review. Hence, a reporting institution may establish a manual or automated system to perform its risk assessment.

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

(a) Specific risk factors or high risk crimes that the reporting institution may consider for the purpose of identifying its ML/TF risks;

(b) Type of customers;

(c) Geographic location of the reporting institution;

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

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

(f) Structure of the reporting institution; and

(g) Findings of the National Risk Assessment (NRA).

3.3 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, a reporting institution is expected to make its own determination as to the risk weightage or materiality for each factor under consideration. These factors either individually or in combination, may increase or decrease potential ML/TF risks posed to the reporting institution.

3.4 To assist a reporting institution in assessing the extent of its ML/TF risks, the reporting institution may consider the following examples of risk factors:

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

- *Exposure by type of customer, individuals and non-individuals (companies, businesses, legal arrangements, associations, etc.);*
- *Exposure by nationality i.e. local or foreign;*
- *Nature and type of business or occupation of the customers;*
- *Exposure to foreign PEP customers;*
- *Exposure to domestic PEP customers assessed as higher risk;*
- *Exposure to customers related to PEPs assessed as higher risk;*
- *Exposure to customers that are legal arrangements (e.g. trusts) and legal persons and the level of complexity of such legal structures;*
- *Exposure to customers that authorise a proxy/agent to represent on their behalf;*
- *Exposure to companies that have nominee shareholders or shares in bearer form;*
- *Exposure to legal persons or arrangements that are personal asset holding vehicles;*

- *Exposure to customers originating from or domiciled in, and/or transactions conducted in or through higher risk countries (called by FATF or Government of Malaysia) or tax haven jurisdictions.*

(b) ***Countries or geographic location*** – a reporting institution should take into account such factors including the location of the reporting institution's holding company, head office, branches and subsidiaries and agents (where applicable), 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 holding company, branches, subsidiaries, merchants and/or agents in:

- *Tourist hotspots, crime hotspots, country's border and entry-points;*
- *High risk countries called by the FATF or by the Government of Malaysia;*
- *Jurisdictions that have been identified by credible sources as having significant levels of corruption or other criminal activities e.g. reports by Transparency International, United Nations Office on Drugs and Crimes etc.;*
- *Jurisdictions that have been identified by credible sources as providing funding or support for money laundering, terrorism or proliferation of weapons of mass destruction.*

(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. For example, products sold via non-face-to-face channels are more susceptible to ML/TF as compared to products sold via face-to-face channels, and transactions conducted with third party agents of the reporting institution may be more vulnerable to ML/TF in comparison to those conducted at the reporting institution's own branches. In this regard, a reporting institution is expected to consider the appropriate ML/TF risks attributed to all available modes of transactions and distribution that are offered to customers by the reporting institution, including the following non-exhaustive examples:

- *Mode of distribution e.g. direct channel, or via agents, brokers, financial advisors, introducers, online or technology based transaction;*
- *Volume and frequency of non-face-to-face business relationships or transactions;*
- *Mode of payment e.g. cash-based transactions, e-payments;*
- *Cash intensive or other forms of anonymous transactions;*
- *Volume and frequency of transactions carried out in high risk areas or jurisdictions;*
- *Number of distribution channels located in high risk areas or jurisdictions; and/or*
- *Exposure to cross-border transactions and/or transactions in high risk jurisdictions.*

(d) ***Products and services*** – a reporting institution is expected to 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 and services;*
- *Level of complexity of the products and services;*
- *Cash intensity related to the products and services;*
- *Market segments of the products and services;*
- *Products that are easily transferable to another party;*
- *Product's ownership not easily traceable to the owner;*
- *Product can be easily converted to cash or exchanged to another form;*
- *Customer can place deposit for a period of time for purchasing a product;*
- *Product can be easily transported or concealed;*
- *Product can be used as an alternative form of currency;*
- *Product that has high value in nature;*
- *Product can be purchased through non face-to-face channel;*
- *Allow use of virtual asset and other anonymous means of payment;*
- *Allow use of unusual means of payment e.g. high value items such as real estate, precious metals and precious stones;*
- *Services that enable clients to move funds anonymously; and/or*
- *Nominee services that may obscure ownership of legal person or legal arrangements.*

(e) ***Reporting institution's structure*** – the ML/TF risk of a reporting institution may differ according to its size, nature and complexity of the reporting institution's business operations. 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, subsidiaries and/or agents;*
- *Size of the reporting institution relative to industry/sector;*
- *Number and profile of employees;*
- *Degree of dependency on technology;*
- *Volume and value of cross border transactions;*
- *Volume and value of high-valued products;*
- *Cash intensity of the business; and/or*
- *Level of staff turnover, especially in key personnel positions.*

(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 is expected to fully consider the outcome of the NRA or any other equivalent risk assessments by relevant authorities:

Under the NRA, a reporting institution is expected to take into account the following:

- *Sectors identified as highly vulnerable to ML/TF risks and the reporting institutions exposure to such sectors in relation to customer segments served;*
- *Crimes identified as high risk or susceptible to ML/TF and the adequacy of the reporting institutions' mitigating measures to detect and deter such illegal proceeds or in preventing dealings with customers involved in such illicit activities; and/or*
- *Terrorism Financing and/or Proliferation Financing risks faced by the industry.*

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

- *Current trends and typologies for the sector in relation to ML/TF and other crimes;*
- *The reporting institution's internal audit and regulatory findings;*
- *Current trends and typologies for other sectors with similar business model or product/service offerings in relation to ML/TF and other crimes;*
- *The number of suspicious transaction reports it has filed with Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and/or*
- *Whether the reporting institution has been subjected to service any freeze or seize order by any law enforcement agencies pursuant to AMLA, Dangerous Drugs (Forfeiture of Property) Act 1988, Malaysian Anti-Corruption Commission Act 2009, etc.*

3.5 In considering each risk factor mentioned above, a reporting institution is expected to formulate parameters that indicate their risk appetite in relation to the potential ML/TF risks it may be exposed to. The reporting institution is expected to set its own parameters according to the size, complexity of its business. Example 1 below is strictly for illustration purpose and is intended to facilitate better understanding on how the risk factors and parameters may be applied. It is **not** intended to serve as a prescription or recommendation on the parameters or specific thresholds to be adopted by the reporting institution:

Example 1 for all sectors:

Risk Factor	Examples	Formulated Parameters
Customer	Higher risk customer	• Number of higher risk customers more than 20% of total customer base for a year • Number of politically exposed person (PEP) customers who are high risk is more than 5% of total customers
	Local and foreign customers	• Percentage of local and foreign customer for a year
	Companies with nominee shareholders or shares in bearer form	• Percentage of such companies against total non-individual customer base
Transactions and Distribution Channels	Cash intensive or other forms of anonymous transactions	• High volume of cash transactions above RM50,000 within a year • High volume of anonymous/proxy transactions exceeding RM50,000 per transaction within a year
	Percentage of non-face-to-face transactions	• Non-face-to-face transactions exceeding 50% of total transactions
	Frequency and amount of cash payments	• Cash transactions above RM10,000
	Wide array of e-banking products and	• More than 30% of new accounts are opened via internet, mail or

	services	telephone without prior relationship
Findings of the NRA	Sectors identified as highly vulnerable to ML/TF risks	• Number of customers with occupation or nature of business from highly vulnerable sectors identified under the NRA

Note: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which reporting institutions should apply in assessing the ML/TF risks of the business. Reporting institutions are expected to determine which risk factors and parameters are most appropriate in the context of the nature, scale and complexity of their respective businesses.*

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

3.7 The outcome of the risk assessment would determine the level of ML/TF risks 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 policies, controls and procedures adopted by the reporting institution.

3.8 Apart from ensuring that the risk assessment is reflected in its policies and procedures, a reporting institution is also expected to justify the outcome of the risk assessment conducted. Reporting institutions are reminded of the requirement under the AMLA and the AML/CFT and TFS for DNFBPs and NBFIs policy document to maintain proper records on any assessments and approvals by senior management and/or the Board of Directors on the ML/TF risk assessments conducted to enable reviews to be conducted as and when it is requested by the competent authority or supervisory authority.

B. Formulate and implement institutional risk management and mitigation control measures

3.9 Once a reporting institution has identified and assessed the ML/TF risks it faces after performing its risk assessment under paragraph 3A above, a reporting institution is expected to formulate and implement appropriate risk control measures in order to manage and mitigate those risks.

3.10 The intended outcome is that the mitigation measures and controls are commensurate with the ML/TF risks that have been identified.

3.11 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
(g) degree to which the reporting institution has outsourced its operations to other entities or at group level, where relevant.

3.12 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.

4.0 Customer Risk Profiling (CRP)

A. Determine the risk parameters for customer profiling

4.1 A reporting institution is expected to determine the appropriate risk parameters when considering the risk factors such as customer, country or geographic location, 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 the example below for illustration purposes:

Example for all sectors:

Risk Factor	Parameters determined for risk profiling		Risk Rating
Customer	Type	Individual	Low
		Legal Person	Medium
		Legal Arrangement	High
	Social status	Non-PEP	Low
		Local PEP	Medium
		Foreign PEP	High
	Nationality	Malaysian	Low
		Other countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High

	Country of Residence	Malaysia	Low
		Other countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High
Transaction or Distribution Channel	Face-to-face		Low
	On behalf/Through intermediaries and/or agents		Medium
	Non Face-to-face		High

Note 1: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which reporting institutions should apply for purpose of client risk profiling. Reporting institutions are expected to determine which risk factors and parameters are most appropriate in the context of the nature and complexity of clients served, products/services offered etc.*

Note 2: *In relation to 'Risk Rating', while the examples above are based on a simple three-scale rating model (i.e. Low, Medium or High), this is not intended to restrict the client risk rating models adopted by reporting institutions, which could be based on more granular approach e.g. four-scale or five-scale or more rating model.*

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

4.3 The different CRP 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.

4.4 Identifying one high risk indicator for a customer does not necessarily mean that the customer is high risk[1]. The CRP ultimately requires a reporting institution to draw together all risk factors, parameters considered, including patterns of transaction and activity throughout the duration of the business relationship to determine how best to assess the risk of such customers on an on-going basis.

4.5 Therefore, a reporting institution is expected to ensure that the CDD information obtained at the point of on-boarding and on-going due diligence is accurate and up to date.

B. Conduct risk profiling on customers

4.6 Based on the processes under paragraph 4A above, a reporting institution is

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

expected to 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.

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

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

4.9 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. On-going monitoring would assist in determining whether the transactions are consistent with the customer's last known information.

C. Apply customer risk management and mitigation control measures

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

4.11 Non-exhaustive examples of risk management and mitigation control measures for CRP 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,

(d) Obtain additional information on the intended nature of the business relationship;

(e) Obtain information on the source of funds and/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 commensurate with risks identified;

(i) Scrutinise transactions based on a reasonable monetary threshold and/or pre-determined transaction patterns; and

(j) Impose transaction limit or set a certain threshold.

5.0 Continuous application of RBA

5.1 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.

5.2 A reporting institution is expected to conduct periodic assessment of its ML/TF risks (preferably 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.

5.3 Through the periodic assessment, a reporting institution may be required to update or review either its IRA or CRP.

5.4 A reporting institution is expected to 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.

6.0 Documentation of the RBA process

6.1 A reporting institution is expected to ensure the RBA process is properly documented.

6.2 Documentation by the reporting institution is expected to include:

(a) Process and procedures of the RBA;

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

(c) Analysis of the ML/TF risks and conclusions of the ML/TF threats and vulnerabilities to which the reporting institution is exposed to; and

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

6.3 In addition, on a case-by-case basis, a reporting institution is expected to document the rationale for any additional due diligence measures it has undertaken compared to the standard CDD approach.

6.4 The documented risk assessment is expected to be presented, discussed and deliberated with the senior management (including the CEO) and the Board of Directors of the reporting institution, where applicable.