GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR CAPITAL MARKET INTERMEDIARIES

SC-GL/AML-2014 (R1-2016)

1st issued	: 15 January 2014
Revised	: 7 December 2016

Suruhanjaya Sekuriti
Securities Commission
Malaysia

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR CAPITAL MARKET INTERMEDIARIES

Effective date upon 1st issuance:	15 January 2014

List of Revisions

Revision Series	Revision Date	Effective Date of Revision	Series Number
1st revision	**7.12.2016**	**7.12.2016**	**SC-GL/AML-2014 (R1-2016)**

CONTENTS

APPENDICES

PART I: INTRODUCTION AND APPLICABILITY

1. INTRODUCTION

1.1 The *Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries* (Guidelines) are issued pursuant to section 83 and section 66E of the *Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001* (AMLA) and section 158(1) of the *Securities Commission Act 1993*.

1.2 These Guidelines are drawn up in accordance with the AMLA and the Financial Action Task Force (FATF) 40 Recommendations.

1.3 These Guidelines provide guidance for reporting institutions to comply with the obligations imposed under the AMLA.

1.4 These Guidelines are made in addition to and not in derogation of any other guidelines issued by the Securities Commission Malaysia (SC) or any requirements as provided under the securities laws and the AMLA. Therefore, a reporting institution must comply with other relevant guidelines and requirements.

1.5 A reporting institution that is jointly regulated by Bank Negara Malaysia (BNM) and the SC, is required to comply with these guidelines and the *Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1)* issued by BNM. Where there are differing requirements between the said guidelines, the more stringent requirements shall apply.

1.6 Non-compliance with any of the provisions in these Guidelines will subject the reporting institution to actions under the AMLA, *Capital Markets and Services Act 2007* (CMSA) or any other relevant provisions under the laws of which these Guidelines are subject to.

2. APPLICABILITY

2.1 These Guidelines are applicable to a reporting institution, including its branches and majority-owned subsidiaries outside Malaysia carrying out the activities as listed in the First Schedule of the AMLA.

2.2 In the case of foreign operations, where anti-money laundering and counter financing terrorism (AML/CFT) measures of the host country are less stringent than the Malaysian standards, a reporting institution is required to ensure that its foreign branches and majority-owned subsidiaries apply AML/CFT measures which are consistent with the Malaysian standards, to the extent that the host country laws and

regulations permit.

2.3 If the host country does not permit the proper implementation of the AML/CFT measures consistent with the Malaysian standards, the reporting institution is required to apply appropriate additional measures to mitigate the money laundering and terrorism financing (ML/TF) risks, and inform the SC on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

2.4 Where the reporting institution is unable to put in place the necessary mitigating measures as required under paragraph 2.3 above, the reporting institution may consider ceasing the operations of the branch or subsidiary.

3. DEFINITIONS

3.1 Unless otherwise defined, all words used in these Guidelines shall have the following and the same meaning as defined in the CMSA and AMLA:

beneficial owner	means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes that person who exercises ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.
constituent document	in relation to a body corporate or an unincorporated body, means any document or instrument that– • constitutes, establishes or incorporates the body; • sets out its governing and administrative structure; or • sets out the scope of its functions, business, powers or duties.
customer	means new or existing customer.
FIED	Means the Financial Intelligence and Enforcement Department of Bank Negara Malaysia.
legal arrangement	means an express trust or other similar legal arrangement.

legal person	means any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This can include company, body corporate, foundation, partnership, or association and other relevantly similar entity.
politically-exposed person (PEP)	means: • Foreign PEP i.e. individual who is or who has been entrusted with prominent public functions by a foreign country, for example, Head of State or of government, senior politician, senior government, judicial or military official, senior executive of state owned corporation, important political party official; • Domestic PEP i.e. individual who is or has been entrusted domestically with prominent public functions, for example Head of State or of government, senior politician, senior government, judicial or military official, senior executive of state owned corporation, important political party official; or • Person who is or has been entrusted with a prominent function by an international organisation which refers to member of senior management, i.e. director, deputy director and member of the board or equivalent functions. The definition of PEP is not intended to cover middle ranking or more junior individual in the foregoing categories.
private retirement scheme	has the same meaning as provided under section 139A of the CMSA.
reporting institution	means a person carrying on regulated activities under the CMSA as specified under the First Schedule of the AMLA.

third party	means a financial institution that is supervised and monitored and meets the requirements under paragraph 8.7 of these Guidelines, who is relied upon by the reporting institution to conduct the due diligence process. Reliance on third party often occurs through introductions made by another member of the same group or by another reporting institution. This definition does not include outsourcing or agency relationship.

4. GENERAL DESCRIPTION OF MONEY LAUNDERING

4.1 In principle, money laundering generally involves proceeds of unlawful activities that are related directly or indirectly, to any serious offence, that is processed through transactions, concealments, or other similar means, so that they appear to have originated from a legitimate source.

4.2 The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a reporting institution to the money laundering activities. These stages are:

(a) **Placement:** the physical disposal of benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;

(b) **Layering:** the separation of benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and

(c) **Integration:** where integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

4.3 The illegal funds laundered through the capital market sector may be generated by unlawful activities from outside and within the sector. For illegal funds generated outside the sector, transactions involving capital market products may be used as the mechanism for concealing or obscuring the source of these funds.

5. GENERAL DESCRIPTION OF TERRORISM FINANCING

5.1 Financing of terrorism generally refers to carrying out transactions involving funds or property, whether from a legitimate or illegitimate source, that may or may not be owned by terrorists, or those have been, or are intended to be used to assist the commission of terrorist acts, and/or the financing of terrorists and terrorist organisations.

5.2 Section 3(1) of the AMLA defines a "terrorism financing offence" as any offence under section 130N, 130O, 130P or 130Q of the *Penal Code*, which are essentially:

(a) Providing or collecting property for terrorist acts;

(b) Providing services for terrorism purposes;

(c) Arranging for retention or control of terrorist property; or

(d) Dealing with terrorist property.

6. GENERAL PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORISM FINANCING

6.1 A reporting institution is required to take the necessary steps in order to prevent ML/TF and have a system in place for reporting suspected ML/TF transactions to the FIED.

6.2 In combating ML/TF, a reporting institution must ensure the following:

(a) **Compliance with laws:** A reporting institution must ensure that laws and regulations are adhered to, that business is conducted in conformity with high ethical standards, and that service is not provided where there is good reason to suppose that transactions are associated with ML/TF activities.

(b) **Co-operation with law enforcement agencies:** A reporting institution must co-operate fully with relevant law enforcement agencies. This includes taking appropriate measures such as timely disclosure of information by the reporting institution to the FIED and the relevant law enforcement agencies.

(c) **Establishing internal controls:** A reporting institution must issue and adopt policies and procedures which are consistent with the principles set out under the AMLA and these Guidelines. A reporting institution must also ensure ongoing training programmes are conducted to keep its board of

directors and employees abreast on matters under the AMLA and these Guidelines.

(d) **Risk-based approach:** A reporting institution must ensure that the depth and breadth of its policies and procedures to identify, assess, monitor, manage and mitigate ML/TF risks commensurate with the nature, scale and complexity of its activities.

(e) **Customer Due Diligence:** A reporting institution must have an effective procedure to identify its customers and to obtain satisfactory evidence to verify its customers' identity.

6.3 The board of directors must ensure that the reporting institution regularly reviews its policies, procedures and controls to ensure that they are effective and in line with international developments, particularly the FATF Recommendations on combating ML/TF.

PART II: RISK-BASED APPROACH APPLICATION

7. RISK-BASED APPROACH APPLICATION

In formulating policies and procedures for the prevention of ML/TF, a reporting institution must take appropriate steps to identify, assess and mitigate its ML/TF risks. **Appendix A** of these Guidelines provides the measures to be adopted in implementing a risk-based approach.

7.1 Risk assessment and profiling

7.1.1 The assessment and profiling processes must incorporate the following:

(a) Documenting the reporting institution's risk assessments and findings;

(b) Considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) Keeping the reporting institution's risk assessment up-to-date taking into account changes in surrounding circumstances affecting the reporting institution;

(d) Having a scheduled periodic assessment or as and when specified by the SC; and

(e) Having appropriate mechanisms to provide risk assessment information to the SC.

7.1.2 A reporting institution is also required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. The reporting institution must undertake risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate such risks.

7.1.3 In assessing the level of risk of a customer from a particular country, a reporting institution shall assess the standards of prevention of ML/TF in that country based on the reporting institution's knowledge, experience and other reliable sources of that country. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with the customer from that country.

7.1.4 A reporting institution is required to also implement and maintain appropriate policies and procedures to conduct risk profiling of their customer during the

establishment of the business relationship. In determining the risk profile of a particular customer, the reporting institution must take into account, among others the following factors:

(a) Customer risks e.g. residents or non-residents, occasional or one off, natural or legal person;

(b) Geographical location of business or country of origin of customers;

(c) Products or services;

(d) Transactions or distribution channel e.g. cash-based, face-to-face or non-face-to-face or cross-border; and

(e) Any other information suggesting that the customer is of higher risks.

7.2 Risk management and mitigation

7.2.1 A reporting institution is required to–

(a) have policies, procedures and controls, which are approved by the board of directors, to enable it to manage and mitigate effectively the ML/TF risks that have been identified;

(b) monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

PART III: CUSTOMER DUE DILIGENCE

8. CUSTOMER DUE DILIGENCE (CDD)

8.1 CDD at the point of establishing business relationship

8.1.1 Section 16 of the AMLA among others clearly sets out customer identification requirements for reporting institutions. A reporting institution is expected to obtain satisfactory evidence of the identity and legal existence of the customer and beneficial owner at the point of establishing the business relationship.

8.1.2 A reporting institution must not keep anonymous accounts or accounts in fictitious names.

8.1.3 A reporting institution is required to–

(a) identify the customer (including foreign body corporate) and verify such customer's identity using reliable, independent source of documents, data or information;

(b) verify that any person purporting to act on behalf of the customer is authorised, and identify and verify the identity of that person;

(c) identify and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from reliable sources; and

(d) understand and where relevant obtain information on the purpose of opening an account and the intended nature of the business relationship.

8.1.4 A customer who fails to provide evidence of his identity must not be allowed to engage in business relations with the reporting institution. Additional measures must be undertaken to determine whether to proceed with the business relationship, where initial checks failed to identify the customer or give rise to suspicions that the information provided is false.

8.1.5 **Delayed verification in relation to private retirement scheme**

(a) Paragraph 8.1.5 herein is only applicable to a reporting institution that provides and manages a private retirement scheme.

(b) The reporting institution may complete the verification after the establishment of the business relationship to allow some flexibility for its customer and beneficial owner to furnish the relevant documents.

(c) Before a reporting institution adopts delayed verification, it must ensure that–

(i) any ML/TF risk arising from the delayed verification can be effectively managed; and

(ii) the delay is essential so as not to interrupt the reporting institution's normal conduct of business with the customer.

(d) Where a reporting institution adopts delayed verification, verification must be completed no later than seven business days or any time before redemption, whichever is earlier.

(e) If delayed verification cannot be completed in accordance with sub-paragraph (d) above, the business relationship must be terminated and the reporting institution must comply with paragraph 8.8.

CDD requirements for legal persons and legal arrangements

8.1.6 For customers that are legal persons or legal arrangements, a reporting institution is required to understand the nature of the customer's business, its ownership and control structure. A reporting institution is required to undertake the following:

(a) Identify its customers and verify their identity through the following information:

(i) Name, legal form and proof of existence, for instance the certified true copy or duly notarised copy of the constituent documents, as the case may be, or any other reliable references;

(ii) The powers that regulate and bind the customer such as directors' resolution, as well as names of relevant persons having a senior management position; and

(iii) The address of the registered office and the principal place of business.

(b) Identify and take reasonable measures to verify the identity of the beneficial owners–

I. in relation to the identity of the natural person (if any) who ultimately has controlling ownership interest in a legal person, by way of:

(i) duly certified true copy/duly notarised copy of the latest Forms 24 and 49 as prescribed by the Companies Commission of Malaysia or equivalent document for a foreign body corporate; constituent document of a partnership, club, society and charity (as the case

may be); and identification document of the shareholders with an equity interest of more than 25%, directors, partners and office bearers (as the case may be);

(ii) authorisation for any person to represent the company/business either via a letter of authority or directors resolution;

(iii) relevant document such as NRIC for Malaysians/permanent residents or passport for foreigners, to identify the identity of the person authorised to represent the company/business in its dealing with the reporting institution; and

(iv) to the extent, there is a doubt as to whether the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person (if any) who exercises control of the legal person through other means or who holds the position of senior management.

II. in relation to legal arrangements, by way of–

(i) in the case of a trust, the identity of the settlor, the trustee or the protector, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a gain of control/ownership); or

(ii) in the case of other types of legal arrangement, the identity of the person in equivalent or similar position referred to in II (i) above.

8.1.7 Notwithstanding the above, a reporting institution is exempted from obtaining the constituent document, and from identifying and verifying the directors and shareholders of legal persons which fall under the following categories:

(a) Public-listed companies/corporations listed on Bursa Malaysia or majority-owned subsidiaries of such public-listed companies;

(b) Foreign public-listed companies:

(i) Listed on exchanges recognised by Bursa Malaysia. A reporting institution may refer to the directive in relation to recognised stock exchanges issued by Bursa Malaysia; and

(ii) Not listed in jurisdictions identified in the FATF Public Statements;

(c) Government-linked companies in Malaysia;

(d) State-owned corporations and companies in Malaysia;

(e) Authorised person as operator of a designated payment system, a registered person (as the case may be) under the *Financial Services Act 2013* or the *Islamic Financial Services Act 2013*;

(f) entities licensed under the *Labuan Financial Services and Securities Act 2010* or the *Labuan Islamic Financial Services and Securities Act 2010*;

(g) persons licensed or registered under the CMSA; and

(h) prescribed institutions under the *Development Financial Institutions Act 2002*.

8.1.8 **CDD requirements for establishing non face-to-face business relationship**

(a) A reporting institution is required to establish appropriate measures for identification and verification of a customer's identity before establishing non face-to-face business relationship.

(b) A reporting institution must develop and implement policies and procedures to address and mitigate specific ML/TF risks associated with establishing non face-to-face business relationship.

(c) For the purpose of verification of the identity of a non face-to-face customer, a reporting institution must undertake any of the following measures:

(i) requesting for additional identification documents or information e.g. bank statements, utility bills;

(ii) substantiating the customer's information with any independent source, e.g. contacting the customer's employer and verification through database maintained by any relevant authorities;

(iii) contacting the customer through any digital communication channel to visually verify the customer's identity; or

(iv) requesting the customer to make a nominal payment from his own account with a licensed bank under the *Financial Services Act 2013* or licensed Islamic bank under the *Islamic Financial Services Act 2013* to enable the reporting institution to satisfy itself of the customer's true identity.

(d) Where the reporting institution is unable to verify the customer's identity by adopting the measures provided under paragraph (c) above, the reporting institution must initiate face-to-face business relationship.

(e) Sub-paragraphs (a) to (d) above are not applicable to:

(i) customers that are identified as foreign PEP;

(ii) customers from higher-risk and non co-operative jurisdictions as identified by the FATF; or

(iii) listed persons or entities subjected to targeted financial sanctions for terrorism financing and financing of proliferation of weapons of mass destruction pursuant to the UNSCR.

8.2 Ongoing CDD

8.2.1 A reporting institution must conduct ongoing due diligence and scrutiny of its customers throughout the course of the business relationship. Such measures shall include–

(a) monitoring and detecting patterns of transactions undertaken throughout the course of that business relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, its business, and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and are relevant, by undertaking periodic reviews of existing records, particularly for higher risk categories of customer.

8.2.2 A reporting institution must apply CDD measures to existing customers on the basis of materiality and risk, and conduct due diligence on such existing relationship at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of the data verified.

8.2.3 A reporting institution must monitor the customers' accounts on a regular basis for suspicious transactions. One method is to 'flag' accounts with suspicious transactions for monitoring purpose.

8.2.4 A reporting institution should consider reclassifying a customer as higher risk and consider lodging a suspicious transaction report (STR) with the FIED under the following circumstances:

(a) Following initial acceptance of the customer, the pattern of account activity of the customer is inconsistent and does not fit in with the reporting institution's profile knowledge of the customer;

(b) The transaction appears unusual and not in line with the customer's normal trading pattern; or

(c) There is a material change in the way the account is operated.

8.2.5 While extra care should be exercised in such cases, the reporting institution must weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF and consider whether to refuse to do any business with such customers.

8.2.6 The frequency of the ongoing CDD shall commensurate with the level of ML/TF risks posed by the customer based on the risk profile and nature of transactions.

8.2.7 A reporting institution is required to undertake a renewed CDD when–

(a) there is a suspicion of ML/TF risks; or

(b) there is a doubt about the veracity or adequacy of previously obtained identification data.

8.3 Conducting CDD

8.3.1 A reporting institution must adopt a risk-based approach in determining whether to apply standard CDD (as prescribed under paragraph 8.1 above) or enhanced CDD measures based on the customers' background, transaction types or specific circumstances.

8.3.2 When conducting CDD for the purpose of opening an account or when conducting ongoing CDD, a reporting institution may take into account the following risk factors and risk parameters when determining circumstances of higher risk:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances.
- Non-resident customer.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- The ownership structure of a company appears unusual or excessively complex given the nature of the company's business.

- High-net-worth individuals and entities.
- Persons from jurisdictions known for their high crime rates (e.g. drug producing, trafficking, smuggling).
- Businesses/activities identified by the FATF as having higher risk for ML/TF.
- Domestic PEPs.
- Persons entrusted with prominent function by international organisations.
- Legal arrangements that are complex.
- Any persons who match the 'flag' criteria of the reporting institution.

(b) Country or geographic risk factors:

- Countries having inadequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by international organisations such as the United Nations.
- Countries with significant levels of corruption or other criminal activities.
- Countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Transaction or distribution channel risk factors:

- Anonymous transactions (which may include cash transactions).
- Non-face-to-face business relationships or transactions.
- Payment received from multiple persons and/or countries that do not fit into the customer's nature of business and risk profile.
- Payment received from unknown or unassociated third parties.

8.3.3 Subject to paragraph 8.6 below, a reporting institution in identifying country and geographic risk factors, must refer to credible sources such as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports

published by international organisations such as the FATF, Asia Pacific Group on Money Laundering, United Nations, World Bank and International Monetary Fund.

Note:

A non-exhaustive list of websites that may be referred to in assessing the ML/TF risk exposure is published on the SC's website.

8.4 Enhanced CDD measures

8.4.1 Upon determining a customer as "high risk", a reporting institution must undertake enhanced CDD measures on the customer and, where applicable, the beneficial owner. These measures must include–

(a) obtaining additional information and verification on the customer and beneficial owner, particularly for non face-to-face transactions (e.g. volume of assets and other information from public database);

(b) obtaining additional information on the intended level and nature of the business relationship;

(c) enquiring on the source of wealth and source of funds;

(d) updating on a more regular basis, the identification data of the customer and the beneficial owner;

(e) obtaining approval from the senior management before establishing (or continuing for existing customer) such business relationship with the customer; and

(f) conducting enhanced ongoing monitoring on the business relationship.

8.5 Politically exposed persons (PEPs)

8.5.1 The requirements set out in paragraph 8.5 herein are also applicable to family members or close associates of PEPs. **Appendix B** of these Guidelines provides measures to be adopted by a reporting institution in dealing with the family members or close associates of PEPs.

8.5.2 A reporting institution is required to have in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

8.5.3 Upon determining that a customer or a beneficial owner is a foreign PEP, the

requirement to conduct enhanced CDD is applicable and the reporting institution is also required to conduct ongoing CDD.

8.5.4 A reporting institution is required to have in place reasonable measures to determine whether a customer or the beneficial owner is a domestic PEP or person entrusted with a prominent function by an international organisation. The reporting institution is required to assess the level of ML/TF risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function by an international organisation based on sufficient and appropriate information gathered through publically available information or other reasonable means.

8.5.5 For a high risk domestic PEP or high risk person entrusted with a prominent function by an international organisation, the requirements of enhanced CDD as set out in paragraph 8.4 are applicable.

8.5.6 For a domestic PEP or person entrusted with a prominent function by an international organisation that is assessed as low risk, the reporting institution may apply the standard CDD measures.

8.6 Higher-Risk Countries

8.6.1 A reporting institution is required to conduct enhanced CDD for any business relationship and transaction with any person from countries identified by–

(a) the FATF as issued under the "FATF Public Statement" – on jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial ML/TF risks emanating from such jurisdictions; or

(b) the Government of Malaysia as having ongoing or substantial ML/TF risks.

8.6.2 In addition to the enhanced CDD measures required under paragraph 8.6.1 above, the reporting institution is required to apply appropriate counter-measures, proportionate to the risk, for higher-risk countries as follows:

(a) Limiting business relationships or financial transactions with identified countries or persons located in the country concerned;

(b) Where relevant, to conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned; and

(c) Conduct any other measures as may be specified by the SC.

8.6.3 For business relationship and transaction with any person from countries identified by–

(a) the FATF as issued under the "FATF Public Statement"- on jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies; or

(b) the Government of Malaysia as having strategic AML/ CFT deficiencies and have not made sufficient progress in addressing the deficiencies;

a reporting institution is required to assess the risk and where the risk is identified as higher risk, the reporting institution is required to conduct enhanced CDD as set out in paragraph 8.4 above.

8.7 Reliance on third parties to conduct CDD

8.7.1 A reporting institution may rely on a third party to conduct CDD at the point of establishing a business relationship to identify a customer or a beneficial owner. The reporting institution must immediately obtain the necessary information concerning the identification of the customer or the beneficial owner. Reliance on third parties does not extend to verification of the customer or the beneficial owner's identity.

8.7.2 A reporting institution shall have in place internal policies and procedures to mitigate the risks when relying on a third party, including those from foreign jurisdictions. However, the reporting institution must ensure that the third party adequately applies the FATF Recommendations in determining the extent to which reliance could be placed on such third party.

8.7.3 A reporting institution is prohibited from relying on a third party located in higher- risk countries that have been identified as having ongoing or substantial ML/TF risks.

8.7.4 The relationship between a reporting institution and the third party relied upon to conduct the CDD, shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, the reporting institution must be satisfied that the third party–

(a) can obtain immediately the necessary information concerning the CDD in paragraph 8.1 above;

(b) has adequate standard CDD and enhanced CDD processes;

(c) has measures in place for record keeping requirements;

(d) can provide the standard CDD or enhanced CDD information and provide copies of the relevant documentation immediately upon request;

(e) is properly regulated and supervised by the respective authorities; and

(f) complies with the provisions of any applicable laws.

8.7.5 In addition to the requirements set out in paragraph 8.7.4 above, a reporting institution that relies on a third party that is part of the same group is subject to the following conditions:

(a) The group applies CDD and record- keeping requirements and AML/CFT programmes in line with these Guidelines;

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programmes are supervised at a group level by the relevant supervisory authority; and

(c) any higher country risk is adequately mitigated by the financial group's AML/CFT policies.

8.7.6 Where a reporting institution relies on a third party, the ultimate responsibility for CDD measures remains with the reporting institution.

8.8 Failure to satisfactorily complete CDD

8.8.1 A reporting institution must not commence any business relation, or execute any transaction, or in the case of existing customers, must terminate such business relationship, if the customer fails to comply with the CDD requirements.

8.8.2 A reporting institution must also consider lodging a STR in relation to such customer with the FIED.

9.0 GROUP-WIDE ML/TF PROGRAMMES

9.1 Where applicable, a reporting institution is required to implement appropriate group-wide ML/TF programmes appropriate to its holding company, branches and majority-owned subsidiaries. Such ML/TF programmes must include–

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) the provision at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(c) adequate safeguards on the confidentiality and use of information exchanged.

PART IV: RETENTION OF RECORDS

10. RECORD KEEPING

10.1 A reporting institution must keep record of all transactions and ensure they are up to date and relevant. The records must at least include the following information for each transaction:

(a) Documents relating to the identification of the customer in whose name the account is opened or transaction is executed;

(b) The identification of the beneficial owner or the person on whose behalf the account is opened or transaction is executed;

(c) Records of the relevant account pertaining to the transaction executed;

(d) The type and details of transaction involved;

(e) The origin and the destination of the funds, where applicable; and

(f) Such other information as the SC and BNM may specify in writing.

10.2 A reporting institution is required to maintain records for a period of at least seven years from–

(a) in the case of record obtained through the CDD and enhanced CDD process, the date the account is closed; or

(b) in the case of transaction records, the date the transaction is completed or terminated.

10.3 A reporting institution must retain a record beyond the retention period provided in paragraph 10.2 above, if the record is in relation to–

(a) a STR that has been lodged to FIED;

(b) a transaction that is subject to an ongoing investigation by any law enforcement agency; or

(c) a transaction that is subject to prosecution in court,

until it is confirmed that the case is closed or records are no longer required.

10.4 A reporting institution must retain, maintain and update the relevant records

(including CDD records) in such a way that–

(a) the relevant law enforcement agencies and internal and external auditors of the reporting institution will be able to reliably judge the reporting institution's transactions and its compliance with the AMLA;

(b) any transaction effected via the reporting institution can be reconstructed; and

(c) the reporting institution can satisfy within a reasonable time any enquiry or order from the relevant law enforcement agencies as to the disclosure of such relevant record.

PART V: SUSPICIOUS TRANSACTIONS

11. REPORTING OF SUSPICIOUS TRANSACTIONS

11.1 A reporting institution is required to have in place strong mechanisms for reporting suspicious transactions, including having an appointed AML/CFT compliance officer, and where appropriate, having a unit primarily responsible for complying with the AML/CFT requirements on reporting of suspicious transactions.

11.2 A reporting institution must also ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain the confidentiality and preservation of secrecy.

11.3 A reporting institution must clarify the economic background and purpose of any transaction or business relationship if it appears unusual in relation to the reporting institution's knowledge of the customer, or if the economic purpose or legality of the transaction is not immediately clear. Special attention should also be paid to all complex and unusual patterns of transaction.

11.4 A reporting institution must also consider whether the transactions involve a number of factors which when taken together may raise a suspicion that the transactions may be connected with certain unlawful activities.

11.5 In considering whether a transaction is suspicious, a reporting institution must take into account, among others, the following factors:

(a) The nature of, or unusual circumstances, surrounding the transaction;

(b) The known business background of the person conducting the transaction;

(c) The production of seemingly false identification in connection with any transaction, the use of aliases and a variety of similar but different addresses;

(d) The behaviour of the person or persons conducting the transactions; and

(e) The person or group of persons with whom they are dealing.

11.6 If in bringing together all relevant factors, a reporting institution has reasonable grounds to suspect that the transaction or the funds utilised involve proceeds of an unlawful activity or is related to terrorism financing, such transaction should be reported immediately to the FIED through lodgement of a STR.

11.7 Where the reporting institution decides that there are no reasonable grounds for suspicion to warrant a lodgement of a STR, the reporting institution must establish the grounds for such decision. In this regard, the compliance officer must ensure that the reporting institution's decision together with all supporting documentary evidence is recorded and maintained.

11.8 A reporting institution is required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. A reporting institution should be aware that in some cases, suspicion may be formed after a considerable time from the date of the transaction, in view of subsequent additional information.

11.9 STRs must be lodged to the FIED in accordance with the method as provided in **Appendix C** herein.

11.10 The fact that a STR may have been lodged with the FIED previously should not preclude the reporting institution from lodging a fresh STR if a new suspicion arises.

11.11 When required by FIED, a reporting institution must provide additional information and documentation and respond promptly to any further enquiries with regard to the STR lodged.

11.12 Where a reporting institution forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, the reporting institution is permitted not to pursue the CDD process and is required to lodge a STR.

11.13 The reporting institution must ensure that the compliance officer maintains a complete file of all internal reports on suspicious transactions and STRs lodged with FIED together with the relevant supporting documentary evidence.

11.14 The board of directors must ensure that the compliance officer has the necessary authority, resources and support to discharge his obligation independently and effectively in complying with the reporting institution's compliance policies and procedures on AML/CFT, particularly on reporting suspicious transactions.

11.15 The compliance officer has the sole discretion and independence to report suspicious transactions.

11.16 The compliance officer must act as a central reference point within the organisation for all AML/CFT matters, including–

(a) analysing identified suspicious transactions;

(b) reviewing regularly all internal reports on suspicious transactions or ad hoc

reports made by employees; and

(c) lodging of STRs to the FIED.

11.17 For the avoidance of doubt, unless permitted by law, a reporting institution and its directors, officers and employees are prohibited from disclosing the fact that a STR or related information is being filed with the FIED.

Note:

Some examples of suspicious transactions are published on SC's website. The list is non- exhaustive and only provides examples of ways in which money may be laundered through the capital market.

12. CONFIDENTIALITY OF REPORTING

12.1 It shall be an offence to disclose to anyone any information that a suspicion has been formed or that information or a STR has been communicated to the FIED and the SC or to infer that any of these have occurred.

12.2 A person does not commit an offence under paragraph 12.1 above, where such a disclosure is made pursuant to the provisions of the AMLA.

12.3 A reporting institution is required to establish proper policies and procedures to ensure effective controls when considering disclosures of report or related information under section 14A(3) of the AMLA.

12.4 The compliance officer must establish parameters on the types of report or related information that may be disclosed and to whom it may be disclosed under section 14A(3) of the AMLA. All disclosures made pursuant to these parameters must be properly documented with reasonable justification.

12.5 The compliance officer must ensure that the transmission of the report or related information must be conducted in a controlled environment and that confidentiality of the report or related information is safeguarded to avoid any leakage to an unauthorised third party.

PART VI: COMPLIANCE AND TRAINING PROGRAMMES

13. INTERNAL PROGRAMMES, POLICIES, PROCEDURES AND CONTROLS

13.1 Pursuant to the provisions of the AMLA, a reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls having regard to the ML/TF risks and size of business. These programmes shall include–

(a) procedures to ensure high standards of integrity of its directors, employees or persons acting on behalf of the reporting institution, and adopt a screening system to evaluate the personnel when hiring;

(b) regular independent audit function to check on the compliance and effectiveness of the reporting institution's AML/CFT framework in relation to the AMLA and provisions of these Guidelines. Any audit findings and any necessary corrective measures to be undertaken must be tabled to the board of directors;

(c) effective internal control systems to assess, profile and address ML/TF issues; and

(d) structured ongoing training programmes for directors and employees to enhance compliance with the reporting institution's policies and procedures on AML/CFT. The training programmes must be according to their level of responsibilities.

13.2 A reporting institution shall also designate compliance officers at management level in each of its branch, who will be responsible for the application of the AML/CFT internal programmes, policies and procedures.

13.3 The compliance officer appointed by a reporting institution must have necessary knowledge, expertise and the required authority to discharge his responsibilities effectively, including knowledge on the relevant laws and regulations and the latest AML/CFT developments. A reporting institution should encourage its compliance officer to pursue professional qualifications in AML/CFT to enable him to carry out his obligations effectively.

13.4 A reporting institution must also ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of a compliance officer include to ensure the following:

(a) The reporting institution's compliance with the AML/CFT requirements;

(b) The appropriate AML/CFT policies and procedures, including customer

identification, CDD, reporting of suspicious transactions and compliance and training programmes are implemented effectively;

(c) The AML/CFT policies and procedures are regularly assessed and kept up-to-date to ensure that they are effective and sufficient to address any changes in ML/TF trends;

(d) Timely reporting of the risk-based approach measures to the board of directors;

(e) All employees are aware of the reporting institution's AML/CFT framework;

(f) Internally generated reports on suspicious transactions are appropriately evaluated and recorded before submission to the FIED;

(g) The channel of communication for reporting suspicious transactions is secured and that information is kept confidential; and

(h) The ML/TF risks associated with new products and services or arising from the reporting institution's operational changes, including the introduction of new technology and processes, are identified and are brought to the attention of the board of directors.

13.5 Notwithstanding the duties of the compliance officer, the ultimate responsibility for proper supervision, reporting and compliance pursuant to AMLA and these Guidelines remains with the reporting institution and its board of directors.

PART VII: COMBATING TERRORISM FINANCING

14. IDENTIFICATION AND DESIGNATION

14.1 A reporting institution is required to keep itself updated with–

(a) the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures, in particular, the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 2253 (2015) and other subsequent resolutions which require sanctions against individuals and entities associated to al-Qaida, Taliban, and the Islamic State in Iraq (Da'esh) organisations; and

(b) orders as may be issued under sections 66B and 66C of the AMLA by the Minister of Home Affairs.

14.2 In ensuring efficient detection of suspected financing of terrorism, a reporting institution should maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLA by the Minister of Home Affairs (collectively referred to as "listed persons").

> **Note**:
> The updated UN Consolidated List can be obtained at http://www.un.org/.

14.3 For the purpose of implementing the obligations under section 66B and section 66C of AMLA, a reporting institution must conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, against the names in the database. If there is any name match, the reporting institution must take reasonable and appropriate measures to verify and confirm the identity of its customer. Upon such confirmation, the reporting institution must immediately–

(a) freeze without delay the customer's fund or block the transaction, if it is an existing customer;

(b) reject the customer, if the transaction has not commenced;

(c) lodge a STR with the FIED; and

(d) notify the SC.

14.4 A reporting institution is required to submit a STR when there is an attempted transaction by any of the listed persons.

14.5 A reporting institution must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match.

14.6 In addition to relying on the consolidated list, a reporting institution is also required to closely monitor news or developments concerning terrorist activities or terrorism financing. Where names of individuals or entities involved in such terrorist activities or terrorism financing are identified, the reporting institution must check these names against its existing customer database. Where there is a name match, the reporting institution must–

(a) lodge a STR with the FIED; and

(b) notify the SC.

14.7 **Appendix D** provides the detailed obligations of a reporting institution for the implementation of the targeted financial sanctions in relation to terrorism financing.

APPENDIX A

Guidance on Risk-Based Approach (RBA) for the purpose of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)

1.0 Introduction

1.1 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.

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) 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.

1.3 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.

1.4 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.

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 RBA Steps

2.1 The RBA entails two (2) assessments:

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.

Relationship-based Risk Assessment (RbRA)

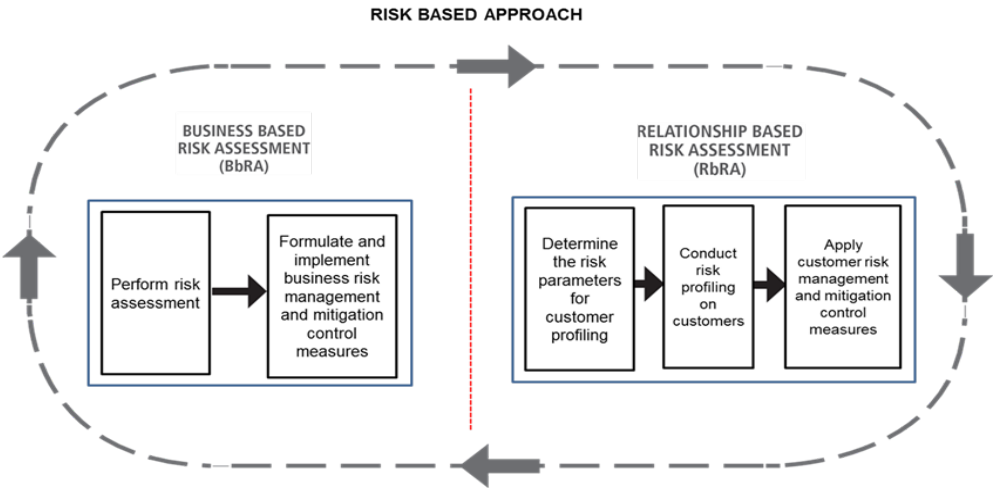
In a RbRA, a reporting institution must consider types of products, services, distribution channels, etc. that the customers are using and mitigate the risks identified.

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.

The RBA steps above are illustrated in the diagram below:



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

2.3 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.

2.4 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.

2.5 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.

Business-based Risk Assessment (BbRA)

3.0 A: Perform Risk Assessment

3.1 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.

3.2 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.

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, 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.

3.4 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.*

3.5 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
Transactions and Distribution Channels	Number of cash-based transaction	• Cash transaction above RM50,000
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

3.6 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.

3.7 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.

3.8 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.

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

4.1 Once the reporting institution has identified and assessed the ML/TF risks it faces upon performing its risk assessment under paragraph 3 above, a reporting institution must ensure that appropriate risk control measures are formulated and implemented in order to manage and mitigate these risks.

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

4.3 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 operation to other entities (Group).

4.4 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.

Relationship-based Risk Assessment (RbRA)

5.0 Determine the risk parameters for customer profiling

5.1 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
		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

5.2 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.

5.3 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.

5.4 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.

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

6.0 B: Conduct risk profiling on customers

6.1 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.

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

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

6.3 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.

6.4 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.

7.0 C: Apply customer risk management and mitigation control measures

7.1 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.

7.2 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.

APPENDIX B

Guidance on Politically Exposed Person (PEP) – Family Members and Close Associates of PEP

1.1 The requirements imposed on PEP also extend to family members and close associates of a PEP.

1.2 A reporting institution is required to effectively identify family members or close associates of a PEP.

Family Members of a PEP

1.3 Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage.

1.4 A family member of the PEP includes the PEP's:

(a) parents*;

(b) siblings*

(c) spouse;

(d) child*; or

(e) spouse's parents*;

(*) covers both biological and non-biological relationship.

Close Associates of a PEP

1.5 A close associate is an individual reasonably known to the reporting institution to be closely connected to a PEP, either socially or professionally.

1.6 An individual who is closely connected to a PEP may include the PEP's business partners or associates, extended family members, close friends and financially dependent individuals.

1.7 Reporting institutions must determine the extent to which the close associate is directly engaged or involved in the activity of the PEP on best effort basis.

Applicable CDD or Enhanced CDD Measures

Family Member or Close Associate of a Foreign PEP

1.8 If the customer or beneficial owner is identified as a family member or close associate of a foreign PEP, a reporting institution is required to conduct enhanced CDD.

Family member of Close Associate of a Domestic PEP or person entrusted with prominent public function by an international organisation (PEPFIO)

1.9 If the customer or beneficial owner is identified as a family member or close associate of a domestic PEP or PEPFIO, a reporting institution is required to assess the level of ML/TF risks posed by the business relationship with the family members or close associates.

1.10 In assessing the ML/TF risk level of customer or beneficial owner identified as family members or close associates of a domestic PEP or PEPFIO, the reporting institution may consider the following factors:

(a) The family members or close associates have business interests to the related PEP's public functions (conflict of interest);
(b) The social standing or official capacity of the family members or close associates are such that it can be controlled, directed or influenced by the PEP;
(c) Jurisdictions of which the family members or close associates originate from or reside in; and
(d) The family members or close associates are known to be involved in businesses or activities that have a high probability of being abused as a vehicle for ML/TF by the PEP.

1.11 For a domestic PEP or PEPFIO that is assessed as low risk, the reporting institution must apply the standard CDD measures and where he is assessed as high risk, enhanced CDD measures are applicable.

Source of Information of Family Members and Close Associates of a PEP

1.12 For the purpose of determining whether an individual is a family member or a close associate of a PEP, the reporting institution may refer to any information which is in its possession, or which is publicly known.

1.13 A reporting institution may refer to any of the following sources of information in identifying a family member or close associate of a PEP:

(a) internet and media searches;
(b) commercial databases;
(c) in-house databases and information sharing within financial group;
(d) customer's self-declaration; and/or
(e) risk information shared by supervisory/regulatory authorities.

1.14 The sources of information referred above are not exhaustive and a reporting institution is encouraged to develop its own internal references in identifying individuals who are family members or close associates of a PEP.

Extent of Application of Family Member or Close Associate of a PEP

1.15 A reporting institution should apply appropriate risk assessment on family members or close associates of a PEP who no longer holds prominent public function.

1.16 A reporting institution may consider the following factors in determining whether a family member or close associate of a PEP who no longer holds a prominent public function should be considered as high risk:

(a) the level of informal influence that the PEP could still exercise, even though he no longer holds a prominent public function; and

(b) whether the PEP's previous and current function (though not in a public/official capacity) are linked by the fact that the PEP continues to deal with the same substantive matters.

APPENDIX C

Submission of Suspicious Transaction Report (STR)

1. A STR should be lodged with the FIED using the prescribed STR form which can be downloaded via the BNM's website.

2. The lodgement of the STR may be made by any of the following means:

Mail	The physical forms should be placed in a sealed envelope and addressed to the following: Director Financial Intelligence and Enforcement Department Bank Negara Malaysia Jalan Dato' Onn 50480 Kuala Lumpur
Fax	03-2693 3625
E-mail	str@bnm.gov.my
Others (where and if available)	FIED's Financial Intelligence System (FINS) https://bnmapp.bnm.gov.my/fins2

APPENDIX D

Guidance on the Implementation of Targeted Financial Sanction in Relation to Terrorism Financing

The relevant legal instruments

1.1 Malaysia as a member of the United Nations has an obligation to implement all the Resolutions passed in relation to targeted financial sanctions (TFS) on terrorism financing. The United Nations Security Council Resolutions (UNSCR) relating to terrorism financing are implemented pursuant to section 66B and section 66C of the AMLA by publication in the gazette by the Minister of Home Affairs.

1.2 In implementing TFS, a reporting institution should refer to the relevant legal instruments as stated below:

AMLA Provision	Section 66C	Section 66B
Listing	UNSCR List	Domestic List
UNSC Resolutions	• UNSCR 1267 (1999) and UNSCR 1989 (2011) (Individuals and entities associated with Al-Qaida) • UNSCR 1988 (2011) and other subsequent resolutions (Individuals and entities associated with Taliban) • UNSCR 2253 (2015) and other subsequent resolutions (Individuals and entities associated with Islamic State in Iraq)	UNSCR 1373(2001)

Subsidiary Legislation	• *Anti-Money Laundering and Anti-Terrorism Financing (Security Council Resolution) (Al-Qaida and Taliban) (Amendment) Order 2011* (P.U.(A) 402/2011); • *Anti-Money Laundering and Anti-Terrorism Financing (Security Council Resolution) (Al-Qaida and Taliban) (Amendment) Order 2013* (P.U.(A) 187/2013); • *Anti-Money Laundering and Anti-Terrorism Financing (Security Council Resolutions) (Al-Qaida and Taliban) (Amendment) Order 2014* (P.U. (A) 225/2014); and • Other subsidiary legislations made under section 66C of the AMLA which may be issued by the Ministry of Home Affairs from time to time.	• *Anti-Money Laundering and Anti-Terrorism Financing (Declaration of Specified Entities and Reporting Requirements) Order 2014* (P.U.(A)93/2014); • *Anti-Money Laundering and Anti-Terrorism Financing (Declaration of Specified Entities and Reporting Requirements) (Amendment) Order 2014* (P.U.(A) 301/2014); and • Other subsidiary legislations made under section 66B of the AMLA which may be issued by the Ministry of Home Affairs from time to time.

Obligation to maintain the sanctions list

2.1 In implementing the requirements in paragraphs 14.1 and 14.2 of the Guidelines, a reporting institution should have policies and procedures to ensure compliance with the obligation to maintain the lists of listed entities in respect the UNSCR and domestic lists.

2.2 A reporting institution must take note that Amendment Order 2014 (P.U. (A) 225/2014) provides for an automatic application of the UNSCR lists by making reference to the updated list in the UN website. Therefore, for the UNSCR lists, a

reporting institution is advised to update its database regularly, not more than two weeks interval.

2.3 For the domestic lists, a reporting institution should keep the lists updated as soon as the subsidiary legislation via Orders are published in the gazette by the Ministry of Home Affairs.

2.4 Reporting institution must observe the following for the purpose of delisting any listed entities:

(a) For any listed entities under UNSCR list, delisting shall take effect automatically as soonest as the listed entities are removed from the UNSCR lists; and

(b) For any listed entities under the domestic list, delisting shall take effect upon the publication of the subsidiary legislation via Orders by the Ministry of Home Affairs on removal of such listed entities.

2.5 A reporting institution may consider subscribing electronic subscription services to maintain the updated UNSCR and domestic lists. However, the ultimate responsibility to ensure that the lists are up to date remains with the reporting institution.

Obligation to conduct screening on customers

3.1 The obligation to conduct screening on customers is applicable both on the existing as well as new and potential customers. As such, a reporting institution is required to conduct screening on the customers when it undertakes CDD and ongoing CDD.

3.2 A reporting institution is also required to screen its entire customer database within a reasonable time when the new names are listed by UNSCR or the domestic lists.

3.3 The obligation to conduct screening on customers also includes fund derived from property owned or controlled directly or indirectly by the listed entities or by persons acting on their behalf or at their discretion (related parties). Therefore, a reporting institution must also conduct checks on–

(a) relationship and transactions connected with the listed entities;

(b) properties or accounts that are jointly owned and/or indirectly controlled by the listed entities; and

(c) parties related to the frozen accounts including beneficial owners, signatories, power of attorney relationships, guarantors, nominees, trustees, assignees and payors.

3.4 Further, a reporting institution is also advised to search, examine and analyse past financial activities of the listed entities or related parties.

Obligation to freeze funds, properties or accounts

4.1 A reporting institution is required to freeze funds, properties or accounts that are owned or controlled directly and indirectly by the listed entities without delay[2].

4.2 Funds, properties or accounts that are owned or controlled indirectly by the listed entities includes situation where the listed entity is a director of a customer. In such instance, once the reporting institution is satisfied that the director owns or controls directly or indirectly the funds, properties or accounts of the customer, the reporting institution is required to freeze the same without delay.

4.3 The obligation to freeze funds, properties or accounts of a listed entity continues until the person is delisted from the sanction lists. Even death of the listed entity is not a basis for a reporting institution not to continue its freezing obligation.

4.4 If an asset is owned or controlled by a listed entity and the interest owned or controlled by the listed party cannot be segregated, then the entire asset should be subjected to freezing.

4.5 Notwithstanding the funds, properties or accounts are frozen, a reporting institution may continue receiving dividends, interests, or other benefits, but such benefits shall still remain frozen, so long as the individuals or entities continue to be listed.

4.6 However no outgoing payment should be made out from the frozen funds, properties or accounts, including payment of any fees or service charges for maintaining the frozen funds without the approval of Minister of Home Affairs.

Reporting requirements

5.1 Once a reporting institution determines that it is in the possession of funds, properties or accounts that are owned or controlled by or on behalf of the listed entity, the reporting institution is required to report to the following authorities. This obligation also extends to any attempted transactions undertaken by listed entities or related parties:

[2] According to FATF, without delay is defined to be ideally within a matter of hours of designation by the United Nations Security Council.

No.	Authority	Source of obligation
1.	SC as the relevant Supervisory Authority	• Section 66D(2) of AMLA • Section 66E of AMLA • Paragraph 14.3 (d) of the Guidelines
2.	FIED, Bank Negara Malaysia [as STR]	• Paragraph 14.3 (c) of the Guidelines
3.	Inspector-General of Police	• Section 66B(3)(d) of the AMLA

5.2 For the purpose of submitting suspicious transaction report to the FIED, a reporting institution–

(a) should include details and analysis of the CDD, ongoing CDD information, activities of transactions of the listed entity or related parties; and

(b) is encouraged to search, examine and analyse past financial activities of customers and related parties with a name match that have closed their accounts with the reporting institution.

5.3 A reporting institution is also under an obligation to report to the SC periodically every six months for both lists on frozen funds, properties or accounts of customers that are listed.

List	UNSCR List	Domestic List
Reporting intervals	Every 31 January and 31 July	Every 31 May and 30 November

False positives

6.1 A reporting institution may forward queries to the Ministry of Home Affairs to ascertain whether or not the customer is a listed individual or entity in cases of similar name match with any listed entities.

6.2 A reporting institution should direct its customers to the Ministry of Home Affairs to verify the false positive match in the event their accounts have been mistakenly frozen or transactions have been mistakenly rejected or blocked.

The contact point for the Ministry of Home Affairs in relation to targeted financial sanctions on terrorism financing is:

Secretary General
Ministry of Home Affairs
Level 10, Block D1, Complex D
62546 Putrajaya
(Attn.: Security and Public Order Division)
Tel: 03-8886 8000 ext. 8064, 8543, 8055, 3453
Fax: 03-8889 1763
Email: amlcft@moha.gov.my
Website: http://www.moha.gov.my/index.php/en/maklumat-perkhidmatan/membanteras-pembiayaan-keganasan