Suruhanjaya Sekuriti
Securities Commission
Malaysia

# GUIDELINES ON PREVENTION OF MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, COUNTERING PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS FOR REPORTING INSTITUTIONS IN THE CAPITAL MARKET

**SC-GL/AML-2014 (R3-2024)**


| | |
|---|---|
| 1st issued | : 15 January 2014 |
| Revised | : 13 June 2024 |

# GUIDELINES ON PREVENTION OF MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, COUNTERING PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS FOR REPORTING INSTITUTIONS IN THE CAPITAL MARKET

| | |
|---|---|
| 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) |
| 2nd revision | 26.4.2021 | 26.4.2021 | SC-GL/AML-2014(R2-2021) |
| 3rd revision | 13.6.2024 | 13.6.2024 | SC-GL/AML-2014 (R3-2024) |

# CONTENTS

**APPENDICES** **Page**

# PART I: INTRODUCTION AND APPLICABILITY

## 1.0 INTRODUCTION

1.1 The *Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market* (Guidelines) are issued pursuant to the following:

(a) in relation to anti-money laundering and countering financing of terrorism including Targeted Financial Sanctions relating to Terrorism Financing (TFS-TF), section 158(1) and section 160A of the *Securities Commission Malaysia Act 1993 (SCMA)* read together with section 66B, section 66E and section 83 of the *Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)*;

(b) in relation to countering proliferation financing including Targeted Financial Sanctions relating to Proliferation Financing (TFS-PF), section 158(1) and section 160A of the SCMA read together with the following legislations (collectively referred to as "TFS-PF related legislations") which provides the legal basis for domestic implementation of TFS-PF in relation to United Nations Security Council Resolutions (UNSCR) imposed on the designated countries and persons:

(i) *Strategic Trade Act 2010* (Act 708) (STA);

(ii) Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 *(P.U. (A) 481/2010)* [1];

(iii) Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 *(P.U. (A) 484/2010);*

(iv) Strategic Trade (Delisting of Prohibited End-Users) Regulations 2014 (*P.U. (A) 289/2014)*; and

(v) Strategic Trade (Unfreezing of Property in relation to Prohibited End-Users) Regulations 2014 *(P.U. (A) 290/2014).*

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

[1] Regulation 3 of Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 *(P.U. (A) 481/2010)* is set out in **Appendix G** of these Guidelines.

1.3 These Guidelines provide:

(a) requirements and obligations imposed on reporting institutions in preventing and combating money laundering, terrorism financing, proliferation financing and targeted financial sanctions; and

(b) guidance for reporting institutions to comply with the obligations imposed under the AMLA and TFS-PF.

1.4 These Guidelines supersede and replace the *Guidelines on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing for Capital Markets*.

1.5 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.

1.6 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, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs)* issued by BNM. Where there are differing requirements between the said guidelines, the more stringent requirements shall apply.

1.7 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. Enforcement actions can be taken against the reporting institutions including its directors, officers, representatives, employees for any non-compliance with any requirements in these Guidelines.

## 2. APPLICABILITY

2.1 These Guidelines are applicable to reporting institutions as defined under Part I on Definition, Part VII on Combating Terrorism Financing and Part VIII on Combating Proliferation Financing as the case may be, including its branches and majority-owned subsidiaries outside Malaysia which carry out, among others, the activities as listed in the First Schedule of the AMLA.

2.2 In the case of foreign operations, where anti-money laundering, counter financing terrorism and counter proliferation financing (AML/CFT/CPF) 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/CPF 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/CPF measures consistent with the Malaysian standards, the reporting institution is required to apply appropriate additional measures to mitigate the money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks and inform the SC on the AML/CFT/CPF gaps and additional measures implemented to manage the ML/TF/PF 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.

2.5 Part VIII of these Guidelines set out TFS-PF obligations that must be complied with by reporting institutions. The Strategic Trade Controller may from time-to-time issue new guidelines or directives under the STA which a reporting institution may need to comply with. In this regard, the SC will notify all relevant reporting institutions of such issuances accordingly. Where there are differing requirements, the more stringent requirements shall apply.

2.6 The SC may, upon application, grant an exemption from or variation to the requirements of these Guidelines if the SC is satisfied that:

(a) such variation is not contrary to the intended purpose of the relevant requirement in these Guidelines; or

(b) there are mitigating factors which justify the said exemption or variation.

## 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, AMLA and TFS-PF legislations:

| | |
|---|---|
| AML/CFT/CPF | means Anti-Money Laundering / Counter Financing of Terrorism / Counter Proliferation Financing. |
| beneficial owner | in the context of legal person, means any natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes the natural person who exercises ultimate effective control over a legal person.<br><br>Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.<br><br>in the context of legal arrangements, beneficial owner includes: (a) the settlor(s); (b) the trustee(s); (c) the protector(s) (if any); (d) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (e) any other natural person(s) exercising ultimate effective control over the legal arrangement. In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.<br><br>Reference to "ultimate effective control" over trusts or similar legal arrangements includes situations in which ownership or control is exercised through a chain of ownership or control. |
| beneficiary | the meaning of the term *beneficiary* depends on |

| | |
|---|---|
| | the context. |
| | in trust law, a beneficiary refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period or following exercise of trustee discretion in the case of a discretionary trust.<br><br>In wire transfer, refers to the natural or legal person or legal arrangement identified by the originator as the receiver of the requested wire transfer. |
| beneficiary institution | in wire transfer, refers to the institution which receives the wire transfer from the ordering institution and makes the digital assets available to the beneficiary. |
| CMSA | means *Capital Markets and Services Act 2007.* |
| constituent document | in relation to a body corporate or an unincorporated body, means any document or instrument that:<br><br>(a) constitutes, establishes or incorporates the body;<br>(b) sets out its governing and administrative structure; or<br>(c) sets out the scope of its functions, business, powers or duties. |
| customer | means new or existing[2] customer. |

[2] Refers to those customers who are customers prior to CDD obligations under section 16 of AMLA becoming applicable to the reporting institution.

| | |
|---|---|
| customer due-diligence (CDD) | means any measures undertaken pursuant to section 16 of AMLA. |
| digital asset | refers collectively to a digital currency and digital token. |
| digital currency | means a digital currency that is prescribed as securities under the *Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019.* |
| digital token | means a digital token that is prescribed as securities under the *Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019.* |
| designated person | means a person who has been designated under the Second Schedule of the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 *(P.U. (A) 484/2010)*. |
| FIED | means the Financial Intelligence and Enforcement Department of Bank Negara Malaysia. |
| financial group | means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subjected to AML/CFT/CPF policies and procedures at the group level. |
| 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 companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entity. |

| | |
|---|---|
| National Risk Assessment (NRA) | National Risk Assessment (NRA) by the National Coordination Committee to Counter Money Laundering (NCC) assesses and identifies the key threats and sectoral vulnerabilities that Malaysia's financial system and economy is exposed to, has guided the strategies and policies of Malaysia's overall AML/CFT/CPF regime. The NRA is the primary tool used for periodic assessment and tracking of effectiveness of the relevant Ministries, law enforcement agencies, supervisory authorities and reporting institutions in preventing and combating ML/TF/PF.<br><br>Reference to NRA is not limited to the National ML/TF Risk Assessment and includes any sectoral, thematic or emerging risk assessments undertaken by the NCC. |
| nominator | means an individual (or group of individuals) or legal person that issues instructions (directly or indirectly) to a nominee to act on its behalf in the capacity of a director or a shareholder, also sometimes referred to as a 'shadow director' or 'silent partner'. |
| nominee | means an individual or legal person instructed by the nominator to act on its behalf in a certain capacity regarding a legal person. |
| nominee director | means an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct or indirect instructions of the nominator. A nominee director is never the beneficial owner of a legal person. |
| nominee shareholder | means an individual or legal person that exercises the associated voting rights according to the instructions of the nominator and/or receives dividends on behalf of the nominator. A nominee shareholder is never the beneficial owner of a legal person based on the shares it holds as a nominee. |

| | |
|---|---|
| ordering institution | refers to the institution which initiates a wire transfer of digital asset upon receiving the request of a wire transfer of digital asset on behalf of the originator. |
| originator | refers to the account holder or customer who allows the wire transfer of digital asset from his account, or where there is no account the natural or legal person that places the order with the ordering institution to perform the wire transfer of digital asset. |
| politically exposed person (PEP) | means—<br><br>(a) 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;<br><br>(b) 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<br><br>(c) 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.<br><br>The definition of PEP is not intended to cover middle ranking or more junior individual in the foregoing categories. |
| related party | means— |

| | |
|---|---|
| | (a) person acting on behalf of or at the direction or under the control of designated person;<br><br>(b) person engaged in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;<br><br>(c) person assisting designated person in evading sanctions, or violating resolution provisions; and<br><br>(d) person with joint ownership or the beneficiaries of the assets (which includes property) of a designated person. |
| reporting institution | means a person carrying on regulated activities or registered under the CMSA as specified under the First Schedule of the AMLA. |
| senior management | refers to any person having authority and responsibility for planning, directing or controlling the activities of a reporting institution or a legal person or legal arrangement including the management and administration of a reporting institution, legal person or legal arrangement. |
| STR | means a Suspicious Transaction Report, to be submitted to FIED as in **Appendix C**. |
| strategic trade controller | has the same meaning assigned to the word Controller in the *Strategic Trade Act 2010*. |
| third-party institution | means a financial institution that is supervised and monitored and meets the requirements under paragraph 8.6 of these Guidelines, who is relied upon by the reporting institution to conduct the due diligence process.<br><br>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. |
| third-party deposit | refer to monies deposited by a third-party into the customer's account with a reporting institution. |
| third-party payment | refer to monies paid from the customer's account into a third-party account. |
| TFS-PF | means Targeted Financial Sanctions relating to Proliferation Financing. |
| TFS-TF | means Targeted Financial Sanctions relating to Terrorism Financing. |
| UN | means United Nations. |
| unique transaction number | refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer. |
| UNSCR | means United Nations Security Council Resolution. |
| Virtual Asset Service Providers (VASP) | means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for on behalf of another natural or legal person:<br>(a) exchange between virtual assets and fiat currencies;<br>(b) exchange between one or more forms of virtual assets;<br>(c) transfer of virtual assets;<br>(d) safekeeping and/or administration of virtual assets or instruments enabling |

| | |
|---|---|
| | control over virtual assets; and<br><br>(e) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. |
| wire transfer | refers to any transaction carried out on behalf of an originator through an institution by electronic means with a view to making an amount of digital asset available to a beneficiary at a beneficiary institution irrespective of whether the originator and the beneficiaryare the same person. |

## 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 notbe 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.

## 5A. GENERAL DESCRIPTION OF PROLIFERATION FINANCING

5A.1 In response to growing concerns over the proliferation of nuclear, biological and chemical weapons and their means of delivery which continue to pose a significant threat to international peace and security, the United Nations Security Council (UNSC) has intensified efforts to strengthen its global sanctions regime in order to prevent, suppress and disrupt proliferation of weapons of mass destruction and its financing.

5A.2 As is the case with other UNSC sanctions programmes, targeted financial sanctions on countries and specifically identified individuals and entities (i.e. designated persons) is the primary aspect of its overall sanctions regime to effectively disrupt financial flows across known proliferation networks.

5A.3 Recommendation 7 of the Financial Action Task Force (FATF) Standards requires countries to implement TFS-PF made under UNSCRs. Under this standard, countries are required to implement targeted financial sanctions without delay to comply with UNSCRs relating to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing.

5A.4 Proliferation financing refers to the act of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction (WMD) proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).

5A.5 TFS-PF are applicable to persons designated by the UNSC or the relevant committees set up by the UNSC. Designation or listing criteria are:

(a) Person engaging in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;

(b) Acting on behalf of or at the direction of designated person;

(c) Owned or controlled by designated person; and

(d) Person assisting designated person in evading sanctions, or violating UNSCR provisions.

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

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

6.2 In combating ML/TF/PF, 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/PF 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, TFS-PF related legislations and these Guidelines. A reporting institution must also ensure ongoing training programmes are conducted to keep its board of directors, senior management 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/PF 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.

# PART IA: AML/CFT/CPF INTERNAL PROGRAMMES AND OBLIGATIONS OF THE BOARD OF DIRECTORS, SENIOR MANAGEMENT AND COMPLIANCE OFFICER

## 6A. INTERNAL PROGRAMMES, POLICIES, PROCEDURES AND CONTROLS

6A.1 A reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls having regardto its ML/TF/PF risks and size of business. These programmes shall include–

(a) procedures to ensure high standards of integrity of its board of directors, senior management, 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/CPF framework in relation tothe 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/PF 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/CPF. The training programmes must be according to their level of responsibilities.

## 6B. BOARD OF DIRECTORS

6B.1 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.

6B.2 The board of directors has the following roles and responsibilities:

(a) maintain accountability and oversight for establishing AML/CFT/CPF policies and procedures;

(b) provide oversight and accord adequate priority and dedicated resources to manage ML/TF/PF risks faced by the reporting institution including defining the lines of authority and responsibility for implementing the AML/CFT/CPF measures;

(c) approve policies and procedures regarding AML/CFT/CPF measures within the reporting institution;

(d) ensure that the policies and procedures are implemented effectively by the senior management;

(e) monitor the effectiveness of the implementation of the policies and procedures;

(f) ensure that the policies and procedures are periodically reviewed and improved where required in line with the changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF/PF;

(g) ensure effective independent audit function in assessing and evaluating the robustness and adequacy of overall AML/CFT/CPF measures; and

(h) ensure that the board keeps itself updated and is aware of new or emerging trends of ML/TF/PF including the relevant UNSCRs and any order issued pursuant to section 66B of the AMLA and understand the potential impact of such developments to the reporting institution.

***Guidance for paragraph 6B.2(c):***

*AML/CFT/CPF measures include but are not limited to those required for risk assessment, mitigation and profiling, customer due diligence (CDD), record keeping, enhanced CDD and ongoing due diligence, suspicious transaction report and targeted financial sanctions.*

***Guidance for paragraph 6B.2(f):***

*Periodic reviews and improvements of policies and procedures are to be conducted where there are changes and developments in a reporting institution's products, services, technology, regulatory development, nature of business to capture changes in distribution channel, clients' segment and etc.*

## 6C. SENIOR MANAGEMENT

6C.1 The senior management is responsible for effective implementation of AML/CFT/CPF internal programmes, policies and procedures that can manage the ML/TF/PF risks identified. In particular, the senior management has the following roles and responsibilities:

(a) be aware of and understand the ML/TF/PF risks associated with among others its business activities or strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new business activities or strategies, new products, new delivery channels and new geographical coverage;

(b) formulate AML/CFT/CPF policies to ensure that they are in line with the risks profiles, nature of business, complexity, value or volume of the transactions undertaken by the reporting institution and its geographical coverage;

(c) establish appropriate mechanisms to effectively formulate and implement AML/CFT/CPF policies and procedures approved by the board of directors;

(d) undertake review and propose to the board of directors the necessary enhancements to the AML/CFT/CPF policies to reflect changes in the reporting institution's risk profiles;

(e) provide periodic reporting to the board of directors on the level of ML/TF/PF risks faced by the reporting institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT/CPF which may have an impact on the reporting institution;

(f) allocate adequate resources to effectively implement and administer AML/CFT/CPF compliance programmes that are reflective of the size and complexity of the reporting institution's operations and risk profiles;

(g) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT/CPF policies and procedures to all relevant employees;

(h) ensure that AML/CFT/CPF issues raised are addressed in a timely manner; and

(i) provide appropriate levels of AML/CFT/CPF training for employees throughout the organisation.

## 6D. COMPLIANCE OFFICER

6D.1 A reporting institution shall designate compliance officers at management level in each of its branches, who will be responsible for the compliance of the AML/CFT/CPF internal programmes, policies and procedures.

6D.2 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/CPF developments. A reporting institution should encourage its compliance officer to pursue professional qualifications in AML/CFT/CPF to enable him to carry out his obligations effectively.

6D.3 A reporting institution must also ensure that the roles and responsibilities of the compliance officer are clearly defined and documented.

6D.4 The roles and responsibilities of a compliance officer include to ensure the following:

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

(b) Effective implementation of appropriate AML/CFT/CPF policies and procedures, including CDD, ongoing due diligence, reporting of suspicious transactions, record keeping, combating the financing of terrorism and compliance and training programmes;

(c) AML/CFT/CPF 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/PF 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/CPF measures, including policies, control mechanism and reporting channels;

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

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

(h) The ML/TF/PF 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.

## 6E. GROUP-WIDE AML/CFT/CPF PROGRAMMES

6E.1 The requirements under this paragraph 6E are only applicable to reporting institutions that are part of a financial group.

6E.2 Where applicable, a reporting institution is required to implement appropriate group-wide AML/CFT/CPF programmes appropriate to its branches and majority-owned subsidiaries. Such AML/CFT/CPF programmes must include–

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

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

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

# PART II: RISK-BASED APPROACH APPLICATION

## 7. RISK-BASED APPROACH APPLICATION

### 7.1 ML/TF Risk assessment

7.1.1 A reporting institution must take appropriate steps to identify, assess and understand its ML/TF risks, in relation to its customers, countries or geographical areas and products, services, transactions or delivery channels, and other relevant risk factors. **Appendix A** of these Guidelines provides for the measures to be adopted in implementing a risk-based approach.

7.1.2 The risk assessment 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.

7.1.3 A reporting institution must conduct additional assessment as and when required by the SC.

7.1.4 A reporting institution must be guided by the results of the NRA issued by the National Coordination Committee to Counter Money Laundering (NCC) in conducting its own risk assessments. A reporting institution must take enhanced measures to manage and mitigate the risks identified in the NRA.

*Guidance for paragraphs 7.1.1, 7.1.2, 7.1.3 and 7.1.4 :*

*In conducting the ML/TF risk assessment, reporting institutions may consider whether:*

*(a) they are susceptible to the key and emerging crimes as well as higher-risk sectors identified in the NRA; and*

*(b) enhancements to their AML/CFT compliance programme are warranted to ensure any areas of higher ML/TF risks are appropriately mitigated.*

7.1.5 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.

## 7.2 ML/TF 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 and assessed;

(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.

7.2.2 The risk control and mitigation measures implemented by reporting institutions must commensurate with the risk profile of the particular customer or type of customer.

## 7.3 PF Risk assessment

7.3.1 A reporting institution must take appropriate steps to identify, assess and understand PF risks, in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels, and other relevant risk factors where the extent of the assessment shall be appropriate to the nature, size and complexity of its business. The PF risk in this context is limited to potential breach, non-implementation or evasion of the targeted financial sanctions on PF under Part VIII of these Guidelines. **Appendix A** of these Guidelines provides for the measures to be adopted in implementing a risk-based approach.

7.3.2 In conducting the risk assessment, a reporting institution may consider if the existing ML/TF risk assessments methodologies are adequate to incorporate PF risks and may not necessarily require a stand-alone or an entirely new methodology.

7.3.3 The risk assessment processes must incorporate the following:

(a) Documenting the reporting institution's PF 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.

7.3.4 A reporting institution is also required to identify and assess the PF 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.

7.3.5 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 PF risks that have been identified and assessed;

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

(c) take commensurate measures to manage and mitigate the risks:

(i) where higher PF risks are identified, a reporting institution must ensure that it adequately address such higher PF risk by introducing enhanced controls to detect possible breaches, non-implementation or evasion of targeted financial sanctions on PF under Part VIII of these Guidelines;

(ii) where lower PF risks are identified, reporting institution must ensure that the measures applied are commensurate with the level of PF risk while still ensuring full implementation of the targeted financial sanctions on PF under Part VIII of these Guidelines.

## 7.4 PF Risk management and mitigation

7.4.1 A reporting institution must ensure full implementation of the targeted financial sanctions on PF as per Part VIII of these Guidelines irrespective of the institutional PF risk level.

## 7.5 Risk profiling of customers

7.5.1 A reporting institution must implement and maintain appropriate policies and procedures to conduct risk profiling of its customer.

7.5.2 A reporting institution must conduct risk profiling on its customers during the establishment of the business relationship and assign a ML/TF/PF risk rating that commensurate with the customer's risk profile.

7.5.3 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, types of PEP, types of occupation;

(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.

7.5.4 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/PF 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.

7.5.5 After the initial acceptance of the customer, reporting institutions are required to regularly update the customer's risk profile based on their level of ML/TF/PF risks.

*Guidance for paragraph 7.5.3:*

*In identifying countries and geographic risk factors, reporting institutions may refer to credible sources such as mutual evaluation reports, detailed assessment report, follow-up reports and other relevant reports published by international organisations and other inter-governmental bodies.*

## 7.6 Risk management and mitigation in third-party deposits and payments

7.6.1 There are ML/TF/PF risks as well as other risks associated with third-party deposits made into accounts maintained by customers of a reporting institution.

7.6.2 In view of the risks associated with third-party deposits, reporting institutions must in conducting its risk assessment consider and assess the risk arising from third-party deposits and ensure that appropriate control measures are implemented to mitigate the risk and/or prevent ML/TF/PF activities.

7.6.3 A reporting institution which accepts third-party deposit must at minimum, comply with the requirements on control measures in accepting third-party deposits set out in **Appendix A1** of these Guidelines.

7.6.4 A reporting institution which is unable to exercise appropriate control measures to mitigate the inherent ML/TF/PF risk and other associated risks and meet the relevant compliance requirements must not accept any third-party deposits.

7.6.5 Generally, a reporting institution must not accept any request from customers for payments to be made from the customers' account into a third-party account except in exceptional circumstances where permitted in relevant guidelines.

# 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 must conduct CDD on customer and 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 For the purpose of conducting CDD, 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 the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from reliable sources, such that the reporting institution is satisfied that it knows who the beneficial owner is; 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 Where applicable, in conducting CDD, a reporting institution is required to comply with requirements on targeted financial sanctions in relation to:

(a) terrorism financing under Part VII of these Guidelines; and

(b) proliferation financing under Part VIII of these Guidelines.

**CDD requirements for individual customer and beneficial owner**

*Identification and Verification*

8.1.6 In conducting CDD, a reporting institution is required to identify an individual customer or beneficial owner, by obtaining **at least** the following information:

(a) Full name;

(b) National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents of the individual customer or beneficial owner;

(c) Residential and mailing address;

(d) Date of birth;

(e) Nationality;

(f) Occupation type;

(g) Name of employer or nature of self-employment or nature of business/sector;

(h) Income or range of income;

(i) Contact number (home, office or mobile);

(j) Email; and

(k) Purpose of transaction.

8.1.7 Where the above information is not sufficient for the reporting institution to complete its identification and verification process, the reporting institution must seek further relevant information from the individual customer or beneficial owner.

**CDD requirements for legal persons**

8.1.8 For customers that are legal persons, a reporting institution is required to understand the nature of the customer's business, its ownership and control structure.

8.1.9 A reporting institution is required to identify its customers and verify its identity through the following information:

(a) 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, unique identifier such as tax identification number or any other reliable references;

(b) 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

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

8.1.10 A reporting institution is required to identify and take reasonable measures to verify the identity of the beneficial owner of a legal person by taking into consideration the following information or document:

(a) duly certified true copy/duly notarised copy of the latest Forms 24 and 49 as prescribed by the Companies Commission of Malaysia under the Companies Act 2016 or equivalent document for a foreign body corporate; and identification document of the shareholders with an equity interest of more than 25%, directors, partners and office bearers (as the case may be);

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

(c) 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

(d) 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.

8.1.11 A reporting institution is required to identify and take reasonable measures to verify the identity of beneficial owners according to the following cascading steps:

(a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person. Where applicable, this includes identifying:

(i) shareholders with equity interest of more than twenty-five percent in a corporation; and

(ii) in the case of a limited liability partnership, partners with capital contribution and/or voting rights of more than twenty-five percent;

(b) to the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in paragraph 8.1.11(a) or where no natural person(s) exert control through ownership interests, the identity of the natural person (if any) exercising control of the legal person through other means; and

(c) where no natural person is identified under paragraphs 8.1.11(a) or (b), the identity of the relevant natural person who holds the position of senior management.

For the avoidance of doubt, a reporting institution is not required to pursue steps (b) and (c) in circumstances where beneficial owner(s) have been identified through step (a). Similarly, where beneficial owner(s) have been identified at step (b), reporting institutions are not required to pursue step (c).

8.1.12 Notwithstanding the above, a reporting institution is exempted from obtaining the constituent document, and from verifying the identity of the directors and shareholders or partners 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) An authorised person, an operator of a designated payment system, under the *Financial Services Act2013* or the *Islamic Financial Services Act 2013*;

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

(e) Persons licensed or registered under the CMSA;

(f) Prescribed institutions under the *Development Financial Institutions Act 2002*; and

(g) Licensed entities under *Money Services Business Act 2011*.

8.1.13 Notwithstanding the above, reporting institutions are required to identify and maintain the information relating to the identity of the directors and shareholders or partners of legal persons referred to in paragraph 8.1.12 (a) to (g), through a public register, other reliable sources or based on information provided by the customer.

**CDD requirements for legal arrangements**

8.1.14 For customers that are legal arrangements, a reporting institution is required to understand the nature of the customer's business, its ownership and control structure.

8.1.15 A reporting institution is required to identify its customers and verify its identity through the following information:

(a) 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, unique identifier such as tax identification number or any other reliable references;

(b) The powers that regulate and bind the customer, as well as names of relevant persons having a senior management position; and

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

8.1.16 A reporting institution is required to identify and take reasonable measures to verify the identity of the beneficial owner of a legal arrangement by taking into consideration the following information:

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

(b) In the case of other types of legal arrangement, the identity of the person in an equivalent or similar position referred to in (a) above.

8.1.17 A reporting institution is required to ensure that trustees or persons holding equivalent positions in similar legal arrangements disclose their status or function in the legal arrangement when establishing business relations.

*Guidance for paragraphs 8.1.8 to 8.1.17*

***Appendix E*** *of these Guidelines sets out guidance and recommended best practices to guide reporting institutions in complying with the relevant requirements in relation to identification of beneficial owners of legal persons and legal arrangement.*

8.1.18 A reporting institution may rely on a third-party institution to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.

8.1.19 Where reliance is placed on a third-party institution under paragraph 8.1.18, a reporting institution is required to comply with paragraph 8.6 of these Guidelines.

**CDD requirements for clubs, societies or charities**

8.1.20 For customers that are clubs, societies or charities, a reporting institution must conduct the CDD requirements applicable for legal person or legal arrangements, as the case may be, and require them to furnish the relevant identification documents including Certificate of Registration and constituent documents. In addition, a reporting institution is required to identify and verify the office bearer, or any person authorised to represent the club, society or charity, as the case may be.

8.1.21 A reporting institution is also required to take reasonable measures to identify and verify the beneficial owners of the clubs, societies or charities.

8.1.22 Where there is any doubt as to the identity of persons referred to under paragraphs 8.1.20 and 8.1.21, the reporting institution must verify the authenticity of the information provided by such person with the Registrar of Societies, Labuan Financial Services Authority, Companies Commission of Malaysia, Legal Affairs Division under the Prime Minister's Department or any other relevant authority.

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

8.1.23 This section applies when a reporting institution chooses to establish non-face-to-face business relationship.

(a) A reporting institution must develop and implement policies and procedures to address and mitigate specific ML/TF/PF risks associated with establishing non face-to-face business relationship, as well as operational and information technology risk.

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

(c) For the purpose of identification and verification of the identity of a customer in a non face-to-face business relationship, a reporting institution must undertake one or more 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 identify and verify the customer's identity;

(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; or

(v) Using new technology solutions including, but not limited to, biometric technologies (e.g. fingerprint or iris scans, facial recognition), which should be linked incontrovertibly to the customer.

(d) Where the reporting institution is unable to identify and 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.

(f) A reporting institution must ensure and be able to demonstrate on a continuing basis that appropriate measures for identification and verification of a customer's identity when establishing non-face-to-face business relationship are as effective as that for face-to-face customer and implement monitoring and reporting mechanism to identify potential ML/TF/PF activities.

**Delayed verification**

8.1.24 A reporting institution may complete the verification after the establishment of the business relationship ("delayed verification") to allow some flexibility for its customer and beneficial owner to furnish the relevant documents in circumstances where verification is not possible at the point of establishing business relationship.

8.1.25 Where delayed verification applies, the following conditions must be satisfied:

(a) Before the reporting institution adopts a delayed verification, the reporting institution must have in place appropriate risk management policies and procedures which can effectively manage any ML/TF/PF risk arising from delayed verification;

(b) The delay is essential so as not to interrupt the reporting institutions' normal conduct of business;

(c) The ML/TF/PF risks are effectively managed; and

(d) There is no suspicion of ML/TF/PF.

8.1.26 The policies and procedures must include:

(a) Establishing a reasonable timeframe for the completion of the identity verification measures to ensure that delayed verification occurs as reasonably practicable. The reasonable timeframe shall not exceed 10 working days or any other period as may be specified by the SC;

(b) Measures that a reporting institution may take to manage risks of delayed verification including conditions under which the customer may utilize the business relationship prior to verification and placing appropriate limits on the number, types and/or amount of transactions that can be performed;

(c) Monitoring of large and complex transactions being carried out outside the expected norms pending completion of verification; and

(d) Keeping senior management periodically informed of any cases pending identity.

8.1.27 If verification cannot be completed within the reasonable timeframe, the reporting institution should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions. However, following the termination of business relationship, the reporting institution may return funds or other assets to the customers.

8.1.28 The reporting institution must assess whether the failure to complete verification within the reasonable timeframe provides sufficient grounds for making a STR to the FIED.

**Existing Customers**

8.1.29 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 obtained and verified.

*Guidance for paragraph 8.1.29:*

*In assessing materiality and risk of existing customers, reporting institutions may consider the following circumstances:*
*(i) the nature and circumstances surrounding the transaction including the significance of the transaction;*
*(ii) any material change in the way the account or business relationship is operated; or*
*(iii) insufficient information held on the customer or change in customer's information.*

## 8.2 Conducting CDD

8.2.1 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.

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

(a) Customer risk factors:

(i) The business relationship is conducted in unusual circumstances.

(ii) Non-resident customer.

(iii) Legal persons or arrangements that are personal asset-holding vehicles.

(iv) Companies that have nominee shareholders or shares in bearer form.

(v) The ownership structure of a company appears unusual or excessively complex given the nature of the company's business.

(vi) High-net-worth individuals and entities.

(vii) Persons from jurisdictions known for their high crime rates (e.g. drug producing, trafficking, smuggling).

(viii) Businesses/activities identified by the FATF as having higher risk for ML/TF/PF.

(ix) Domestic PEPs.

(x) Persons entrusted with prominent public function by international organisations (PEPFIO).

(xi) Legal arrangements that are complex.

(xii) Any persons who match the 'red flag' criteria of the reporting institution.

(b) Country or geographic risk factors:

(i) Countries identified by credible sources, such as mutual evaluation or published follow-up reports, as having inadequate AML/CFT/CPF systems.

(ii) Countries subject to sanctions, embargos or similar measures issued by international organisations such as the United Nations.

(iii) Countries with significant levels of corruption or other criminal activities.

(iv) Countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(v) Countries identified by the FATF, other FATF-style regional bodies or other international bodies as having higher ML/TF/PF risk.

(c) Transaction or distribution channel risk factors:

(i) Anonymous transactions (which may include cash transactions).

(ii) Non-face-to-face business relationships or transactions.

(iii) Payment received from multiple persons and/or countries that do not fit into the customer's nature of business and risk profile.

(iv) Payment received from unknown or unassociated third parties.

8.2.3 Subject to paragraph 8.5 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.*

## 8.3 Enhanced CDD measures

8.3.1 Where the ML/TF/PF risks are assessed as higher 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 for identification 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.

## 8.4 Politically exposed persons (PEPs)

8.4.1 The requirements set out in paragraph 8.4 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.

8.4.2 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.

8.4.3 Upon determining that a customer or a beneficial owner is a foreign PEP, the requirement to conduct enhanced CDD measures under paragraph 8.3 is applicable and the reporting institution is also required to conduct enhanced ongoing due diligence.

8.4.4 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.

8.4.5 The reporting institution is required to assess the level of ML/TF/PF 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 publicly available information or other reasonable means. The assessment of the ML/TF/PF risks also must take into account the profile of the customer under paragraph 7.5.3 of these Guidelines.

8.4.6 For a higher-risk domestic PEP or higher-risk person entrusted with a prominent function by an international organisation, the requirements of enhanced CDD measures are as set out in paragraph 8.3.

8.4.7 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.

8.4.8 A reporting institution must consider the following factors in determining whether the status of a domestic or foreign PEP who no longer holds a prominent public function should cease:

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

(b) whether the domestic or foreign PEP's previous and current functions, in official capacity or otherwise, are linked to the same substantive matters.

## 8.5 Higher-Risk Countries

8.5.1 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/PF risks emanating from such jurisdictions; or

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

8.5.2 In addition to the enhanced CDD measures required under paragraph 8.5.1 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.

8.5.3 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/CPF 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/CPF 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 8.3 above.

## 8.6 Reliance on third-party institutions to conduct CDD

8.6.1 A reporting institution may rely on a third-party institution to conduct CDD at the point of establishing a business relationship to identify and verify a customer or a beneficial owner. The reporting institution must immediately obtain the necessary information concerning the identification and verification of the customer or the beneficial owner from the third-party institution.

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

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

8.6.4 The relationship between a reporting institution and the third-party institution relied upon by the reporting institution to conduct the CDD, shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. In placing the reliance on the third-party institution, the reporting institution at the minimum:

(a) Must be able to obtain immediately the necessary information concerning the CDD in paragraph 8.1 above;

(b) Must be satisfied that the third-party institution:

(i) has adequate CDD processes;

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

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

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

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

*Guidance for paragraph 8.6.4:*

*A reporting institution may obtain written confirmation from the third-party institution that it has conducted CDD on the customer or the beneficial owner in accordance with paragraph 8.1.*

8.6.5 A reporting institution must obtain an attestation from the third-party institution to satisfy itself that the requirements in paragraph 8.6.4 have been met.

8.6.6 In addition to the requirements set out in paragraph 8.6.4 above, a reporting institution that relies on a third-party institution 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.

8.6.7 Where a reporting institution relies on a third-party institution, the ultimate responsibility and accountability for CDD measures remains with the reporting institution.

8.6.8 A reporting institution shall not rely on a third-party institution to conduct ongoing due diligence of its customers.

## 8.7 Failure to satisfactorily complete CDD

8.7.1 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 reporting institution fails to comply with the CDD requirement.

8.7.2 In addition to the requirement in paragraph 8.7.1, the reporting institution must also consider lodging a STR in relation to such customer with the FIED

## 8.8 Ongoing Due Diligence

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

(a) monitoring, detecting and scrutinizing 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 iskept up-to-date and are relevant, by undertaking periodic reviews of existing records, particularly for higher-risk categories of customer.

8.8.2 The frequency in implementing paragraph 8.8.1(a) under on-going due diligence or enhanced due diligence must commensurate with the level of ML/TF/PF risks posed by the customer based on the risk profiles and nature of transactions.

8.8.3 When conducting enhanced due diligence, reporting institutions must, amongst others, enhance the control measures, increase of the number of monitoring of the relevant customers' accounts, and timing of controls applied.

### *Monitoring of accounts*

8.8.4 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.

8.8.5 A reporting institution should consider reclassifying a customer as higher risk and consider lodging a 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.

8.8.6 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/PF and consider whether to refuse to do any business with such customers.

*Renewed CDD*

8.8.7 A reporting institution is required to undertake a renewed CDD when:

(a) The customer's account has been dormant or inactive and the customer is seekingto reactivate its account or resume its activities;

(b) There is a change in circumstances relating to a customer which give rise to asuspicion of ML/TF/PF risks; or

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

# PART IIIA: WIRE TRANSFER

## 9. WIRE TRANSFER OF DIGITAL ASSETS

### 9.1 General

9.1.1 The requirements under this Part are applicable to a reporting institution providing cross border wire transfer or domestic wire transfer of digital assets.

9.1.2 A reporting institution must not execute wire transfer of digital assets if it does not comply with the requirements specified in this Part IIIA.

9.1.3 In providing wire transfer of a digital asset, the reporting institutions must comply with requirements on targeted financial sanctions:

(a) In relation to terrorism financing under Part VII of these Guidelines; and

(b) In relation to proliferation financing Part VIII of these Guidelines.

9.1.4 A reporting institution must obtain, hold and maintain all originator and beneficiary information collected under this Part IIIA, in accordance with record keeping requirements under Part IV of these Guidelines. This information must be made available to regulators or relevant authorities when necessary.

9.1.5 A reporting institution must have in place adequate policies and procedures and the ability to trace all wire transfers.

### 9.2 Ordering institutions

*Cross-Border or Domestic Wire Transfers*

9.2.1 A reporting institution which is an ordering institution must ensure that the message for cross-border or domestic wire transfer are accompanied by the following:

(a) Required and accurate originator information pertaining to:

(i) Name of originator;

(ii) National registration identity card number or passport number;

(iii) Account number or digital wallet address or a unique transaction reference number used to process the transaction which permits traceability of the transaction; and

(iv) Address or date and place of birth

(b) Required beneficiary information pertaining to:

(i) Name of beneficiary; and

(ii) Account number or digital wallet address or a unique transaction referencenumber used to process the transaction which permits traceability of the transaction.

***Guidance for paragraph 9.2.1 (a)***

1. *Accurate in the context of paragraph 9.2.1(a) means the required originator's information has been verified for accuracy by the ordering institution as part of its KYC process.*

***Guidance for paragraph 9.2.1 (b)***

2. *The name of the beneficiary is not required to be verified for accuracy by the ordering institution. Notwithstanding this, the name of the beneficiary should be reviewed for the purpose of suspicious transaction monitoring and sanction screening.*

9.2.2 A reporting institution which is an ordering institution must submit the information set out in paragraph 9.2.1 to the beneficiary institution immediately and securely.

***Guidance for paragraph 9.2.2:***

a) *The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the digital asset transfers.*

b) *The phrase 'immediately' means that the reporting institutions should submit the required information prior,* ***simultaneously or concurrently*** *with the transfer itself. Post-facto submission of the required information should not be permitted.*

c) *The phrase 'securely' means that the reporting institutions should transmit and store the required information in a secure manner.*

## 9.3 Beneficiary Institutions

9.3.1 A beneficiary institution must take reasonable measures, including post-event or real-time monitoring where feasible, to identify cross border wire transfers or domestic wire transfers that lack the required originator information or required beneficiary information.

9.3.2 A beneficiary institution is required to have effective risk-based policies and procedures for determining—

(a) when to execute, reject, or suspend a wire transfer lacking the required originator orrequired beneficiary information; and

(b) the appropriate follow-up action.

9.3.3 A beneficiary institution must verify the following beneficiary information received from the ordering institution:

(a) Name of beneficiary; and

(b) Account number or digital wallet address or a unique transaction reference number used to process the transaction which permits traceability of the transaction.

## 9.4 Sanctions Screening

9.4.1 An ordering institution must conduct sanctions screening of the following persons:

(a) its customer, at the point of onboarding and ongoing due diligence; and

(b) the beneficiary, when a wire transfer is conducted.

9.4.2 A beneficiary institution must conduct sanctions screening of the following persons:

(a) its beneficiary, at the point of onboarding and ongoing due diligence; and

(b) the originator, when a wire transfer is conducted.

9.4.3 Once the person screened is identified as a designated person, the ordering or beneficiary institution must take freezing actions and prohibit transactions.

9.4.4 Ordering or beneficiary institutions must implement effective control frameworks to ensure that they can comply with their targeted financial sanction obligations.

9.4.5 A reporting institution must document their remediation control actions in their AML/CFT/CPF risk assessment.

*Guidance for paragraph 9.4:*

*As a guide, control measures that could be taken in carrying out sanctions screening requirement include—*

a) *putting a wallet on hold until screening is completed and there is a confirmation that no concern has been raised; and*

b) *arranging to receive a wire-transfer with a provider's wallet that links to a customer's wallet, and only after screening is completed and there is a confirmation that no concern has been raised, the digital asset is then transferred to the customer's wallet.*

## 9.5 Identification and Due Diligence on Counterparty VASP

9.5.1 A reporting institution must identify and conduct due diligence on the counterparty VASP before the reporting institution transmits the required originator or beneficiary information.

**Appendix F** sets out the guide on how due diligence on counterparty VASP could be undertaken.

*Guidance for paragraph 9.5.1:*

- *As a guide, a reporting institution needs to conduct due diligence on their counterparty VASP before the reporting institution transmits the required information to avoid dealing with illicit actors or sanctioned actors unknowingly.*

- *Additionally, a reporting institution should use this due diligence process to determine whether a counterparty VASP can reasonably be expected to protect the confidentiality of information shared with it.*

9.5.2 A reporting institution does not need to undertake due diligence process on the counterparty VASP for every individual wire transfer when dealing with a counterparty VASP for which it has previously conducted counterparty due diligence, unless there is a suspicious transaction history or other information (for example published adverse media information, published regulatory or criminal action involving the counterparty VASP) indicating that it should refresh the due diligence process.

9.5.3 A reporting institution must update its counterparty VASP due diligence information periodically or when risk emerges from the relationship in line with a reporting institution's defined risk-based assessment control structure.

# PART IV: RETENTION OF RECORDS

## 10 RECORD KEEPING

10.1 A reporting institution must keep records 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 and verification of the customer inwhose name the account is opened or transaction is executed;

(b) The identification of the beneficial owner or the person on whose behalf theaccount 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 orterminated.

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 and all relevant transaction 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 and TFS-PF legislations;

(b) it is sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity; 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 must establish in place strong mechanisms for reporting suspicious transactions, including having an appointed AML/CFT/CPF compliance officer, and where appropriate, having a unit primarily responsible for complying with the AML/CFT/CPF requirements on reporting of suspicious transactions.

11.2 A reporting institution must also ensure that the suspicious transaction reporting mechanismis 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 and proliferation financing, such transaction should be reported immediately to the FIED through lodgement of a STR.

11.6A A reporting institution is required to have in place policies on the duration upon which internal suspicious transaction reports must be reviewed by the reporting institution, including the circumstances when the timeframe can be exceeded, where necessary.

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 as and when 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/PF 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/CPF, 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/CPF 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 reporting institution must establish parameters on the circumstances where disclosure is required, 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 part.

# PART VI: ENFORCEMENT ORDERS

## 13 COMPLIANCE WITH ENFORCEMENT ORDERS

13.1 A reporting institution must produce information or document requested by a relevant law enforcement agency, pursuant to any investigation order under the AMLA served on the reporting institution ("enforcement orders"), within a reasonable time frame that has been agreed upon between the investigating officer of the law enforcement agency and the reporting institution.

13.2 A reporting institution must establish policies and procedures and systems to ensure no undue delay in responding to the enforcement orders.

# PART VII: COMBATING TERRORISM FINANCING

## 14 IDENTIFICATION AND DESIGNATION

14.1 For the purposes of this part, a reporting institution refers to reporting institution as defined in the Definition section under Part I of these Guidelines and includes a registered person under section 76 of the CMSA that is registered under the *Guidelines on the Registration of Venture Capital and Private Equity Corporations and Management Corporation*.

14.2 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.

14.3 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" or "listed entities" as the case may be).

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

14.4 For the purpose of implementing the obligations under section 66B and section 66C of the 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.

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

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

14.7 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.

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

# PART VIII: COMBATING PROLIFERATION FINANCING

## 15. DEFINITION AND INTERPRETATION

15.1 For the purpose of Part VIII of these Guidelines, "reporting institution" refers to reporting institution as defined in the Definition section under Part I of these Guidelines and includes a registered person under section 76 of the CMSA that is registered under the *Guidelines on the Registration of Venture Capital and Private Equity Corporations and Management Corporation*.

## 16. MAINTENANCE OF SANCTIONS LIST

16.1 A reporting institution must put in place and implement policies and procedures to:

(a) keep itself updated with the various resolutions passed by the United Nations Security Council on TFS-PF, in particular the list of countries and persons designated under the relevant UNSCR published on the UN website as and when there are new or subsequent decisions by the relevant UNSC Sanctions Committee; and

(b) maintain an updated and current database of names and particulars of designated persons in the UN Consolidated List to enable it to detect suspected proliferators.

16.2 Explanatory notes in relation to maintenance of sanctions list are set out in **Appendix H.**

## 17. CONDUCT SANCTIONS SCREENING ON CUSTOMERS

17.1 A reporting institution must conduct sanctions screening on its existing, new and potential customers, to check for any positive name matched with any designated person.

17.2 A reporting institution must screen its entire customer database without delay when new names are listed in the UNSCR.

17.3 The obligation to conduct sanctions screening on customers also includes funds derived from property owned or controlled directly or indirectly by the designated person or by any of its related party. In this regard, a reporting institution must conduct checks on:

(a) relationship and transactions connected with the designated person;

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

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

17.4 If there is a positive name match, a reporting institution must take reasonable and appropriate measures to verify and confirm the identity of its customer against the designated person.

***Guidance for paragraph 17***

*(a) According to the standards prescribed by the FATF, "without delay" means, ideally within a matter of hours of a designation by the UNSC or its relevant Sanctions Committee. The phrase "without delay" should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to the financing of proliferation of weapons of mass destruction.*

*(b) A reporting institution is also advised to search, examine and analyse past financial activities of the designated person or related party, where relevant.*

*(c) A reporting institution must always be wary of the possible use of among others, false identities, dual nationalities, multiple names and identities when performing name searches for each designated person to prevent unintended omissions.*

*(d) The screening obligations under these Guidelines extend to the delisting of affected customers from the list of countries and persons designated under the relevant UNSCRs.*

## 18. REQUIREMENT TO FREEZE, BLOCK AND REJECT

18.1 Once a customer's identity as a designated person is confirmed, a reporting institution must freeze the customer's funds, properties or accounts or any transaction executed by the customer to prevent the flight or dissipation of the funds, other properties or assets or controlled directly or indirectly by the customer without delay.

18.2 The freezing of funds, properties or accounts shall remain in effect until:

(a) The designated person is delisted by the UNSC; or

(b) It is confirmed that the customer's funds, properties or accounts have been inadvertently affected by virtue of him having a same or similar name with a designated person (false positive).

*Guidance for False Positive under paragraph 18.2(b)*

*(a) A reporting institution may forward queries to the SC to determine whether the customer is a designated person in the case of similar or common names.*

*(b) Any query submitted to the SC must include any additional information, copies of identification documents and relevant analysis conducted by the reporting institution.*

*(c) A reporting institution should advice any customers who complain about their accounts being inadvertently frozen or transactions being erroneously rejected or blocked to contact the Strategic Trade Controller under the STA to verify the false positive match.*

18.3 If circumstances in paragraph 18.2(b) arose, an application may be made by the customer to the Strategic Trade Controller under the Strategic Trade (Unfreezing of Property in relation to Prohibited End-Users) Regulations 2014 *(P.U.(A) 290/2014*) for the unfreezing of such funds, properties and accounts.

18.4 Where the screening assessment results in a match with a potential or new customer, a reporting institution must reject the customer if the transaction has not commenced.

*Guidance for paragraph 18*

*(a) Funds, properties or accounts that are owned or controlled indirectly by the designated person includes situation where the designated person 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.*

*(b) The obligation to freeze funds, properties or accounts of a designated person continues until the person is delisted from the sanction lists. The freezing obligations remains even after the designated person passed away.*

*(c) If an asset is owned or controlled by a designated person and the interest owned or controlled by the designated person cannot be segregated, then the entire asset should be subjected to freezing.*

*(d) 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 designated person continue to be listed.*

*(e) No outgoing payment should be made from the frozen funds, properties or accounts including payment of any fees or service charges for maintaining the frozen fund without prior written authorisation of the Strategic Trade Controller in consultation with the SC.*

## 19. REPORTING REQUIREMENTS

19.1 A reporting institution must immediately report to the SC on any freezing, blocking or rejection actions undertaken in accordance with paragraph 18 towards the identified funds, properties or accounts.

19.2 The form for reporting to the SC upon determination of a name match and actions taken by the reporting institution is attached as **Appendix I**.

19.3 A reporting institution who has reported positive name matches and has control of frozen funds, properties or accounts of a designated person must report to the SC on any change to such frozen funds, properties or accounts by 31 January in the next calendar year (periodic reporting).

> *Guidance for paragraph 19.13*
>
> *Examples of changes to the frozen funds, properties or accounts of customers includes among others, an increase in the funds or value of the property frozen due to interest payments or dividends pay outs.*

19.4 The form for periodic reporting to the SC is set out in **Appendix J**.

19.5 A reporting institution must submit a STR to the FIED in the following circumstances:

(a) In the event of positive name matches arising from ongoing screening of their customer database involving designated person or person identified as related party related to the designated person; and

(b) Where there is an attempted transaction by any of the designated person or its related party.

19.6 The details on the lodgement of STR with FIED are set out in **Appendix C**.

19.7 The contact point for the SC and Strategic Trade Controller in relation to TFS-PF are:

**Securities Commission Malaysia**
Executive Director
Surveillance, Authorisation and Supervision
Securities Commission Malaysia,
3 Persiaran Bukit Kiara,
Bukit Kiara,
50490 Kuala Lumpur
Tel: 03-6204 8000
Website: www.sc.com.my

**Strategic Trade Controller**
Strategic Trade Secretariat,
Ministry of International Trade and Industry,
Level 4, MITI Tower, No. 7, Jalan Sultan Haji Ahmad Shah,
50622 Kuala Lumpur
Tel: 03-8000 8000
E-mail: admin.sts@miti.gov.my
Website: http://www.miti.gov.my/index.php/pages/view/sta2010

**APPENDIX A**

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

## 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/PF risks to which it is exposed to and take the necessary AML/CFT/ CPF control measures to mitigate them.

1.2 This Guidance seeks to:

(a) assist the reporting institution to design and implement AML/CFT/CPF 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/PF 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/PF risks identified; and

(c) facilitates the reporting institution to allocate its resources and internal structures to manage and mitigate the ML/TF/PF 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/PF. By regularly assessing the reporting institution's ML/TF/PF 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/PF risk factors that affect its business and address the impact on the reporting institution's overall ML/TF/PF risks.

I. Perform risk assessment — A reporting institution shall perform an assessment on the degree of ML/TF/PF 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/PF 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/PF risks. These risk control measures should manage and mitigate the ML/TF/PF risks identified as well as be proportionate to the risks recognised.

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

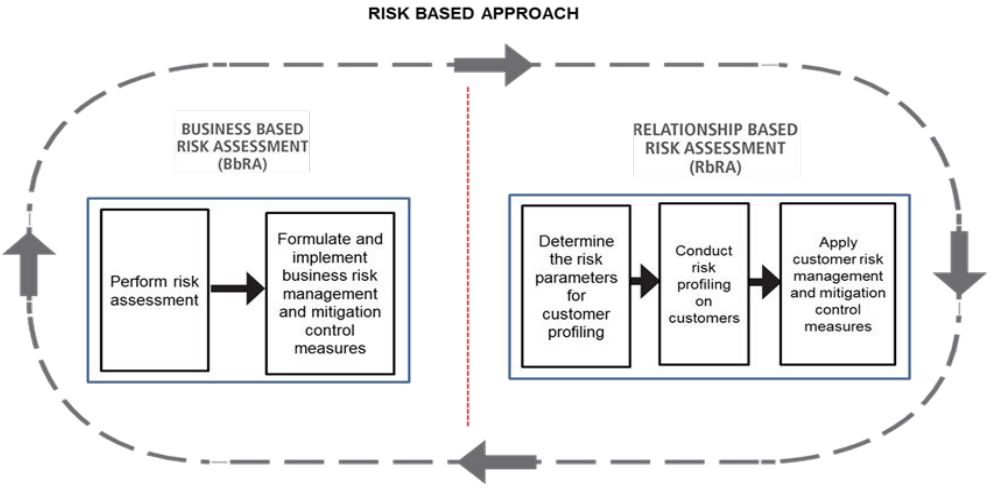
In a RbRA, a reporting institution must consider types of products, services, distribution channels, etc. that the customers are using and mitigate the risks identified.

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/PF 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/PF 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/PF 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/PF 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/PF 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/PF risks at a macro level. When assessing the ML/TF/PF risks, a reporting institution should consider all relevant riskfactors that affect their business and operations:

(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) or any other risk assessment issued by relevant authorities; and
(g) Other specific risk factors that the reporting institution may consider for the purpose of identifying its ML/TF/PF risks.

3.3 The ML/TF/PF 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/PF 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/PF risks posed to the reporting institution.

3.4 To assist a reporting institution in assessing the extent of its ML/TF/PF 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/PF 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 orthe 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/CPF 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/PF risks. In this regard, a reporting institution must consider the appropriate ML/TF/PF 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/PF risks attached to the types of products and services offered. Some of the non-

(e) 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.

(f) Reporting institution's structure – the ML/TF/PF 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/PF 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.

(g) Findings of the NRA or any other risk assessments issued by relevant authorities – in identifying, assessing and understanding the ML/TF/PF 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.

(h) 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 anyfreeze 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/PF 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/PF risks | • Number of customerswith 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/PF 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 onthe proposed risk management and mitigation procedures, systems and controls adoptedby 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.

3.9 Once the reporting institution has identified and assessed the ML/TF/PF 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.

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

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

4.2 The type and extent of the AML/CFT/CPF 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).

4.3 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 A: 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 orservice and transaction or distribution channel. These risk parameters will assist the reporting institution in identifying the ML/TF/PF 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/PF 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, except for circumstances where a high-risk indicator is identified pursuant to high-risk customer relationships prescribed by FATF standards[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 whetherto apply standard or enhanced CDD measures in respect of each customer.

[1] The high-risk customer relationships that have already been prescribed by FATF standards are for 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 customersrated 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 customerhas commenced transactions. Ongoing monitoring determines whether the transactionsare 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/ PF 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/PF 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/PF 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 orreview 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 A 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/PF risks and conclusions of the ML/TF/PF 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 ithas waived) compared to the standard CDD approach.

**APPENDIX A1**

## Control Measures in Accepting Third-Party Deposits

(in relation to **paragraph 7.6** of these Guidelines)

## 1.0 General

1.1 This Appendix sets out requirements on control measures to mitigate ML/TF/PF risk when a reporting institution accepts third-party deposits. For avoidance of doubt, third-party deposits refer to monies deposited by a third-party into the customer's account with a reporting institution.

1.2 A reporting institution which is unable to exercise adequate control measures to mitigate the inherent ML/TF/PF risk and other associated risks and meet the relevant compliance requirements must not accept any third-party deposits.

## 2.0 Policies and procedures

2.1 A reporting institution which accepts third-party deposits must establish and implement a clear, comprehensive and effective policies and procedures to monitor third-party deposits and have control measures to be carried out before accepting third-party deposits to mitigate ML/TF/PF risk and other associated risks.

2.2 A reporting institution is required to comply with the requirements of paragraph 7.6 of these Guidelines in establishing and implementing third-party deposits policies and procedures.

2.3 A reporting institutions' policies and procedures on third-party deposits must cover the following:

(a) circumstances where the third-party deposits can be allowed having regard to thereporting institution's risk assessment;
(b) an effective monitoring systems and controls to identify and accept third-party deposits, including:
    (i) undertake due-diligence and evaluation on third-party deposits; and
    (ii) on-going monitoring of third-party deposits.
(c) Other relevant requirements on record keeping and employee training.

**Circumstances where third-party deposits can be allowed**

2.4 Pursuant to the reporting institutions' risk assessment and findings, a reporting institution may accept arrangement for third-party deposits under controlled and legitimate circumstances having regard to due diligence and evaluation on the third-party.

**Monitoring systems and controls to identify and accept third-party deposits**

2.5 A reporting institution must ensure an effective monitoring systems and controls to identify and accept third-party deposits into their customer's account, including to obtain supporting documents from customers to ascertain whether deposits into the customer's accounts comes from a third-party.

**Due diligence and evaluation**

2.6 On a risk-based approach, a reporting institution must conduct a due-diligence on third-party deposits to determine the following:

(a) The identity of the third-party payor, including national registration identity card number or passport number, residential address and contact number;
(b) The relationship between the customer and the third-party payor;
(c) The reason for making deposits into the customer account; and
(d) Whether the third-party exercises trading authority over the customer's account.

2.7 A reporting institution must evaluate the reasons and the need for third-party deposits to ensure that a third-party deposit is reasonably in line with the customer's profile and normal commercial practices (including the frequency and pattern of previous third-party deposits).The evaluations and assessments must include:

(a) Conducting further inquiries with the customers; and
(b) Obtaining corroborative evidence from relevant sources;

2.8 Where a reporting institution reject a third-party deposits, the reporting institution must ensure that the monies are returned to the sources of their deposits as soon as practicable.

**On-going monitoring**

2.9 A reporting institution must implement an on-going monitoring of customers' accounts involving third-party deposits. A suspicious transaction report should be made immediately to the FIED when there are grounds for suspicion of ML/TF/PF.

2.10 A reporting institution must 'flag' accounts with suspicious transactions relating to third-party deposits for monitoring purposes.

**Record keeping, employee training on third-party deposits and communication to customers**

2.11 A reporting institution must keep records of all documents and the findings of inquiries made together with the corroborative evidence obtained during the due diligence evaluation and approval of a third-party deposit.

2.12 A reporting institution must provide relevant training and guidance to the employee responsible for the implementation of the reporting institution's policies and procedures inrelation to third-party deposits.

**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 associatesof 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 or 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 family members or close associates of a domestic PEP or PEPFIO that is assessed as low risk pursuant to the rating assigned to the domestic PEP or PEPFIO, the reporting institution must apply the standard CDD measures and where he is assessed as higher 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 inits 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 individualswho 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 PE P 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:<br><br>Director<br>Financial Intelligence and Enforcement Department<br>Bank Negara Malaysia<br>Jalan Dato' Onn<br>50480 Kuala Lumpur |
| Fax | 03-2693 3625 |
| E-mail | str@bnm.gov.my |
| Others (where and if available) | FIED's Financial Intelligence System (FINS)<br>FINS 2.0 (bnm.gov.my) |

**APPENDIX D**

# Guidance on the Implementation of Targeted Financial Sanction in Relation toTerrorism 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 TFS-TF. The UNSCR relating to terrorismfinancing 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-TF, 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)<br><br>(Individuals and entities associated with Al-Qaida)<br><br>• UNSCR 1988 (2011) and other subsequent resolutions<br><br>(Individuals and entities associated with Taliban)<br><br>• UNSCR 2253 (2015) and other subsequent resolutions<br><br>(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);<br><br>• Anti-Money Laundering and Anti-Terrorism Financing (Security Council Resolution) (Al-Qaida and Taliban) (Amendment) Order 2013 (P.U.(A) 187/2013);<br><br>• Anti-Money Laundering and Anti-Terrorism Financing (Security Council Resolutions) (Al-Qaida and Taliban) (Amendment) Order 2014 (P.U. (A) 255/2014); and<br><br>• 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);<br><br>• Anti-Money Laundering and Anti-Terrorism Financing (Declaration of Specified Entities and Reporting Requirements) (Amendment) Order 2014 (P.U.(A) 301/2014); and<br><br>• 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 uponthe 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 ownedor 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<br>• Section 66E of AMLA<br>• 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: Membanteras Pembiayaan Keganasan (moha.gov.my)

**APPENDIX E**

## Guidance on Beneficial Ownership for Legal Persons and Legal Arrangement

(in relation to **paragraphs 8.1.8 to 8.1.17** of these Guidelines)

### Introduction

1.1 The obligations of a reporting institution on beneficial ownership requirements are:

(a) identifying a natural person who is the beneficial owner of the customer and obtaininginformation that describes the ownership, control and structure of the legal persons/ legal arrangements relating to the beneficial owner;
(b) taking reasonable measures to verify the accuracy of the information obtained and keeping records of all relevant documents;
(c) conducting customer risk profiling to identify the risk category of the beneficial owner;and
(d) performing further regulatory obligations based on the risk category of the beneficial owner such as CDD, sanction screening and high-risk jurisdiction.

1.2 The purpose of this Appendix is to set out guidance and recommended best practices to guide a reporting institution in complying with the relevant requirements in relation to identification of beneficial owners of legal persons and legal arrangement.

### Identification

1.3 Beneficial owner is defined as a natural person:

(a) who ultimately owns a customer;

(b) who ultimately controls a customer;

(c) on whose behalf a transaction is being conducted; and/or

(d) who exercises ultimate effective control over a legal person or arrangement.

1.4 To determine the identity of beneficial owners of a customer, reporting institutions should seek to understand the complexities of the customer's ownership structure, governance and/or arrangement at each layer. An entity may have several beneficial owners, depending on its size and the complexity of its structure and governance.

1.5 There may be more than one beneficial owner associated with a customer. Reporting institutions' regulatory obligations relating to beneficial ownership are applicable on all thebeneficial owners.

1.6 Issues concerning beneficial owners having ultimate ownership and exercising and/or having ultimate control are relevant to the following types of customers:

*Legal persons*

(a) Private and public companies;

(b) Bodies corporates;

(c) Government-linked companies;

(d) Partnerships;

(e) Foundations;

(f) Co-operatives;

(g) Associations such as clubs and societies; and

(h) Non-governmental organisations such as charities.

*Legal arrangements*

(a) Trust bodies/arrangement or other similar arrangements

**Steps to identify beneficial owner**

*Legal person*

1.7 A reporting institution should identify the beneficial owners of legal persons through the **cascading steps** reflected below. In applying the cascading step, the subsequent step would apply only in circumstances where no natural person is identified as beneficial owner under the preceding step. For example, Step 3 would only apply where no natural person is identified as beneficial owner under Step 1 and Step 2.

## 1.8 Step 1: Identify the natural person(s), if any, who ultimately have controlling ownership interest in the legal person

(a) Having ultimate controlling ownership interest over an entity includes having more than 25% ownership or equity interest in an entity which may be observed, among others, through share capital, capital contribution or voting rights. The ownership may either be direct ownership (through ownership of shares within the entity itself) or indirect ownership (through chain of corporate vehicles). In the case of a limited liability partnership - partners with capital contribution and/or voting rights of more than 25%.

(b) Having a golden share within an entity is similar to having ultimate ownership of the entity, as it refers to 51% ownership.

(c) Shareholders may exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity. In most circumstances, ownership over an entity implies control over the entity, as ownership may come with the power and authority to take actions and make decisions for the entity. Such a situation can be observed, among others, where:

(i) The natural person has majority voting power within the entity to make decisions; or
(ii) The natural person exercises his right to appoint or remove directors or senior management, as a major shareholder.

(d) In implementing Step 1, a natural person identified as fulfilling the criteria in (a) shall be identified as the beneficial owner. However, where there is doubt that the person identified under Step 1 is not the beneficial owner; or where no natural person has ultimate controlling ownership interest over thelegal person, the reporting institution shall carry out Step 2.

## 1.9 Step 2: Identify the natural person, if any, exercising control of the legal person, through other means

(a) A natural person may also exercise effective control over an entity if he has the powers and authority to take actions and make decisions for the entity, including on matters relating to its financial affairs, financial relationships, operations or othermatters that may fundamentally affect the business or direction of the entity, without having ownership interest over the entity.

(b) Such powers and authority may be attained through other means, such as:

(i) Reflecting dominant influence to appoint or remove directors/ senior management;
(ii) Having the power of attorney over the entity;
(iii) Owning stocks or rights over outstanding debts that are convertible into voting equity;
(iv) Participating in the financing of the enterprise; or
(v) Having control through trusts, agreements, arrangements, understandings, policies or practices, close and intimate family relationships or if a company defaults on certain payments.

(c) A natural person demonstrating control may be, among others, the entity's senior management, directors, authorised signatory, controller and etc.

| |
|---|
| Where, in the course of identifying beneficial owners, reporting institutions identified natural persons who exert control over an entity but have no direct ownership or apparent control over the entity, this assessment along with the person suspected of being a beneficial owner, should be recorded. Such a situation may be observed through:<br>(i) personal connections to persons in positions of power within the entity or persons who possess ownership over an entity (close or intimate family relationships and historical or contractual associations)<br>(ii) participation in financing of enterprises which may allow enjoyment or benefits from assets of the legal person |

**1.10 Step 3: Identify the identity of natural persons holding the position of senior management within the legal person**

For the purpose of paragraph 1.9, "senior management" are identified as persons who exercise executive control over the daily or regular affairs of the legal person, which may include, but are not limited to, directors, deputy directors, Board members, chief executive officer, chief financial officer, chief operating officer, or any other individual performing similar management functions.

**Methods to identify beneficial owners**

1.11 A reporting institution may seek to review the beneficial ownership information relating to an entity, based on the following recommended source documents to determine the ownership structure and governance of an entity. The following list is non-exhaustive and reporting institutions are encouraged to explore other possible sources of documents to review such information.

| Type of legal person/ legal arrangement | Information relating to beneficial ownership | Source documents |
|---|---|---|
| Private and public companies/ Bodies corporate/ Partnership/ | Legal vehicle (e.g. corporate, partnership etc) | • Certificate of incorporation<br>• Certificate of registration<br>• Company constitution<br>• Minutes of Board meeting |
| Government linked companies (GLC) | • Shareholding including information on parent company and subsidiaries information<br>• Direct or indirect ownership<br>• Relationship to conglomerates/ corporate groups<br>• Company tree | • Director's and shareholder's resolution<br>• Partnership agreement<br>• Appointment/ Authorisation letter<br>• Senior management list<br>• Company's annual report and annual return<br>• Joint venture agreement, shareholder's agreements and other related agreements<br>• Director nomination agreement<br>• Register of member including beneficial owner<br>• Any other source documents that sufficiently identifies the beneficial owner |
| Trust arrangement | • Parties to the trust<br>• Persons involved in the trust establishment | • Trust deed<br>• Trust registration document |

| Type of legal person/ legal arrangement | Information relating to beneficial ownership | Source documents |
|---|---|---|
| | • Administrator of the trust<br>• Type of trust | |
| Cooperatives | • Management of the cooperatives<br>• Rules governing the cooperatives | • Registration form of the Cooperatives<br>• By-laws of the cooperative<br>• Minutes of General Meeting |
| Clubs/ Societies/ Foundations/ Charities/ NGOs | • Rules governing the clubs/ societies/ foundations/ charities/ NGO | • Constitution/ charter/ rules<br>• Registration form<br>• Minutes of meeting<br>• List of members of committee |

1.12 Depending on the type of legal person or legal arrangement, identity of beneficial owners may be determined based on the following relationships.

| Type of legal person/legal arrangement | Relationships to be determined, if any |
|---|---|
| Companies (private and public) | • Shareholders<br>• Senior management<br>• Joint venture agreement<br>• Persons with voting rights<br>• Nominee directors/shadow directors<br>• Persons with power to appoint or remove directors<br>• Other persons with interest within the company |
| Partnership | • Partners within the partnership<br>• Other natural persons with effective control over the partnership |
| Government linked companies, state-owned enterprises etc | • Persons authorised in the government to exercise or influence decision making on the GLC<br>• Other persons who exercise or influence decisions over the GLC |

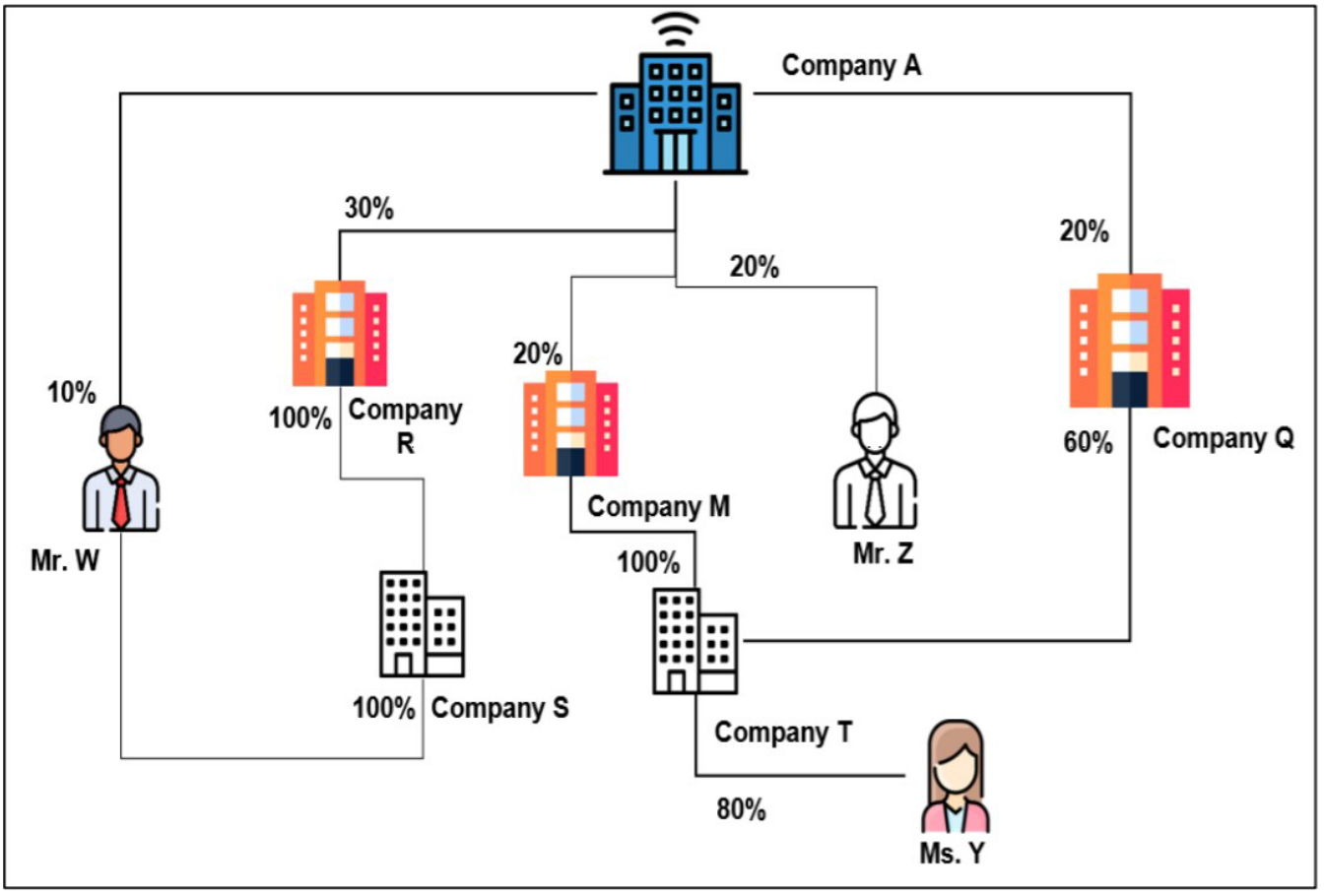
| | |
|---|---|
| Clubs/societies/foundations/charities /NGOs/cooperatives | • Office bearer (e.g. president, secretary, treasurer or other committee)<br>• Senior management/management team |

| Type of legal person/legal arrangement | Relationships to be determined, if any |
|---|---|
| | • Other member with effective control over the club/societies/charities/foundations/ cooperatives |
| Trust arrangement | • Settlor<br>• Trustee<br>• Protector<br>• Beneficiaries or class of beneficiaries<br>• Other natural persons with effective control over the trust |

**Record-keeping of beneficial ownership**

1.13 A reporting institution shall obtain and retain records of beneficial owner information inaccordance with the requirements of the Guidelines.

**Examples of Identification of Beneficial Owners**
**Illustration 1**




From the offset, there is no direct ownership by a natural person of more than 25% of Company A'sshareholding.

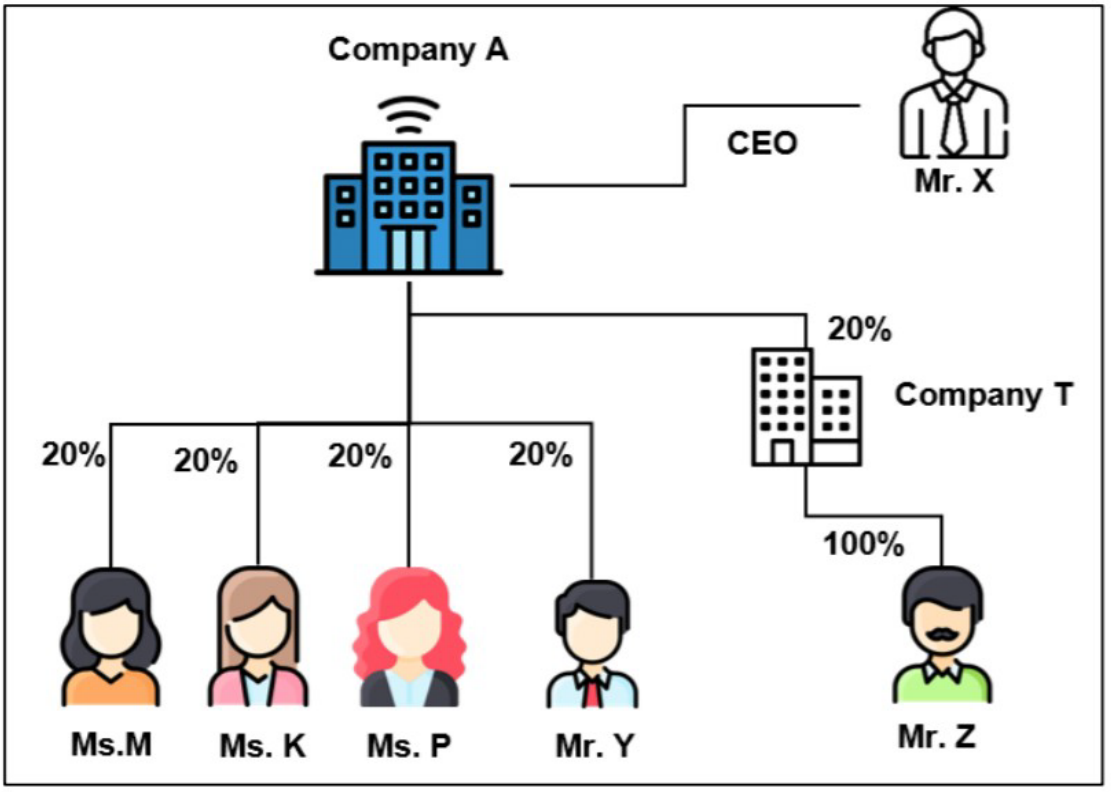
The beneficial ownership breakdown once the complex structure is reviewed is as follows:

A) **Mr. W has 40% ownership of Company A and is a beneficial owner**
(10% direct ownership + 30% indirect ownership through Company R and Company)

B) **Mr Z has only 20% ownership of Company A and is not a beneficial owner**

C) **Ms. Y has 25.6% ownership of Company A and is a beneficial owner**
(9.6% indirect ownership through Company T and Company Q and 16% indirect ownershipthrough Company T and Company M)

**Illustration 2**




Based on the shareholding, there is neither a beneficial owner with 25% or more shareholding nor is there any person with effective control over the company apart from the senior management.

In this case, the senior management with control of decisions over Company A is Mr. X. Mr. X is considered the beneficial owner for AML/CFT requirements purposes.

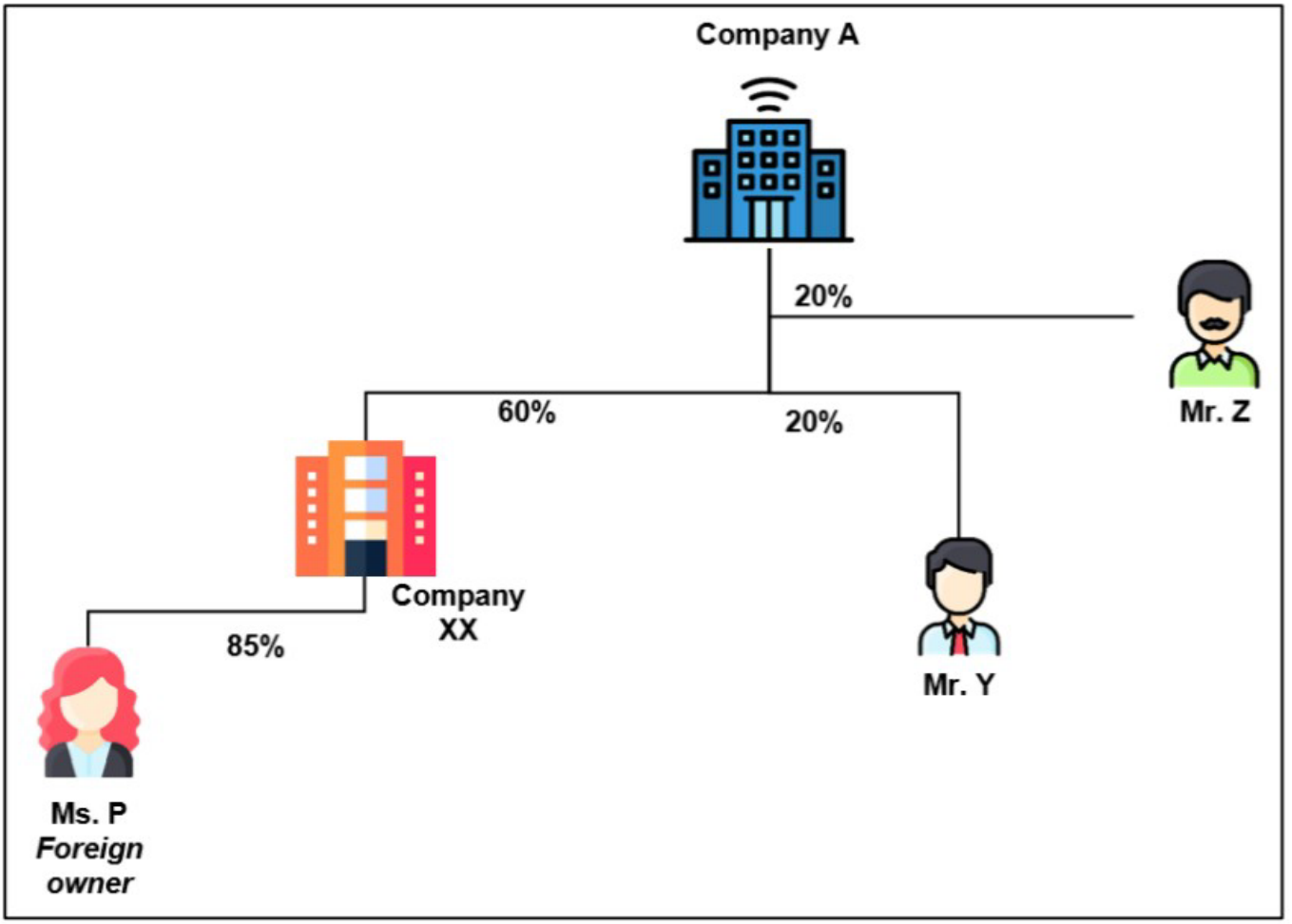
Where there is any doubt on other persons having effective control, reporting institutions may take the effort to explore nature of relationship between shareholders (i.e. spousal, familial relationship, power of attorney relationship).

For example, based on the above shareholding, if Ms. M is the daughter of Mr. Z, Mr. Z may have effective control over Company A even though there is no control through shareholding and may be deemed the beneficial owner.

Similarly, if Mr. Y allows Mr. Z the power of attorney over his shareholding, Mr. Z may also have effective control over Company A and may be deemed the beneficial owner.

The relationships between the relevant stakeholders can be determined and established if the reporting institution truly knows its customer, as required through customer due diligence requirement. Reporting institutions may practise best efforts basis in ensuring these information are discovered.

**Illustration 3**

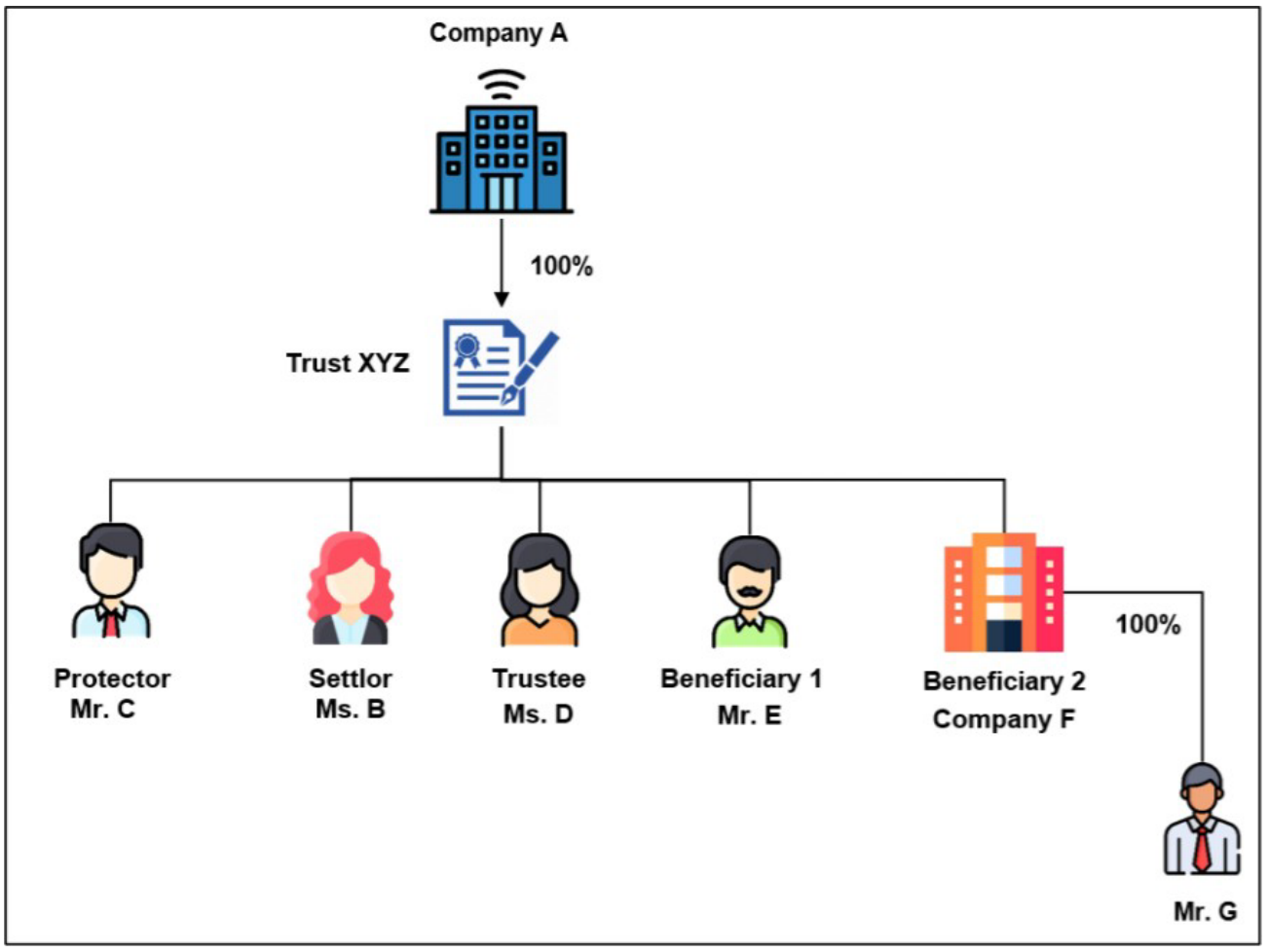



Based on the shareholding, Ms. P is the beneficial owner of Company A, through her ownership of Company XX. The reporting institution having a banking relationship with Company A has endeavoured to obtain all necessary identification documents from Company A relating to Company XX and Ms. P. In verifying those information, the reporting institution has explored all online and offline platforms with publicly available information on Ms. P such as news outlet and websites with company profiles such as Reuters, Asian Nikkei Review etc., reflecting that verification has been conducted on a best effortsbasis.

As Ms. P is a foreign beneficial owner, the reporting institution should also determine whether she is a citizen from high risk jurisdiction or whether she falls within the sanctions list. If Ms. P falls under the category of high risk customers requiring enhanced CDD, the reporting institution should also determine, among others, the sources of funds and wealth of Ms. P.

The reporting institution has the option to choose not to establish or continue business relationship with the customer if it is deemed that Ms. P is not within the reporting institution's risk appetite or if the reporting institution believe it does not have the capacity to appropriately manage the increased risk in relation to the customer/ Ms. P, in accordance with the institution's business decision.

**Illustration 4**




Trust XYZ has 100% ownership of Company A, with the trustee Ms. D holding the shares as the titled legal owner. In such scenario, the beneficial owner of Company A is not Trust XYZ, but rather the individuals that are parties to the trust (e.g. the settlor, protector, trustee and beneficiary) and any other person exercising effective control of the trust.

As one of the beneficiaries of Trust XYZ is not a natural person, i.e. Company F, the beneficial owners of Company F shall also be identified. As such, the beneficial owners in this case for Company A are Ms B, Mr. C, Ms. D, Mr. E and Mr. G.

**Source for images and explanations labelled as Illustration 1-4:**

Guidance on Beneficial Ownership, *Bank Negara Malaysia*, published 1 September 2020, <http://amlcft.bnm.gov.my/document/DNFBP/faq/04.Guidance_on_BO_01092020.pdf>.

**APPENDIX F**

## Guidance on Identification and Due Diligence on Counterparty Virtual Asset Service Provider (VASP) (in relation to **Paragraph 9.5** of the Guidelines)

### 1.0 Introduction

1.1 This Guidance seeks to outline the recommended process involved in conducting identification and counterparty due diligence on counterparty VASP. In the event a reporting institution has developed and adopted its own process, the adopted process must be able to achieve the outcomes intended under this Guidance.

1.2 There are three phases in conducting identification and due diligence on counterparty VASP:

(a) **Phase 1**

(i) A reporting institution should determine whether it will be transacting with another counterparty VASP.

(b) **Phase 2**

(i) A reporting institution should identify the counterparty VASP. In this context, it is possible that the reporting institution only knows the "name" of the counterparty VASP following its previous transaction with the counterparty VASP.

(ii) A reporting institution may identify a counterparty VASP by itself using a reliable database (for example the website of the supervisory authority of the counterparty VASPs), in line with any guidelines from a country on when to rely on such data; and

(c) **Phase 3**

(i) A reporting institution should assess whether the counterparty VASP is an eligible counterparty for it to send customer data to and to have a business relationship.

(ii) A reporting institution should be able to demonstrate its risk-based analysis from an AML/CFT/CPF perspectives, as well as considering other compliance issues, including data storage and security, and the profitability of the business relationship, which forms the basis of its decision to transact with the counterparty VASP.

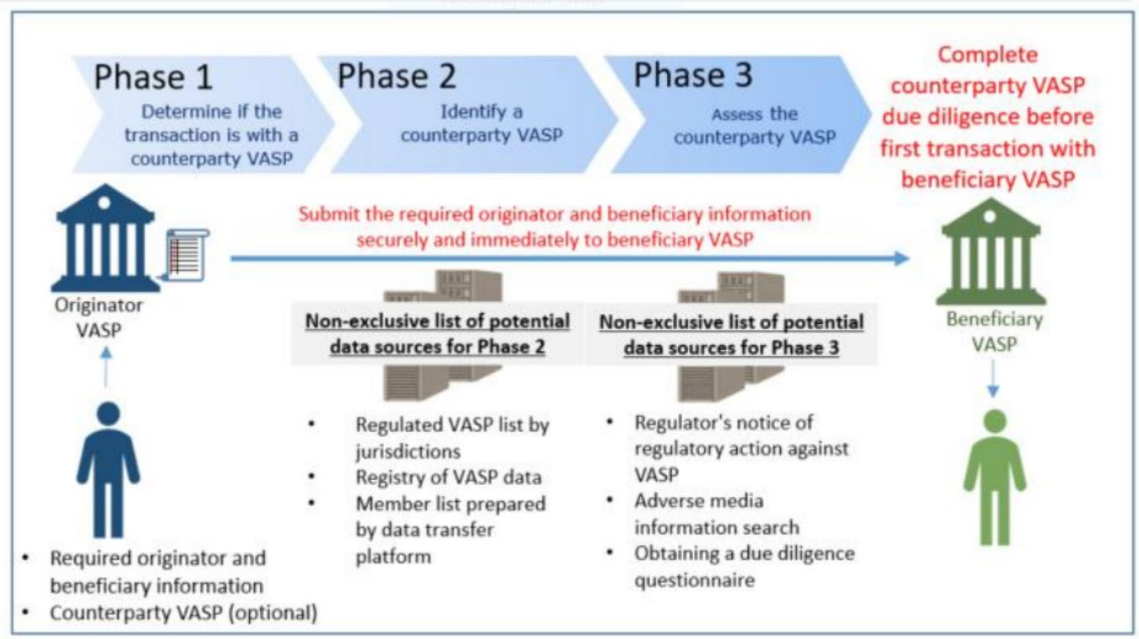
(iii) The due diligence results on the counterparty VASPs must be reviewed

periodically.

(iv) Where a regulated originating institution decide to have a business relationship with an unregulated beneficiary institution, the regulated originating institution may require travel rule compliance from the unregulated beneficiary institutions by way of a contract.

An overview of the due diligence process is set out in **Illustration 1** below.

**Illustration 1:**




**For full FATF Guidance and Source for Illustration 1:**
**Updated Guidance for Risk-Based Approach - Virtual Assets and Virtual Asset Service Providers,** *Financial Action Task Force*, published October 2021, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

**APPENDIX G**

**REGULATION 3 OF STRATEGIC TRADE (UNITED NATIONS SECURITY COUNCIL RESOLUTIONS) REGULATIONS 2010** *(P.U. (A) 481/2010)*
(in relation to **Paragraph 1.1 (b)(ii)** of the Guidelines)

**Regulation 3 of the Strategic Trade (United Nations Security Council Resolutions) Regulations 2010** *(P.U. (A) 481/2010)* requires the following counter-proliferation financing measures to be taken in relation to the countries and persons designated under the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 *(P.U. (A) 484/2010)* in accordance with the relevant UNSCRs:

(a) Freezing of the funds and other financial assets or economic resources of such countries or persons that are located in Malaysia;

(b) Prohibition of investment in Malaysia by such countries or persons involving any restricted activities[3];

(c) Prevention of the provision of financial services, including insurance or re-insurance, or the transfer to, through, or from Malaysia, or to or by Malaysian nationals or entities organised under Malaysian law (including branches abroad), or persons or financial institutions in Malaysia, of any financial or other assets or resources if there is information that provides reasonable grounds to believe that such services, assets or resources could contribute to any restricted activity in any designated country;

(d) Prohibition of such other activities as may be required under the relevant decision of the UNSC.

[3] "Restricted activity" is defined under section 2 of the STA to mean:
a) Any activity that supports the development, production, handling, usage, maintenance, storage, inventory or proliferation of any weapon of mass destruction and its delivery systems; or
b) Participation in transactions with persons engaged in such activities;

**APPENDIX H**

## EXPLANATORY NOTES IN RELATION TO MAINTENANCE OF SANCTIONS LIST

(in relation to **Paragraph 16.2** of the Guidelines)

1. The sanction lists are available in the respective UNSCR sanctions webpage (e.g. 1718 for DPRK), under the heading of 'Sanction List Materials' including:

   (a) DPRK: United Nations Security Council Committee established pursuant to Resolution 1718 (2006); and

   (b) Any other UNSCR as specified by the SC in these Guidelines.

2. The updated UN Consolidated List can be obtained at http://www.un.org/ or https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

3. A capital market intermediary must take note that Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 *(P.U. (A) 484/2010)* 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 capital market intermediary is advised to update its database regularly, without delay.

4. A capital market intermediary may consider subscribing to electronic subscription services to maintain the updated UNSCRs.

5. The delisting of any designated country or designated person under UNSCRs shall automatically take effect when the designated country or person is removed by the relevant UNSC Sanctions Committee.

**APPENDIX I**

**MEASURES PURSUANT TO THE STRATEGIC TRADE (UNITED NATIONS SECURITY COUNCIL RESOLUTIONS) REGULATIONS 2010***([P.U. (A) 481/2010)*

**REPORTING UPON DETERMINATION**

**UNSCR Number (If Available) :**
**Date of UN Listing :**

**Match with Designated Person(s) (YES / NO) :**
*If YES, please fill-up the details in the form below*

| No | UNSCR Permanent Ref No | Customer Name | Address | NRIC / Passport No. | Intermediary Name - if reporting done on group basis | Branch maintaining the account/ facility | Account No. | Account Facility/ Type | Date services given (DD/MM /YYYY) | Account/ Facility Status (on date of freezing) | Date account frozen (DD/MM /YYYY) | Account Balance as at: _____ | Related Parties | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | | | | | | | | | | | | | | |
| **2** | | | | | | | | | | | | | | |
| **3** | | | | | | | | | | | | | | |
| **4** | | | | | | | | | | | | | | |
| **5** | | | | | | | | | | | | | | |

**Details of Capital Market Intermediary**

Name of Capital Market Intermediary :
Contact Person :
Designation :
Tel & Fax No. :
Email :
Reporting Date :

**APPENDIX J**

## MEASURES PURSUANT TO THE STRATEGIC TRADE (UNITED NATIONS SECURITY COUNCIL RESOLUTIONS) REGULATIONS 2010 (P.U. (A) 481/2010)

### PERIODIC REPORTING ON ANY CHANGES TO THE FROZEN OR BLOCKED FUNDS, PROPERTIES OR ACCOUNTS

*(By 31 January of the following calendar year after first reporting on positive name match)*

| Customer No | UNSCR Permanent Ref No (e.g. KPi.001, IRi.001) | Customer Name | NRIC / Passport No. | Account No. | Account Facility/ Type | Date account frozen (DD/MM/YYYY) | Account/ Facility Status | Previous Account Balance (previous reporting) | Transaction Details (line by line transaction) | | | | | New Account Balance as at: (DD/MM/YYYY) | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Transaction No | Date (DD/MM/YYYY) | Transaction Type (for e.g. purchases, sales, redemptions, injections / deposits, withdrawals) | Remarks | Amount (MYR) | | |
| **1.** | | | | | | | | | 1. | | | | | | |
| | | | | | | | | | 2. | | | | | | |
| | | | | | | | | | 3. | | | | | | |
| **2.** | | | | | | | | | 1. | | | | | | |
| **3.** | | | | | | | | | 1. | | | | | | |

**Note:** Please provide supporting documents, i.e. copies of invoices and receipts for each transaction.

**Details of Capital Market Intermediary**

Name of Capital Market Intermediary :
Contact Person :
Designation :
Tel & Fax No. :
Email :
Reporting Date :