



**BANK NEGARA MALAYSIA**  
CENTRAL BANK OF MALAYSIA

**Anti-Money Laundering,  
Countering Financing of Terrorism,  
Countering Proliferation Financing and  
Targeted Financial Sanctions for  
*Designated Non-Financial Businesses and  
Professions (DNFBPs) and Non-Bank  
Financial Institutions (NBFIs)*  
*(AML/CFT/CPF and TFS for  
DNFBPs and NBFIs)***

## TABLE OF CONTENTS

<b>PART A</b>	<b>OVERVIEW .....</b>	<b>1</b>
1	Introduction .....	1
2	Objective .....	2
3	Applicability .....	2
4	Legal Provisions .....	5
5	Effective Date .....	5
6	Definition and Interpretation .....	6
7	Related Legal Instruments and Policy Documents .....	15
8	Policy Documents Superseded .....	15
9	Non-Compliance .....	15
<b>PART B</b>	<b>AML/CFT/CPF/TFS REQUIREMENTS .....</b>	<b>16</b>
10	Application of Risk-Based Approach.....	16
11	AML/CFT/CPF Compliance Programme.....	21
12	New Products and Business Practices .....	32
13	Applicability to Financial/DNFBP Group, Foreign Branches and Subsidiaries and Other DNFBP Structures.....	33
14	Customer Due Diligence (CDD).....	35
14A	Customer Due Diligence: Licensed Casino.....	45
14B	Customer Due Diligence: Licensed Gaming Outlets.....	47
14C	Customer Due Diligence: Accountants, Company Secretaries and Lawyers .....	48
14D	Customer Due Diligence: Trust Companies.....	49
14E	Customer Due Diligence: Dealers in Precious Metals or Precious Stones .....	50
14F	Customer Due Diligence: Registered Estate Agents.....	51
14G	Customer Due Diligence: Moneylenders.....	52
14H	Customer Due Diligence: Pawnbrokers .....	53
15	Politically Exposed Persons (PEPs).....	54
16	Reliance on Third Parties.....	57
17	Higher Risk Countries .....	59
18	Cash Threshold Report.....	60
19	Suspicious Transaction Report.....	62

20	Disclosure of Suspicious Transaction Reports, Cash Threshold Reports and Related Information .....	65
21	Record Keeping .....	66
22	Management Information System .....	67
23	Targeted Financial Sanctions on Terrorism Financing .....	68
24	Targeted Financial Sanctions on Proliferation Financing and Other UN-Sanctions Regimes .....	74
25	Other Reporting Obligations .....	80

## **PART C GLOSSARY, TEMPLATES AND FORMS..... 81**

APPENDIX 1	Glossary .....	82
APPENDIX 2	Definition of Small-sized Reporting Institutions.....	83
APPENDIX 3	Customer Due Diligence Form.....	84
APPENDIX 4	Required Information in CTR .....	91
APPENDIX 5A	Targeted Financial Sanctions Reporting (NBFIs) – Upon Determination .....	93
APPENDIX 5B	Targeted Financial Sanctions Reporting (DNFBPs) – Upon Determination .....	94
APPENDIX 6A	Targeted Financial Sanctions Reporting (NBFIs) – Periodic Reporting on Positive Name Match .....	95
APPENDIX 6B	Targeted Financial Sanctions Reporting (DNFBPs) – Periodic Reporting on Positive Name Match .....	96

## **PART D GUIDANCE..... 97**

APPENDIX 7	Guidance on Application of Risk-Based Approach .....	98
APPENDIX 8	Institutional Risk Assessment Template .....	113
APPENDIX 9	Infographic on Risk Based Approach.....	119
APPENDIX 10	Infographic on Compliance Officer’s Role and Responsibilities	121
APPENDIX 11	Infographic on Customer Due Diligence .....	122
APPENDIX 12	Infographic on Suspicious Transaction Reports .....	126
APPENDIX 13	Infographic on Targeted Financial Sanctions.....	128

## **PART E RED FLAGS ..... 131**

APPENDIX 14	Examples of Red Flags.....	132
-------------	----------------------------	-----

## PART A OVERVIEW

### 1 Introduction

#### *Background*

- 1.1 Money laundering and terrorism financing (ML/TF) are financial crimes with far-reaching and deleterious socio-economic effects. Criminal networks, money launderers and terrorist financiers are highly adaptive and quick to exploit any weak links within an increasingly borderless world to obscure detection of such illicit funds. The globalisation and advancement in technology, including the emergence of new players and innovative products, pose challenges to regulators and law enforcement agencies alike in curbing criminal activities.
- 1.2 In line with the international standards established by the Financial Action Task Force (FATF)<sup>1</sup>, the anti-money laundering, countering financing of terrorism, countering proliferation financing (AML/CFT/CPF) reporting obligations imposed on reporting institutions are risk-informed, and subject to periodic review in tandem with any material changes to the international standards or the evolving risk of ML/TF and proliferation financing (PF) situation in Malaysia. In view of potential development opportunities brought about by the era of digitalisation, enhancements to the existing AML/CFT/CPF reporting obligations are important to ensure areas of higher risk are subject to enhanced controls, while areas of low risk are accorded some policy accommodation, to ensure that the integrity of the financial system is preserved, just as development objectives are facilitated.
- 1.3 Consistent with the FATF's action to strengthen the response to the growing threat of weapons of mass destruction (WMD) PF, reporting institutions are required to assess PF risks and implement commensurate mitigation measures. This aims to ensure that reporting institutions are not subject to abuse, unwittingly support or become part of the PF networks, given the emerging trends on PF risks and techniques adopted by the designated individuals and entities to evade targeted financial sanctions on PF.

---

<sup>1</sup> The Financial Action Taskforce (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering (ML), terrorism financing (TF) and financing of proliferation of weapons of mass destruction (PF). The FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations), issued in February 2012, and updated from time to time, sets out a comprehensive and consistent framework of measures which countries should adapt to their particular circumstances, and implement to ensure the robustness of their respective jurisdiction's AML/CFT/CPF regime. Malaysia was accepted as a FATF member in February 2016. For further information on FATF, please visit their website at [www.fatf-gafi.org](http://www.fatf-gafi.org)

- 1.4 Domestically, the National Risk Assessment (NRA) by the National Coordination Committee to Counter Money Laundering (NCC) that 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.
- 1.5 In line with the United Nations Security Council Resolutions (UNSCR), reporting institutions are also required to adhere to, and implement sanctions imposed on designated countries and persons to combat terrorism, TF, proliferation of weapons of mass destruction and PF as well as suppress other forms of armed conflicts or violence against humanity. These obligations have been further elaborated and clarified in accordance with the relevant UNSCR.

## **2 Objective**

- 2.1 This policy document is intended to set out:
  - (b) obligations of reporting institutions with respect to the requirements imposed under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA);
  - (c) requirements on reporting institutions in implementing a comprehensive risk-based approach in managing ML/TF/PF risks; and
  - (d) requirements on reporting institutions in implementing targeted financial sanctions.

## **3 Applicability**

- 3.1 Where a reporting institution is subject to more than one document relating to AML/CFT/CPF matters issued pursuant to the AMLA, the more stringent set of requirements shall apply.
- 3.2 Where necessary, the competent authority may issue guidelines, circulars or notices to vary, delete, add to, substitute or modify this policy document.
- 3.3 In relation to the AML/CFT/CPF and targeted financial sanctions requirements to combat TF, PF and to suppress other forms of armed conflict related requirements, this policy document is applicable to:
  - (a) any reporting institution carrying out any activity specified in paragraph 9 of the First Schedule to AMLA (referred to as "accountants" in this policy document), when the reporting institution prepares or carries out the following activities for its clients:
    - (i) buying and selling of immovable property;
    - (ii) managing of client's money, securities or other property;
    - (iii) managing of accounts including savings and securities accounts;
    - (iv) organising of contributions for the creation, operation or management of companies; or

- (v) creating, operating or managing of legal entities or arrangements and buying and selling of business entities<sup>2</sup>.
- (b) any reporting institution carrying out any activity specified in paragraph 13 of the First Schedule to AMLA (referred to as “company secretaries” in this policy document), when the reporting institution prepares or carries out the following activities for its clients:
  - (i) act as formation agent of legal entities;
  - (ii) act as (or arrange for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal entities;
  - (iii) provide a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal entities or arrangement;
  - (iv) act as (or arrange for another person to act as) a trustee of an express trust; or
  - (v) act as (or arrange for another person to act as) a nominee shareholder for another person<sup>3</sup>.
- (c) companies incorporated under the Companies Act 2016 and businesses as defined and registered under the Registration of Businesses Act 1956 which are carrying on activities of dealing in precious metals or precious stones (referred to as “dealers in precious metals or precious stones” in this policy document).
- (d) any reporting institution carrying out any activity specified in paragraphs 10, 11 and 12 of the First Schedule to AMLA (collectively referred to as “lawyers” in this policy document), when the reporting institution prepares or carries out the following activities for its clients:
  - (i) buying and selling of immovable property;
  - (ii) managing client’s money, securities or other property;
  - (iii) managing accounts including savings and securities accounts;
  - (iv) organising of contributions for the creation, operation or management of companies; or
  - (v) creating, operating or managing of legal entities or arrangements and buying and selling of business entities<sup>4</sup>.
- (e) licensed casinos carrying on gaming business under the Common Gaming Houses Act 1953;
- (f)
  - (i) licensee as defined in the Pool Betting Act 1967;
  - (ii) totalizator agency as defined in the Racing (Totalizator Board) Act 1961; and
  - (iii) racing club as defined in the Racing Club (Public Sweepstakes) Act 1965.

---

<sup>2</sup> As published in P.U. (A) 340/2004, P.U. (A) 293/2006, P.U. (A) 494/2021 and P.U. (A) 495/2021

<sup>3</sup> As published in P.U. (A) 340/2004, P.U. (A) 293/2006, P.U. (A) 494/2021 and P.U. (A) 495/2021

<sup>4</sup> As published in P.U. (A) 340/2004, P.U. (A) 293/2006, P.U. (A) 494/2021 and P.U. (A) 495/2021

- (referred to collectively as “licensed gaming outlets” in this policy document);
- (g) notaries public as defined in the Notaries Public Act 1959 when they exercise their powers and functions under that Act in relation to the following activities for their clients:
    - (i) buying and selling of immovable property;
    - (ii) managing of client’s money, securities or other property;
    - (iii) managing of accounts including savings and securities accounts;
    - (iv) organising of contributions for the creation, operation or management of companies; or
    - (v) creating, operating or managing of legal entities or arrangements and buying and selling of business entities<sup>5</sup>.
  - (h) any reporting institution carrying out any activity specified in paragraph 23 of the First Schedule to AMLA (referred to as “registered estate agents” in this policy document);
  - (i) the Corporation as defined in the Public Trust Corporation Act 1995 and trust companies as defined in the Trust Companies Act 1949 when they carry out the following activities for their clients:
    - (i) act as (or arrange for another person to act as) a director or secretary of a company, a partner of a partnership, or any similar position in relation to other legal entities;
    - (ii) act as (or arrange for another person to act as) a trustee of an express trust; or
    - (iii) act as (or arrange for another person to act as) a nominee shareholder for another person<sup>6</sup>.
  - (j) activities relating to building credit business, development finance business, factoring business or leasing business carried out by companies incorporated pursuant to the Companies Act 1965 and businesses as defined and registered under the Registration of Businesses Act 1956;
  - (k) moneylenders licensed under the Moneylenders Act 1951;
  - (l) pawnbrokers as defined under the Pawnbrokers Act 1972;
  - (m) any other reporting institution as may be specified by the competent authority; and
  - (n) branches and subsidiaries of reporting institutions, in and outside Malaysia, which carry on any activity listed in the First Schedule of the AMLA, where relevant.

---

<sup>5</sup> As published in P.U. (A) 113/2005 and P.U. (A) 293/2006

<sup>6</sup> As published in P.U. (A) 293/2006 and P.U.(A) 103/2007

- 3.4 This policy document is applicable to accountants, company secretaries and lawyers who are sole practitioners, partners or employed professionals within professional firms. This policy document is not intended to be applicable to lawyers, accountants and company secretaries who are 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies.

## **4 Legal Provisions**

- 4.1 In relation to the AML/CFT provisions, this policy document is issued pursuant to:
- (a) sections 8, 13, 14, 14A, 15, 16, 17, 18, 19, 20 and 83 of the AMLA; and
  - (b) section 143(2) of the Financial Services Act 2013 (FSA).
- 4.2 In relation to the targeted financial sanctions on terrorism financing requirements, this policy document is issued pursuant to section 14(1)(c) of the AMLA.
- 4.3 In relation to CPF, targeted financial sanctions on proliferation financing and other UN-Sanctions Regimes requirements, this policy document is issued for the purposes of monitoring and supervising the implementation of the obligations and restrictions under the Strategic Trade Act 2010 (STA), Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 and Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing<sup>7</sup> (Directive on TFS-PF) issued by the Strategic Trade Controller, Ministry of Investment, Trade and Industry in April 2018, as may be amended or superseded from time to time.

## **5 Effective Date**

- 5.1 This policy document comes into effect on **6 February 2024**.
- 5.2 Compliance to the requirements outlined in this policy document shall take effect immediately, unless otherwise specified by the competent authority.
- 5.3 Notwithstanding paragraph 5.2, CPF requirements in this policy document shall come into effect on such date as shall be specified by the competent authority.

---

<sup>7</sup> Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF) under the Strategic Trade Act 2010, Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 and Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010



## 6 Definition and Interpretation

6.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the AMLA, STA, Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 and Directive on TFS-PF, as the case may be, unless otherwise defined in this policy document or the context requires otherwise.

6.2 For the purpose of this policy document:

<b>“accurate information”</b>	<p>Refers to information that has been verified for accuracy.</p> <p>In the context of beneficial owners, it refers to information that has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable, independently sourced or obtained documents, data or information. The extent of verification may vary depending on the level of risk.</p>
<b>“authorised person”</b>	<p>Refers to a natural person appointed in writing by a legal person to establish business relations or conduct business transactions or activities with a reporting institution including to give any instruction for the conduct of transactions or activities on behalf of the legal person.</p> <p>In writing includes by means of a letter of authority or directors’ resolution or by electronic means, as permitted under the legal person’s constitution.</p>
<b>“beneficial owner”</b>	<p>In the context of legal person, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.</p> <p>Reference to “ultimately owns or control” or “ultimate effective control” refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.</p> <p>For insurance and takaful products, this also refers to any natural person(s) who ultimately owns or controls a beneficiary, as specified in this policy document.</p> <p>In the context of legal arrangements, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the</p>

	<p>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.</p> <p>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.</p>
<b>“beneficiary”</b>	<p>Depending on the context:</p> <p>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.</p> <p>The accumulation period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.</p> <p>In clubs, societies and charities, refers to the natural person(s), or groups of natural persons who receive charitable, humanitarian or other types of services of the clubs, societies and charities.</p>
<b>“Board”</b>	<p>In relation to a company, refers to:</p> <ul style="list-style-type: none"> <li>(a) directors of the company who number not less than the required quorum acting as a board of directors; or</li> <li>(b) if the company has only one director, that director.</li> </ul> <p>In relation to:</p> <ul style="list-style-type: none"> <li>(a) a sole proprietorship, refers to the sole proprietor; or</li> <li>(b) a partnership, including limited liability partnership, refers to the senior or equity partners.</li> </ul>
<b>“cash transaction”</b>	<p>Refers to a transaction where cash or cash equivalent is paid by or on behalf of a customer in the form of:</p> <ul style="list-style-type: none"> <li>(a) bank notes and coins to the reporting institution or into a bank account of the reporting institution;</li> <li>(b) bearer negotiable instruments including traveller’s cheques, vouchers and others; or</li> <li>(c) precious metals and/or stones.</li> </ul>

<b>“close associate of PEP”</b>	Refers to any individual closely connected to a politically exposed person (PEP), either socially or professionally. A close associate in this context includes: (a) extended family members, such as relatives (biological or non-biological relationship); (b) financially dependent individuals (e.g. persons salaried by the PEP such as drivers, bodyguards, secretaries); (c) business partners or associates of the PEP; (d) prominent members of the same organisation as the PEP; (e) individuals working closely with the PEP (e.g. work colleagues or providing professional services); or (f) close friends.
<b>“competent authority”</b>	Refers to a person appointed by the Minister of Finance by order published in the <i>Gazette</i> , pursuant to section 7(1) of the AMLA. As of the date of issuance, this refers to Bank Negara Malaysia.
<b>“customer”</b>	Refers to a person for whom the reporting institution undertakes or intends to undertake business transaction. The term also refers to a client.
<b>“customer due diligence (CDD)”</b>	Refers to any measure undertaken pursuant to section 16 of the AMLA.
<b>“Designated Non-Financial Businesses and Professions (DNFBPs)”</b>	Refers to reporting institutions listed in paragraph 3.3 (a) to (i) of this policy document.
<b>“director”</b>	Refers to any person who occupies the position of director, however styled, of a body corporate and includes a person in accordance with whose directions or instructions the majority of directors or officers are accustomed to act and an alternate or substitute director.  In relation to: (a) a sole proprietorship, refers to the sole proprietor; or (b) a partnership, including limited liability partnership, refers to the senior or equity partners.
<b>“DNFBP Group”</b>	Refers to a group that consists of a parent company incorporated in Malaysia or 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 subject to AML/CFT/CPF policies and procedures at the group level.
<b>“family members of PEP”</b>	Refers to individuals who are related to a PEP either directly (consanguinity) or through marriage. A family member in this context includes: (a) parent;

	<p>(b) sibling; (c) spouse; (d) child; or (e) spouse's parent, for both biological or non-biological relationships.</p>
<b>“financial group”</b>	Refers to a group that consists of a holding company incorporated in Malaysia 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.
<b>“financing of proliferation” or “proliferation financing”</b>	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 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).
<b>“fund-in transaction”</b>	Refers to transactions where a licensed casino accepts funds from its customers or junkets. The transactions can be in cash or other forms.
<b>“fund-out transaction”</b>	Refers to transactions where a licensed casino pays the winning or non-winning funds, commission, rebates and other payment to its customers or junkets. The transactions can be in cash or other forms.
<b>“G”</b>	Denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted.
<b>“higher risk”</b>	<p>Refers to circumstances where the reporting institutions assesses the ML/TF/PF risks as higher, taking into consideration, and not limited to the following factors:</p> <p>(a) Customer risk factors:</p> <ul style="list-style-type: none"> <li>• the business relationship is conducted in unusual circumstances;</li> <li>• non-resident customers;</li> <li>• legal persons or arrangements that are personal asset-holding vehicles;</li> <li>• companies that have nominee shareholders or shares in bearer form;</li> <li>• businesses that are cash-intensive;</li> <li>• the ownership structure of the company appears unusual or excessively complex given the nature of the company’s business;</li> <li>• high net worth individuals;</li> </ul>

	<ul style="list-style-type: none"> <li>• persons from locations known for their high rates of crime;</li> <li>• circumstances, businesses or activities identified by the FATF as having higher ML/TF/PF risks;</li> <li>• legal arrangements that are complex (e.g. nominee relationships or layering with legal persons); and</li> <li>• persons who match the red flag criteria of the reporting institutions.</li> </ul> <p>(b) Country or geographic risk factors:</p> <ul style="list-style-type: none"> <li>• countries identified by credible sources, such as mutual evaluation or published follow-up reports, as having inadequate AML/CFT/CPF systems;</li> <li>• countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;</li> <li>• countries identified by the FATF, other FATF-style regional bodies or other international bodies as having higher ML/TF/PF risks;</li> <li>• countries identified by credible sources as having significant levels of corruption or other criminal activities; and</li> <li>• countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.</li> </ul> <p>(c) Product, service, transaction or delivery channel risk factors:</p> <ul style="list-style-type: none"> <li>• anonymous transactions (which may include cash);</li> <li>• non face-to-face business relationships or transactions;</li> <li>• payment received from multiple persons and/or countries that do not match the person's nature of business and risk profile;</li> <li>• payment received from unknown or unrelated third parties; and</li> <li>• nominee services.</li> </ul>
<b>“higher risk countries”</b>	Refers to countries that are called by the FATF or the Government of Malaysia that pose a risk to the international financial system.
<b>“international organisations”</b>	<p>Refers to entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as residential institutional units of the countries in which they are located. Examples of international organisations include the following:</p> <p>(a) United Nations and its affiliated international organisations;</p>

	<p>(b) regional international organisations such as the Association of Southeast Asian Nations, the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organization of American States;</p> <p>(c) military international organisations such as the North Atlantic Treaty Organization; and</p> <p>(d) economic organisations such as the World Trade Organization.</p>
<b>“junkets”</b>	Refers to individuals or legal persons, including their representatives, approved, registered or appointed by a licensed casino to introduce, organise and/or facilitate the playing of any game in a licensed casino by one or more customers including local and foreign customers.
<b>“legal arrangement”</b>	Refers to express trusts or other similar legal arrangements.
<b>“legal person”</b>	<p>Refers to any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLCs), foundations, partnerships, or associations and other similar entities.</p> <p>GLC refers to an entity where the government is the majority shareholder or single largest shareholder and/or has the ability to exercise and influence major decisions such as appointment of board members and senior management.</p>
<b>“mobile channel”</b>	Refers to conducting transactions through any electronic device using a mobile phone application provided by the reporting institutions.
<b>“National Risk Assessment (NRA)”</b>	Reference to NRA under paragraph 1.4 of this policy document is not limited to the National ML/TF Risk Assessment and includes any sectoral, thematic or emerging risk assessments undertaken by the NCC.
<b>“nominator”</b>	Refers to 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”.
<b>“nominee director and shareholder”</b>	<p>Refers to an individual or legal person instructed by another individual or legal person (“the nominator”) to act on behalf in a certain capacity regarding a legal person.</p> <p>A Nominee Director (also known as a “resident director”) is an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct</p>

	<p>or indirect instructions of the nominator. A Nominee Director is never the beneficial owner of a legal person.</p> <p>A Nominee Shareholder 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.</p>
<b>“Non-Bank Financial Institutions”</b>	Refers to reporting institutions listed in paragraph 3.3 (j) to (l) of this policy document.
<b>“online channel”</b>	Refers to conducting transactions through any electronic device other than transactions conducted via the mobile channel.
<b>“other DNFBP structures”</b>	<p>Refers to DNFBP structures that do not operate like financial groups but share common ownership, management or compliance control, that refer to but not limited to the following:</p> <p>(a) Common ownership</p> <ul style="list-style-type: none"> <li>• Common shareholder(s) or partner(s).</li> </ul> <p>(b) Common management</p> <ul style="list-style-type: none"> <li>• There is a group governing or managing body, each entity works on the basis of a group-wide business strategy and/or business model;</li> <li>• Group level reporting e.g. directors and other senior management;</li> <li>• Group audit or reporting function overseeing implementation of common/group policies and procedures;</li> <li>• Arrangements exist requiring two or more entities/offices to implement and operate to common policies and procedures; or</li> <li>• Where responsibility for developing group policies and procedures rests with one entity in the group/network/franchise.</li> </ul> <p>(c) Common compliance controls</p> <ul style="list-style-type: none"> <li>• Existing group-wide policies, compliance and audit functions;</li> <li>• Where an entity is obliged to periodically report to another connected individual/entity on compliance and/or risk management matters; or</li> <li>• Periodic central administration/compliance costs being charged to the local entity by a connected individual/entity.</li> </ul>

<b>“person”</b>	Includes a body of persons, corporate or unincorporate.
<b>“person conducting the transaction”</b>	Refers to any natural person conducting the transaction or purporting to act on behalf of the customer, such as the person depositing into another customer’s account or person undertaking a transaction on behalf of another person.
<b>“politically exposed persons (PEPs)”</b>	<p>Refers to:</p> <ul style="list-style-type: none"> <li>(a) foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials;</li> <li>(b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government (includes federal, state and local government), judiciary or military officials, senior executives of state-owned corporations and important political party officials; or</li> <li>(c) persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the Board or equivalent functions.</li> </ul> <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>
<b>“S”</b>	Denotes a standard, obligation, requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.
<b>“satisfied”</b>	Where reference is made to a reporting institution being “satisfied” as to a matter, the reporting institution must be able to justify its assessment to the competent authority or supervisory authority in documentary form.
<b>“Self-Regulatory Body (SRB)”</b>	Refers to a body that represents a profession (e.g. lawyers, accountants or company secretaries), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and/or also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to



	ensure that high ethical and moral standards are maintained by those practising the profession.
<b>“Senior Management”</b>	Refers to any person having authority and responsibility for planning, directing or controlling the activities of a reporting institution, legal person or legal arrangement including the management and administration of a reporting institution, legal person or legal arrangement.
<b>“small-sized reporting institution”</b>	Refers to reporting institutions that satisfy the criteria and parameter relevant to respective DNFBPs and non-bank financial institutions as listed in Appendix 2 of this policy document.
<b>“supervisory authority”</b>	Refers to ministries, agencies or SRBs which may exercise powers pursuant to section 21 of the AMLA.
<b>“targeted financial sanctions”</b>	Refers to asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of persons designated or entities specified by the relevant United Nations Security Council Sanctions Committee or by the Minister of Home Affairs.
<b>“third parties”</b>	<p>Refers to reporting institutions that are supervised by a relevant competent authority and that meet the requirements under paragraph 16 on Reliance on Third Parties, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process.</p> <p>Reliance on third parties often occurs through introductions made by another member of the same financial group, DNFBP group or by another reporting institution.</p> <p>This definition does not include outsourcing or agency relationships because the outsourced service provider or agent is regarded as synonymous with the reporting institution. Outsourced service providers or agents may include registered estate negotiators, marketing agents or outsourced telemarketers and others.</p>
<b>“up-to-date information”</b>	Refers to information which is as current and up-to-date as possible, and is updated within a reasonable period following any change.

## **7 Related Legal Instruments and Policy Documents**

- 7.1 This policy document shall be read together with other documents issued by the competent authority relating to compliance with AML/CFT/CPF requirements and in relation to the implementation of targeted financial sanctions against countries or persons designated by the United Nations (UN).

## **8 Policy Documents Superseded**

- 8.1 This policy document supersedes the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) which came into effect on 1 January 2020.

## **9 Non-Compliance**

- 9.1 Enforcement and/or supervisory actions can be taken against the reporting institution including its directors, officers and employees for any non-compliance with any provision marked as “S” in Part B of this policy document.

## **PART B AML/CFT/CPF/TFS REQUIREMENTS**

### **10 Application of Risk-Based Approach**

#### **10.1 Risk Management Function**

- S** 10.1.1 Reporting institutions are required to apply risk-based approach to identify, assess and understand the ML/TF/PF risks to which they are exposed and take AML/CFT/CPF measures commensurate to those risks in order to mitigate them effectively and efficiently.
- S** 10.1.2 Reporting institutions are required to ensure that the risk-based approach is aligned to the size, nature and complexity of their business operations.
- S** 10.1.3 For a licensed casino and non-bank financial institutions, in addition to paragraphs 10.1.1 and 10.1.2, the AML/CFT/CPF risk management function must be aligned and integrated with their overall risk management control function.

#### **10.2 ML/TF Risk Assessment**

- S** 10.2.1 Reporting institutions are required to take appropriate steps to identify, assess and understand their ML/TF risks at the institutional level, in relation to their customers, countries or geographical areas, products, services, transactions or delivery channels, and other relevant risk factors.
- S** 10.2.2 In assessing ML/TF risks, reporting institutions are required to have the following processes in place:
- (a) documenting their 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 assessment up-to-date through a periodic review; and
  - (d) having appropriate mechanism to provide risk assessment information to the competent authority or supervisory authority.
- S** 10.2.3 Reporting institutions are required to conduct additional assessment as and when required by the competent authority or supervisory authority.
- S** 10.2.4 Reporting institutions shall be guided by the results of the NRA issued by the NCC in conducting their own risk assessments and shall take enhanced measures to manage and mitigate the risks identified in the NRA.

- G** 10.2.5 In conducting the risk assessment in paragraph 10.2.1, reporting institutions may consider whether:
- (a) it is susceptible to the key emerging crimes as well as higher risk sectors identified in the NRA when assessing their institutional ML/TF risk; and
  - (b) enhancements to their AML/CFT Compliance Programme are warranted to ensure any areas of higher ML/TF risk are appropriately mitigated.

### 10.3 **ML/TF Risk Control and Mitigation**

- S** 10.3.1 Reporting institutions are required to:
- (a) have policies, procedures and controls to manage and mitigate ML/TF risks that have been identified;
  - (b) monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and
  - (c) take enhanced measures to manage and mitigate the risks where higher risks are identified and where specified by the competent authority or supervisory authority.
- S** 10.3.2 In addition to paragraph 10.3.1, a licensed casino and non-bank financial institutions shall conduct independent control testing on their policies, procedures and controls for the purpose of monitoring the implementation thereof under paragraph 10.3.1(b).

### 10.4 **PF Risk Assessment**

- S** 10.4.1 Reporting institutions are required to identify, assess and understand PF risks, where the extent of the assessment shall be appropriate to the nature, size and complexity of their business. The PF risk in this context is limited to potential breach, non-implementation or evasion of the targeted financial sanctions on PF under paragraph 24 of this policy document.
- G** 10.4.2 In conducting the risk assessment, reporting institutions 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.
- S** 10.4.3 For the purpose of paragraph 10.4.1, reporting institutions are required to identify, assess and understand their PF risks at the institutional level, in relation to their customers, countries or geographical areas and products, services transactions or delivery channels and other relevant risk factors.

- S** 10.4.4 In assessing PF risks, reporting institutions are required to have the following processes in place:
- (a) documenting their PF risk assessments and findings;
  - (b) keeping the assessment up-to-date through a periodic review; and
  - (c) having appropriate mechanism to provide risk assessment information to the competent authority or supervisory authority.

- S** 10.4.5 Reporting institutions shall be guided by the results of the NRA and related thematic risk assessment issued by the NCC in conducting their own risk assessments and shall take enhanced measures to manage and mitigate the risks identified in the NRA.

## 10.5 **PF Risk Mitigation**

- S** 10.5.1 Reporting institutions are required to:
- (a) have policies, procedures and controls to manage and mitigate PF risks that have been identified;
  - (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, reporting institutions shall introduce enhanced controls to detect possible breaches, non-implementation or evasion of targeted financial sanctions on PF under paragraph 24 of this policy document; and
    - (ii) where lower PF risks are identified, reporting institutions shall ensure that measures to manage and mitigate the risks are commensurate with the level of risk while ensuring full implementation of the targeted financial sanctions on PF under paragraph 24 of this policy document.

- S** 10.5.2 Reporting institutions shall ensure full implementation of the targeted financial sanctions on PF under paragraph 24 of this policy document irrespective of the institutional PF risk level.

## 10.6 **Customer Risk Profiling**

- S** 10.6.1 Reporting institutions are required to conduct risk profiling on their customers and assign an ML/TF/PF risk rating that is commensurate with their risk profile.

- S** 10.6.2 A risk profile must consider the following factors, where relevant:
- (a) customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of PEP, types of occupation);
  - (b) country or geographical risk (e.g. location of business, origin of customers);
  - (c) products, services, transactions or delivery channels (e.g. cash-based or non cash-based, face-to-face or non face-to-face, domestic or cross-border); and
  - (d) any other information suggesting that the customer is of higher risk.
- G** 10.6.3 In identifying countries and geographic risk factors under paragraph 10.6.2(b), reporting institutions may refer to credible sources such as mutual evaluation reports, follow up reports and other relevant reports published by international organisations and other inter-governmental bodies.
- S** 10.6.4 The risk control and mitigation measures implemented by reporting institutions shall be commensurate with the risk profile of the particular customer or type of customer.
- S** 10.6.5 After the initial acceptance of the customer, reporting institutions are required to regularly review and update the customer's risk profile based on their level of ML/TF/PF risks.
- S** 10.6.6 In addition to paragraph 10.6.1, a licensed casino is required to conduct ML/TF/PF risk profiling on junkets.

## 10.7 **AML/CFT/CPF Risk Reporting**

- S** 10.7.1 A licensed casino and non-bank financial institutions shall provide timely reporting of the risk assessment, ML/TF/PF risk profile and the effectiveness of risk control and mitigation measures to their Board and Senior Management. The frequency of reporting shall be commensurate with the level of risks involved and their operating environment.
- G** 10.7.2 The report referred to under paragraph 10.7.1 above may include the following:
- (a) results of AML/CFT/CPF monitoring activities carried out by a licensed casino and non-bank financial institutions such as the level of their exposure to ML/TF/PF risks, break-down of ML/TF/PF risk exposures based on key activities or customer and junket segments, trends of suspicious transaction reports and cash threshold reports, trends of orders received from law enforcement agencies, where relevant;
  - (b) details of recent significant risk events, that occur either internally or externally, modus operandi and its impact or

- potential impact to the licensed casino and non-bank financial institutions; and
- (c) recent developments in AML/CFT/CPF laws and regulations, and its implications to the licensed casino and non-bank financial institutions.

## 10.8 Risk Guidance

- G** 10.8.1 Reporting institutions may refer to documents provided in Parts C and D of this policy document, other documents issued by the competent authority or guidance papers on the implementation of risk-based approach published by the FATF, FATF style regional bodies or any other internationally recognised institution.

## **11 AML/CFT/CPF Compliance Programme**

### **11.1 Application for Small-sized Reporting Institutions**

- S** 11.1.1 For small-sized reporting institutions as defined under paragraph 6.2, the following exemption or simplification applies:
- (a) Paragraph 11.2 on Policies, Procedures and Controls requirements does not apply. However, such reporting institutions shall, at a minimum, adopt this policy document as their policies and procedures;
  - (b) Paragraphs 11.3.4 (c) and (f) of requirements on Board do not apply;
  - (c) Paragraphs 11.4.2 (b), (c) and (h) of requirements on Senior Management do not apply. However, the approval of overall Compliance Programme and enhanced due diligence is still within the accountability of the individual with control on the overall operations of the reporting institution;
  - (d) Paragraph 11.7 on Employee Screening requirements shall apply upon initial hiring only;
  - (e) Paragraph 11.8 on Employee Training and Awareness Programmes requirements shall be adopted in a simplified approach, such as via on-the-job training and third party training programme; and
  - (f) Paragraph 11.9 on Independent Audit Functions requirements shall be exempted.
- S** 11.1.2 Notwithstanding paragraph 11.1.1, such reporting institutions are required to comply with the AML/CFT/CPF Compliance Programme requirements as and when specified by the competent authority or supervisory authority.

### **11.2 Policies, Procedures and Controls**

- S** 11.2.1 Reporting institutions are required to develop AML/CFT/CPF policies, procedures and controls which correspond to their ML/TF/PF risks and the size, nature and complexity of their business operations.
- S** 11.2.2 Reporting institutions must ensure that policies and procedures are kept up-to-date with the regulatory requirements.



- S** 11.2.3 For purpose of paragraph 11.2.2, reporting institutions are required to:
- (a) document any changes to the policies, procedures and controls;
  - (b) document the communication of the changes to employees; and
  - (c) make (a) and (b) available to the competent authority or supervisory authority upon request.

### 11.3 **Board**

#### ***General***

- S** 11.3.1 Board members must understand their roles and responsibilities in managing ML/TF/PF risks identified by the reporting institution.
- S** 11.3.2 Board members must have knowledge and awareness of the ML/TF/PF risks associated with business strategies, delivery channels, segment of customers and geographical coverage of its business products and services.
- S** 11.3.3 Board members must understand the AML/CFT/CPF measures required by the relevant laws, instruments issued under the AMLA, as well as the industry's standards and best practices in implementing AML/CFT/CPF measures.

#### ***Roles and Responsibilities***

- S** 11.3.4 The Board has the following roles and responsibilities:
- (a) maintain accountability and oversight for establishing AML/CFT/CPF policies and minimum standards;
  - (b) approve policies regarding AML/CFT/CPF measures within the reporting institution, including those required for risk assessment, mitigation and profiling, customer due diligence (CDD), record keeping, enhanced CDD and on-going due diligence, suspicious transaction report and targeted financial sanctions;
  - (c) approve appropriate mechanisms to ensure the AML/CFT/CPF policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF/PF;
  - (d) approve an effective internal control system for AML/CFT/CPF and maintain adequate oversight of the overall AML/CFT/CPF measures undertaken by the reporting institution;
  - (e) define the lines of authority and responsibility for implementing AML/CFT/CPF measures and ensure that

- there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- (f) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF/PF;
  - (g) assess the implementation of the approved AML/CFT/CPF policies through regular reporting and updates by the Senior Management and Audit Committee; and
  - (h) establish a Management Information System (MIS) that is reflective of the nature of the reporting institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

#### 11.4 Senior Management

- S** 11.4.1 Senior Management is accountable for the implementation and management of AML/CFT/CPF compliance programmes in accordance with policies, procedures and controls approved by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

##### ***Roles and Responsibilities***

- S** 11.4.2 The Senior Management has the following roles and responsibilities:
- (a) be aware of and understand the ML/TF/PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including 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, volume of the transactions undertaken by the reporting institution and its geographical coverage;
  - (c) establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT/CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;
  - (d) undertake review and propose to the Board the necessary enhancements to the AML/CFT/CPF policies to reflect changes in the reporting institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;
  - (e) provide timely periodic reporting to the Board on the level of ML/TF/PF risks facing 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, nature and complexity of the reporting institution's operations and risk profiles;
- (g) appoint a Compliance Officer at management level at the Head Office and designate a Compliance Officer at management level at each branch or subsidiary;
- (h) ensure appropriate levels of AML/CFT/CPF training for its employees at all levels within the organisation, where relevant;
- (i) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT/CPF policies and procedures to all levels of employees;
- (j) ensure that AML/CFT/CPF issues raised are addressed in a timely manner; and
- (k) ensure integrity of its employees by establishing appropriate employee assessment procedures.

## 11.5 Compliance Management Arrangements at the Head Office

- S** 11.5.1 The Compliance Officer shall act as the reference point for AML/CFT/CPF matters within the reporting institution.
- S** 11.5.2 The Compliance Officer must have sufficient stature, authority and seniority within the reporting institution to participate and be able to effectively influence decisions relating to AML/CFT/CPF matters.
- S** 11.5.3 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT/CPF responsibilities effectively.
- S** 11.5.4 For the purpose of paragraph 11.5.3, "fit and proper" shall include minimum criteria relating to:
  - (a) probity, personal integrity and reputation;
  - (b) competency and capability; and
  - (c) financial integrity.
- G** 11.5.5 With reference to requirements under paragraph 11.5.4(a), reporting institutions may take into consideration, the following factors or examples that may impair the effective discharging of the Compliance Officer's responsibilities, whether the person:
  - (a) is or has been the subject of any proceedings of a severe disciplinary or criminal nature;
  - (b) has contravened any provision made by or under any written law designed to protect members of the public against

- financial loss due to dishonesty, incompetence or malpractice;
  - (c) has contravened any of the requirements and standards in relation to fitness and propriety, of a regulatory body, government or its agencies or SRBs;
  - (d) has engaged in any business practices which are deceitful, oppressive or otherwise improper (whether unlawful or not), or which otherwise reflect discredit on his professional conduct;
  - (e) has been dismissed, asked to resign or has been resigned from employment or from a position of trust, fiduciary appointment or similar position because of questions about his honesty and integrity; and
  - (f) has acted unfairly or dishonestly in the past, in his dealings with his customers, employer, auditors and regulatory authorities.
- G** 11.5.6 With reference to requirements under paragraph 11.5.4 (b), reporting institutions may consider whether the person has satisfactory past performance or expertise, in consideration of the size, nature and complexity of their business operations.
- G** 11.5.7 With reference to requirements under paragraph 11.5.4 (c), reporting institutions may consider the following factors:
  - (a) whether he has been and will be able to fulfil his financial obligations, whether in Malaysia or elsewhere, as and when they fall due; and
  - (b) whether the person has been the subject of a judgment debt which is unsatisfied, either in whole or in part.
- G** 11.5.8 In conducting assessment under paragraphs 11.5.4 (c) and 11.5.7, reporting institutions may refer to commercially available financial or credit databases, require the person to submit relevant credit reports or to complete self-declarations on the required information, depending on the size, nature and complexity of their business operations.
- S** 11.5.9 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including keeping abreast with the latest developments in ML/TF/PF techniques and the AML/CFT/CPF measures undertaken by the industry.
- G** 11.5.10 The Compliance Officer is encouraged to have the relevant AML/CFT/CPF certification or professional qualifications to carry out his responsibilities effectively.

- S** 11.5.11 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.
- S** 11.5.12 The Compliance Officer has a duty to ensure:
- (a) compliance with the AML/CFT/CPF requirements;
  - (b) effective implementation of appropriate AML/CFT/CPF policies and procedures, including CDD, record-keeping, on-going due diligence, suspicious transaction report and targeted financial sanctions;
  - (c) regular assessment of the AML/CFT/CPF mechanism such that it is effective and sufficient to address any change in ML/TF/PF trends;
  - (d) security and confidentiality of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer;
  - (e) all employees are aware of the reporting institution's AML/CFT/CPF measures, including policies, control mechanism and reporting channels;
  - (f) establish and maintain relevant internal criteria (red-flags) to enable identification and detection of suspicious transactions;
  - (g) appropriate evaluation of internal suspicious transaction reports by the branch or subsidiary compliance officers before being promptly reported to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia;
  - (h) proper identification of ML/TF/PF risks associated with new products or services or risks arising from the reporting institution's operational changes, including the introduction of new technology and processes; and
  - (i) compliance with any other obligations that are imposed under the AMLA, subsidiary legislation and relevant instruments.
- S** 11.5.13 Reporting institutions are required to inform the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, in writing or by completing the form at <https://amlcft.bnm.gov.my/co>, within ten working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, e-mail address and such other information as may be required.

## **11.6 Fit and Proper Test on Junkets**

- S** 11.6.1 A licensed casino is required to ensure that all junkets are "fit and proper" before appointing, registering or approving the application of any junkets. For existing junkets, a licensed casino must take reasonable measures to ensure that they are "fit and proper".

- S** 11.6.2 For the purpose of paragraph 11.6.1, “fit and proper” shall include minimum criteria relating to:
- (a) probity, personal integrity and reputation;
  - (b) competency and capability; and
  - (c) financial integrity.
- S** 11.6.3 After the initial appointment, registration or approval of junkets, a licensed casino is required to regularly assess the fitness and propriety of the junkets based on the level of ML/TF/PF risks.
- G** 11.6.4 With reference to the requirements under paragraph 11.6.2, a licensed casino may take into consideration the factors provided under paragraphs 11.5.5, 11.5.6, 11.5.7 and 11.5.8.

## **11.7 Employee Screening Procedures**

- S** 11.7.1 Reporting institutions are required to establish employee assessment procedures that are commensurate with the size, nature and complexity of their business operations and ML/TF/PF risk exposure.
- S** 11.7.2 For a licensed casino, employee screening shall be conducted on junkets assessed to have higher ML/TF/PF risks.
- S** 11.7.3 The screening procedures shall apply upon initial hiring of the employee and throughout the course of employment.
- S** 11.7.4 The employee assessment procedures under paragraph 11.7.1 shall include:
- (a) an evaluation of an employee’s personal information, including employment and financial history; and
  - (b) clear parameters or circumstances to trigger re-screening of employees during the course of their employment.
- G** 11.7.5 In conducting financial history assessment, reporting institutions may refer to commercially available financial or credit databases, require employees to submit relevant credit reports or to complete self-declarations on the required information.
- G** 11.7.6 The parameters to trigger re-screening may include change in job function or responsibility, promotion, or being in a position for a long period of time.

- G** 11.7.7 Reporting institutions may determine that several functions may not be subject to screening requirements, provided that such functions do not have direct dealings with customers and/or are not involved in the monitoring of transactions, based on the size, nature, and complexity of their business operations and ML/TF/PF risk profile.
- S** 11.7.8 Reporting institutions shall maintain comprehensive records of documents and information relating to, or relied on in, the employee screening process.
- 11.8 Employee Training and Awareness Programmes**
- S** 11.8.1 Reporting institutions shall conduct awareness and training programmes on AML/CFT/CPF practices and measures for their employees. Such training programmes must be conducted regularly and supplemented with refresher courses at appropriate intervals.
- S** 11.8.2 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF/PF activities and the risks of ML/TF/PF identified by reporting institutions.
- S** 11.8.3 Employees who deal directly with customers shall be trained on AML/CFT/CPF practices and measures prior to dealing with the customer.
- S** 11.8.4 The scope of training shall include, at a minimum:
- (a) ML/TF/PF risks;
  - (b) CDD, enhanced CDD and on-going due diligence;
  - (c) targeted financial sanctions screening;
  - (d) risk profiling and risk assessment;
  - (e) suspicious transaction reporting mechanism and red flags; and
  - (f) record keeping.
- G** 11.8.5 Reporting institutions may consider distribution of circulars, guidance, publications and attendance of continuing education programs provided by the competent authority, SRBs and/or other relevant agencies in developing, and as part of their internal training programmes.
- S** 11.8.6 Reporting institutions shall document the provision of training to employees, including details on the date and nature of the training given.

- S** 11.8.7 Reporting institutions must make available its AML/CFT/CPF policies and procedures for all employees and its documented AML/CFT/CPF measures must contain at least the following:
- (a) the relevant documents on AML/CFT/CPF issued by the competent authority or relevant supervisory authorities; and
  - (b) the reporting institution's internal AML/CFT/CPF policies and procedures.
- S** 11.8.8 The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT/CPF requirements.
- G** 11.8.9 Reporting institutions may determine that several functions may not be subject to the AML/CFT/CPF training requirements, provided that such functions do not have direct dealings with customers and/or are not involved in the monitoring of transactions, based on the size, nature and complexity of their business operations and ML/TF/PF risk profile.

***Training for Junkets***

- S** 11.8.10 A licensed casino shall conduct awareness and training programmes on AML/CFT/CPF practices and measures for its junkets.
- S** 11.8.11 The frequency of and scope of training and awareness programmes shall commensurate with the level of ML/TF/PF risks posed by the junkets based on their risk profiles as assessed under paragraph 10.6.6.
- S** 11.8.12 The scope of training for the junkets shall include, at a minimum:
- (a) AML/CFT/CPF policies and procedures of the licensed casino;
  - (b) CDD, enhanced CDD and on-going due diligence; and
  - (c) the identification and escalation of suspicious transactions.
- S** 11.8.13 Upon identification of any suspicious transaction, the junkets must report the suspicious transaction to the AML/CFT/CPF Compliance Officer at the licensed casino in accordance with its reporting mechanism.



## 11.9 Independent Audit Functions

- S** 11.9.1 The Board shall ensure regular independent audits of the internal AML/CFT/CPF measures to determine their effectiveness and compliance with the AMLA, subsidiary legislations and instruments, the relevant documents on AML/CFT/CPF issued by the competent authority as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.
- S** 11.9.2 For the purpose of paragraph 11.9.1, the independent audit function must be separate from the compliance function.
- G** 11.9.3 Reporting institutions may appoint internal or external auditors to carry out the independent audit function.
- S** 11.9.4 The Board shall ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor shall include, at a minimum:
- (a) checking and testing the compliance with the AML/CFT/CPF policies, procedures and controls and effectiveness thereof; and
  - (b) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT/CPF requirements.
- S** 11.9.5 The Board shall determine and ensure the frequency and scope of independent audits conducted commensurate with the ML/TF/PF risks and vulnerabilities assessed by the reporting institution.
- S** 11.9.6 The scope of the independent audit shall include, at a minimum:
- (a) compliance with the AMLA, its subsidiary legislation and instruments issued under the AMLA;
  - (b) compliance with the reporting institution's internal AML/CFT/CPF policies and procedures;
  - (c) adequacy and effectiveness of the AML/CFT/CPF Compliance Programme; and
  - (d) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.
- G** 11.9.7 In determining the frequency of the independent audit, reporting institutions may be guided by the following circumstances:
- (a) structural changes to the business of the reporting institutions such as mergers and acquisition;
  - (b) changes to the number or volume of transactions reported to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia;

- (c) introduction of new products and services or new delivery channels; or
  - (d) previous non-compliance relating to AML/CFT/CPF requirements which resulted in supervisory and/or enforcement action taken against the reporting institutions.
- S** 11.9.8 Reporting institutions shall comply with any additional requirements on the frequency and scope of the independent audit as specified by the competent authority.
- S** 11.9.9 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of established AML/CFT/CPF measures and inadequacies in internal controls and procedures including recommended corrective measures.
- S** 11.9.10 Reporting institutions must ensure that such audit report including audit findings and the necessary corrective measures undertaken are made available to the competent authority or supervisory authority, upon request.
- S** 11.9.11 Notwithstanding paragraph 11.9.10, a licensed casino and non-bank financial institutions shall ensure that the audit report including audit findings and the necessary corrective measures undertaken are submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia within ten working days of their submission to the Board.

## **12 New Products and Business Practices**

- S** 12.1 Reporting institutions are required to identify and assess the ML/TF/PF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.
  
- S** 12.2 Reporting institutions are required to:
  - (a) undertake risk assessment prior to the launch or use of such products, practices and technologies; and
  - (b) take appropriate measures to manage and mitigate the risks.

### **13 Applicability to Financial/DNFBP Group, Foreign Branches and Subsidiaries and Other DNFBP Structures**

#### **13.1 Financial/DNFBP Group**

13.1.1 The requirements under this paragraph are only applicable to reporting institutions that are part of a financial and/or DNFBP group.

**S** 13.1.2 A parent company in a group of corporations, as the case may be, is required to implement group-wide programmes against ML/TF/PF. These programmes must be applicable and appropriate to all branches and subsidiaries of the group. These shall include the following measures:

- (a) framework for AML/CFT/CPF compliance programme at the group level;
- (b) appoint a Group Compliance Officer at management level;
- (c) policies and procedures for sharing information required for the purposes of CDD and ML/TF/PF risk management;
- (d) the provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes; and
- (e) safeguards on the confidentiality and use of information exchanged.

**S** 13.1.3 A Group Compliance Officer is responsible for developing, coordinating and making a group-wide assessment for the implementation of a single AML/CFT/CPF strategy, including mandatory policies and procedures, and the authorisation to give directions to all branches and subsidiaries.

#### **13.2 Foreign Branches and Subsidiaries**

**S** 13.2.1 Reporting institutions and financial/ DNFBP groups are required to closely monitor their foreign branches or subsidiaries operating in jurisdictions with inadequate AML/CFT/CPF laws and regulations as highlighted by the FATF or the Government of Malaysia.

**S** 13.2.2 Reporting institutions and financial/DNFBP groups shall ensure that their foreign branches and subsidiaries apply AML/CFT/CPF measures in a manner that is consistent with the AML/CFT/CPF requirements in Malaysia. Where the minimum AML/CFT/CPF requirements of the host country are less stringent than those of Malaysia, the reporting institution must apply Malaysia's AML/CFT/CPF requirements, to the extent that host country laws and regulations permit.

- S** 13.2.3 If the host country does not permit the proper implementation of AML/CFT/CPF measures in a manner that is consistent with the AML/CFT/CPF requirements in Malaysia, the reporting institution is required to apply additional measures to manage the ML/TF/PF risks, and report to the competent authority or supervisory authority in Malaysia on the AML/CFT/CPF gaps and additional measures implemented to manage the ML/TF/PF risks arising from the identified gaps.
- G** 13.2.4 The reporting institution may consider ceasing the operations of the said branch or subsidiary that is unable to put in place the necessary mitigating controls as required under paragraph 13.2.3.

### 13.3 Other DNFBP Structures

- 13.3.1 The requirements under this paragraph are only applicable to reporting institutions that operate under other DNFBP structures, as defined in paragraph 6.2 of this policy document and meet the following conditions:
- (a) reliance on other reporting institutions under the same structure to conduct CDD; and
  - (b) undertake more than one type of activity within and across more than one jurisdiction.
- S** 13.3.2 Reporting institutions are required to have common policies and procedures that is consistent with the AML/CFT/CPF requirements in Malaysia. Where the minimum AML/CFT/CPF requirements of the host country are less stringent than those of Malaysia, the reporting institution must apply Malaysia's AML/CFT/CPF requirements, to the extent that the host country laws and regulations permit.

## **14 Customer Due Diligence (CDD)**

- S** 14.1 Reporting institutions are required to conduct CDD on customers and persons conducting the transaction, when:
- (a) establishing business relations;
  - (b) carrying out any or occasional transaction involving the circumstances or amount as specified under paragraphs 14A to 14H;
  - (c) they have any suspicion of ML/TF/PF, regardless of amount; or
  - (d) they have any doubt about the veracity or adequacy of previously obtained information.
- S** 14.2 Reporting institutions are also required to comply with other specific CDD requirements as may be specified by the competent authority from time to time.
- S** 14.3 When conducting CDD, reporting institutions are required to:
- (a) identify the customer and verify that customer's identity using reliable, independent source documents, data or information;
  - (b) verify that any person acting on behalf of the customer is so 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 the relevant information or data obtained from a reliable source, 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 and intended nature of the business relationship.
- S** 14.4 Where applicable, in conducting CDD, reporting institutions are required to comply with the requirements on targeted financial sanctions in relation to:
- (a) terrorism financing under paragraph 23; and
  - (b) proliferation financing of weapons of mass destruction and other UN-sanctions under paragraph 24.

### ***Verification***

- S** 14.5 Reporting institutions must verify and be satisfied with the identity of the customer or beneficial owner through reliable and independent documentation, electronic data or any other measures that reporting institutions deem necessary.
- S** 14.6 Reporting institutions shall determine the extent of verification method that commensurate with the identified ML/TF/PF risks.
- S** 14.7 Reporting institutions must be satisfied with the veracity of the information referred to in paragraph 14.5 when verifying the identity of a customer or a beneficial owner.

- S** 14.8 Reporting institutions shall verify the identity of a customer or a beneficial owner before or during the course of establishing a business relationship or conducting a transaction for an occasional customer.
- G** 14.9 For the purpose of paragraph 14.5, reporting institutions may obtain information available through commercial or public databases in verifying the identity of the customer or beneficial owner.

#### 14.10 Standard CDD Measures

##### ***Individual Customer and Beneficial Owner***

- S** 14.10.1 In conducting CDD, the reporting institution is required to identify an individual customer and 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 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;
  - (h) contact number (home, office or mobile); and
  - (i) purpose of transaction.
- S** 14.10.2 Reporting institutions shall verify the identity of the customer and beneficial owner.

##### ***Legal Persons***

- S** 14.10.3 For customers that are legal persons, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.
- S** 14.10.4 Reporting institutions are required to identify the customer and verify its identity through the following information:
- (a) name, legal form and proof of existence, such as Certificate of Incorporation/Constitution/Partnership Agreement (certified true copies/duly notarised copies, may be accepted), unique identifier such as tax identification number or any other reliable references to verify the identity of the customer;
  - (b) the powers that regulate and bind the customer such as directors' resolution, as well as the names of relevant persons having a Senior Management position; and

- (c) the address of the registered office and, if different, a principal place of business.

**S** 14.10.5 Reporting institutions are required to identify and verify the person authorised to represent the company or business either by means of a letter of authority or directors' resolution when dealing with such person.

**S** 14.10.6 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners according to the cascading steps:

- (a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person. At a minimum, this includes identifying the directors/shareholders with equity interest of more than twenty-five percent/partners;
- (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 14.10.6(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 14.10.6(a) or (b), the identity of the relevant natural person who holds the position of Senior Management.

For the avoidance of doubt, reporting institutions are 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).

**G** 14.10.7 For the purpose of paragraph 14.10.6(b), exercising control of the legal person through other means may include exercising control through nominees or another person who has the right to appoint or remove any member of the Board of the legal person.

**S** 14.10.8 Where there is any doubt as to the identity of persons referred to under paragraphs 14.10.4, 14.10.5 and 14.10.6, the reporting institution shall:

- (a) conduct a basic search or enquiry on the background of such person to ensure that the person has not been or is not in the process of being dissolved or liquidated, or is a bankrupt; and
- (b) verify the authenticity of the information provided by such person with the Companies Commission of Malaysia, Labuan Financial Services Authority or any other relevant authority.



- S** 14.10.9 Reporting institutions are exempted from obtaining a copy of the Certificate of Incorporation or Constitution and from verifying the identity of directors and shareholders of the legal person which fall under the following categories:
- (a) public listed companies or corporations listed in Bursa Malaysia;
  - (b) foreign public listed companies:
    - (i) listed in recognised exchanges; and
    - (ii) not listed in higher risk countries;
  - (c) foreign financial institutions that are not from higher risk countries;
  - (d) an authorised person under the FSA and the Islamic Financial Services Act 2013 (i.e. any person that has been granted a licence or approval);
  - (e) persons licensed or registered under the Capital Markets and Services Act 2007;
  - (f) licensed entities under the Labuan Financial Services and Securities Act 2010 and the Labuan Islamic Financial Services and Securities Act 2010;
  - (g) prescribed institutions under the Development Financial Institutions Act 2002; or
  - (h) licensed entities under the Money Services Businesses Act 2011.
- S** 14.10.10 Notwithstanding the above, reporting institutions are required to identify and maintain information relating to the identity of the directors and shareholders of legal persons referred to in paragraph 14.10.9 (a) to (h) through a public register, other reliable sources or based on information provided by the customer.
- G** 14.10.11 Reporting institutions may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

### ***Legal Arrangements***

- S** 14.10.12 For customers that are legal arrangements, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

- S** 14.10.13 Reporting institutions are required to identify the customer and verify its identity through the following information:
- (a) name, legal form and proof of existence, such as trust deed or equivalent document, the unique identifier such as tax identification number or equivalent, or any reliable references to verify the identity of the customer;
  - (b) the powers that regulate and bind the customer as well as the names of relevant persons having a Senior Management position; and
  - (c) the address of the trustee's registered office and if different, a principal place of business.
- S** 14.10.14 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:
- (a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), 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 the chain of control/ownership); or
  - (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.
- S** 14.10.15 Reporting institutions are required to take measures to ensure that trustees or persons holding equivalent positions in similar legal arrangements disclose their status when, in their function, establishing business relations or carrying out any or an occasional transaction.
- G** 14.10.16 Reporting institutions may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.
- S** 14.10.17 Where reliance is placed on third parties under paragraph 14.10.16, reporting institutions are required to comply with paragraph 16 on Reliance on Third Parties.

### ***Clubs, Societies and Charities***

- S** 14.10.18 For customers that are clubs, societies or charities, reporting institutions shall conduct the CDD requirements applicable for legal persons or legal arrangements, as the case may be, and require the customers to furnish the relevant identification documents including Certificate of Registration and other constituent documents. In addition, reporting institutions are required to identify and verify the office bearer or any person authorised to represent the club, society or charity, as the case may be.

- S** 14.10.19 Reporting institutions are also required to take reasonable measures to identify and verify the beneficial owners of the clubs, societies or charities.
- S** 14.10.20 Where there is any doubt as to the identity of persons referred to under paragraphs 14.10.18 and 14.10.19, the reporting institution shall verify the authenticity of the information provided by such person with the Registrar of Societies, Labuan Financial Services Authority, Companies Commission of Malaysia, *Bahagian Hal Ehwal Undang-Undang, Jabatan Perdana Menteri* or any other relevant authority.

### ***Delayed Verification***

- G** 14.10.21 In certain circumstances where the ML/TF/PF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the reporting institution may complete verification after the establishment of the business relationship to allow some flexibilities for its customer or beneficial owner to furnish the relevant documents.
- S** 14.10.22 Where delayed verification applies, the following conditions must be satisfied:
- (a) this occurs as soon as reasonably practicable;
  - (b) the delay is essential so as not to interrupt the reporting institution's normal conduct of business;
  - (c) the ML/TF/PF risks are effectively managed; and
  - (d) there is no suspicion of ML/TF/PF.
- S** 14.10.23 The term "reasonably practicable" under paragraph 14.10.22(a) shall not exceed ten working days or any other period as may be specified by the competent authority.
- S** 14.10.24 Reporting institutions are required to adopt risk management procedures relating to the conditions under which the customer may utilise the business relationship prior to verification, and procedures to mitigate or address the risk of delayed verification.
- G** 14.10.25 The measures that reporting institutions may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.

## **14.11 Enhanced CDD**

- S** 14.11.1 Reporting institutions are required to perform enhanced CDD where the ML/TF/PF risks are assessed as higher risk. An enhanced CDD, shall include at least, the following:
- (a) obtaining CDD information under paragraph 14.10;

- (b) obtaining additional information on the customer and beneficial owner (e.g. volume of assets and other information from commercial or public databases);
- (c) enquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and
- (d) obtaining approval from the Senior Management of the reporting institution before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office.

- G** 14.11.2 In addition to paragraph 14.11.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF/PF risks identified:
- (a) obtaining additional information on the intended level and nature of the business relationship;
  - (b) where relevant, obtain additional information on the beneficial owner of the beneficiaries (for example, occupation, volume of assets, information available through commercial or public databases); and
  - (c) enquiring on the reasons for intended or performed transactions.

## 14.12 On-Going Due Diligence

- S** 14.12.1 Reporting institutions are required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:
- (a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and
  - (b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.
- G** 14.12.2 In conducting on-going due diligence, reporting institutions may take into consideration the economic background and purpose of any transaction or business relationship which:
- (a) appears unusual;
  - (b) is inconsistent with the expected type of activity and business model when compared to the volume of transaction;
  - (c) does not have any apparent economic purpose; or
  - (d) casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

- S** 14.12.3 The frequency in implementing paragraph 14.12.1(a) under on-going due diligence and enhanced on-going due diligence shall be commensurate with the level of ML/TF/PF risks posed by the customer based on the risk profiles and nature of transactions.
- S** 14.12.4 Reporting institutions shall periodically review its on-going due diligence measures to ensure it remains relevant and effective for accurate customer risk profiles and proportionate risk-based measures.
- S** 14.12.5 In conducting enhanced on-going due diligence, reporting institutions are required to:
- (a) increase the number and timing of controls applied; and
  - (b) select patterns of transactions that need further examination.

#### **14.13 Existing Customer – Materiality and Risk**

- 14.13.1 Existing customers in this paragraph refer to those that are customers prior to the CDD obligations under section 16 of the AMLA becoming applicable to the reporting institution.
- S** 14.13.2 Reporting institutions are required to apply CDD requirements to existing customers on the basis of materiality and risk.
- S** 14.13.3 Reporting institutions are required to conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.
- G** 14.13.4 In assessing materiality and risk of the existing customer under paragraph 14.13.2, reporting institutions may consider the following circumstances:
- (a) the nature and circumstances surrounding the transaction including the significance of the transaction;
  - (b) any material change in the way the account or business relationship is operated; or
  - (c) insufficient information held on the customer or change in customer's information.

#### **14.14 Non Face-to-Face Business Relationship**

- G** 14.14.1 Reporting institutions may establish non face-to-face (non-FTF) business relationships with its customers.
- S** 14.14.2 Reporting institutions shall obtain approval from their Board prior to the implementation of non-FTF business relationships.

- S** 14.14.3 Reporting institutions must comply with any additional measures imposed on the implementation of non-FTF as deemed necessary by the competent authority.
- S** 14.14.4 Reporting institutions are required to be vigilant in establishing and conducting business relationships via electronic means, which includes mobile channel and online channel.
- S** 14.14.5 The Board shall set and ensure the effective implementation of appropriate policies and procedures to address any specific ML/TF/PF risks associated with the implementation of non-FTF business relationships, as well as operational and information technology risks.
- S** 14.14.6 Reporting institutions shall ensure and be able to demonstrate on a continuing basis that appropriate measures for identification and verification of the customer's identity through non-FTF are secure and effective. Measures for identification and verification shall be proportionate to the risk dimensions of non-FTF business relationship.
- G** 14.14.7 In relation to paragraph 14.14.6, where reference is made to face-to-face processes, this should mainly serve as a guide on the minimum expected baseline.
- S** 14.14.8 In relation to paragraph 14.14.6, reporting institutions shall take measures to identify and verify the customer's identity through any of the following:
- (a) establishing independent contact with the customer;
  - (b) verifying the customer's information against reliable and independent sources to confirm the customer's identity and identifying any known or suspected ML/TF/PF risks associated with the customer; or
  - (c) requesting, sighting and maintaining records of additional documents required to perform face-to-face customer verifications.
- G** 14.14.9 In relation to paragraph 14.4.6, reporting institutions may identify and verify a customer's identity by:
- (a) conducting video calls with the customer before establishing business relationship or allowing the customer to perform transactions;
  - (b) communicating with the customer at a verified residential or office address where such communication shall be acknowledged by the customer;

- (c) verifying the customer's information against a database maintained by relevant authorities including the National Registration Department or Immigration Department of Malaysia; telecommunication companies, sanctions lists issued by credible domestic or international sources in addition to the mandatory sanctions lists or social media platforms with a broad outreach; or
- (d) requesting to sight additional documents such as recent utility bills, bank statements, student identification or confirmation of employment.

**S** 14.14.10 Reporting institutions must ensure the systems and technologies developed and used for the purpose of establishing business relationships using non-FTF channels (including verification of identification documents) have capabilities to support an effective AML/CFT/CPF Compliance Programme.

#### **14.15 Failure to Satisfactorily Complete CDD**

**S** 14.15.1 Where a reporting institution is unable to comply with CDD requirements;

- (a) the reporting institution shall not open the account, commence business relations or perform any transaction in relation to a potential customer, or shall terminate business relations in the case of an existing customer; and
- (b) the reporting institution must consider lodging a suspicious transaction report under paragraph 19.

#### **14.16 CDD and Tipping-Off**

**S** 14.16.1 In cases where the 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, document the basis of not completing the CDD and immediately file a suspicious transaction report under paragraph 19.

**G** 14.16.2 Notwithstanding paragraph 14.16.1, the reporting institution may consider proceeding with the transaction itself for purposes of furthering any inquiry or investigation of the ML/TF/PF suspicion.

#### **14.17 Customer Due Diligence Guidance**

**G** 14.17.1 Reporting institutions may refer to guidance and templates provided in parts C and D of this policy document in implementing the CDD and risk profiling requirements.

## **14A Customer Due Diligence: Licensed Casino**

### **14A.1 When CDD is required**

- S** 14A.1.1 A licensed casino is required to conduct CDD on the customer, the person conducting the transaction and junket, when engaging in any transaction equivalent to **RM10,000** and above. This includes circumstances where the transaction is carried out in a single transaction or in several transactions in a day that appear to be linked.
- S** 14A.1.2 For the purpose of paragraph 14A.1.1, “engaging in any transaction” includes:
- (a) all fund-in and fund-out transactions received and paid by the licensed casino, in cash or other forms that carry the same value;
  - (b) bank intermediated transaction prior to the customer, the person conducting the transaction or junket, being allowed to use the funds;
  - (c) request for payment to be made to any other person, by the customer, the person conducting the transaction and junket; and
  - (d) any other transaction specified by the competent authority.
- S** 14A.1.3 In relation to paragraph 14A.1.2(b), for bank intermediated transactions, a licensed casino is required to identify and maintain the information on the relationship:
- (a) between a customer and junket, and other fund-in remitter; and
  - (b) between a customer and junket, and beneficiary of fund-out transactions.
- S** 14A.1.4 In relation to paragraph 14A.1.2(c), for payment to other persons, a licensed casino is required to obtain the following information:
- (a) the relationship between the other person, and the customer and junket; and
  - (b) the purpose of payment to the other person.



## **14A.2 Specific CDD Measures**

### ***Junkets who are Individuals***

- S** 14A.2.1 In conducting CDD on junkets who are individuals, a licensed casino is required to conduct CDD as specified under paragraphs 14.1 to 14.9 and 14.10.1 to 14.10.2.

### ***Junkets which are Legal Persons***

- S** 14A.2.2 For junkets which are legal persons, a licensed casino is required to conduct CDD as specified under paragraphs 14.1 to 14.9 and 14.10.3 to 14.10.11.

## **14B Customer Due Diligence: Licensed Gaming Outlets**

### **14B.1 When CDD is required**

- S** 14B.1.1 Licensed gaming outlets are required to conduct CDD on the customer and the person conducting the transaction when a customer's winning is equivalent to **RM50,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions that appear to be linked.
- S** 14B.1.2 In addition to the requirements under paragraph 14B.1.1, licensed gaming outlets are required to obtain and check the accuracy of the following information:
- (a) ticket number;
  - (b) registration number and address of the outlet where the winning ticket was purchased; and
  - (c) winning amount.
- S** 14B.1.3 Licensed gaming outlets are required to conduct CDD on any other person specified by the winner when the winner requests for payment to such person's account for an amount equivalent to **RM50,000** and above.
- S** 14B.1.4 In addition to the requirement in paragraph 14B.1.3, licensed gaming outlets must obtain the following information:
- (a) the relationship between the winner and the other person specified by the winner; and
  - (b) the purpose for payment to the other persons specified by the winner.

## **14C Customer Due Diligence: Accountants, Company Secretaries and Lawyers**

### **14C.1 When CDD is required**

- S** 14C.1.1 Accountants and lawyers are required to conduct CDD, as specified under paragraphs 3.3 (a) and (d) respectively.
- S** 14C.1.2 Company secretaries are required to conduct CDD, as specified under paragraph 3.3 (b).

### **14C.2 Enhanced CDD**

- S** 14C.2.1 In relation to paragraphs 14C.1.1 and 14C.1.2, where nominee services are provided, such business relations must be subjected to enhanced CDD and enhanced on-going due diligence.
- S** 14C.2.2 For the purpose of paragraph 14C.2.1, nominee services refer to nominee shareholding, directorship or partnership services, where applicable.

## **14D Customer Due Diligence: Trust Companies**

### **14D.1 When CDD is required**

- S** 14D.1.1 Trust companies are required to conduct CDD, as specified under paragraph 3.3 (i).

### **14D.2 Enhanced CDD**

- S** 14D.2.1 In relation to paragraph 14D.1.1, where nominee services are provided, the business relations must be subjected to enhanced CDD and enhanced on-going due diligence.
- S** 14D.2.2 For the purpose of paragraph 14D.2.1, nominee services refer to nominee shareholding, directorship or partnership services, where applicable.

## **14E Customer Due Diligence: Dealers in Precious Metals or Precious Stones**

### **14E.1 When CDD is required**

- S** 14E.1.1 Dealers in precious metals or precious stones are required to conduct CDD on the customer and the person conducting the transaction when they engage in any cash transaction equivalent to **RM50,000** and above with the customer, or any other amount as may be specified by the competent authority. This includes:
- (a) transaction conducted as in a single transaction or through several transactions in a day that appear to be linked and across all branches of the reporting institution; and
  - (b) aggregate payments over a period of time for a single purchase.
- S** 14E.1.2 In relation to the requirements under paragraph 14E.1.1, CDD shall be conducted on both buying and selling of precious metals or precious stones from or to customers.

### **Notice to Customers**

- G** 14E.1.3 For the purpose of CDD, dealers in precious metals or precious stones may display at its business premises (both physical and digital) a notice, in the format provided below, informing its customers of the CDD requirements:

#### **Notice to Customer**

##### **(Dealers in precious metals or precious stones)**

Customer Due Diligence (CDD) is a requirement under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA). CDD shall be conducted on customers conducting cash transactions **equivalent to RM50,000 and above**. Please produce your identification document before making any cash transaction equivalent to RM50,000 and above.

#### **Notis kepada Pelanggan**

##### **(Peniaga logam berharga atau batu berharga)**

Pelaksanaan Usaha Wajar Pelanggan (*Customer Due Diligence/CDD*) adalah satu keperluan di bawah Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil daripada Aktiviti Haram 2001 (AMLA). Usaha Wajar Pelanggan akan dilaksanakan terhadap pelanggan yang melakukan transaksi tunai dengan **nilai bersamaan atau melebihi RM50,000**. Sila sediakan dokumen pengenalan anda sebelum menjalankan transaksi tunai dengan nilai bersamaan atau melebihi RM50,000.

## 14F Customer Due Diligence: Registered Estate Agents

### 14F.1 When CDD is required

- S** 14F.1.1 Registered estate agents are required to conduct CDD on both purchaser and seller, or landlord and tenant of a property.

#### ***Notice to Customers***

- G** 14F.1.2 For the purpose of CDD, registered estate agents may display at its business premises (both physical and digital) a notice, in the format provided below, informing its customers of the CDD requirements:

#### **Notice to Customer**

##### **(Registered estate agent)**

Customer Due Diligence (CDD) is a requirement under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA). CDD shall be conducted on **both purchaser and seller**, or **landlord and tenant** of a property. Please produce your identification document before making the transactions.

#### **Notis kepada Pelanggan**

##### **(Ejen Harta Tanah Berdaftar)**

Pelaksanaan Usaha Wajar Pelanggan (*Customer Due Diligence/CDD*) adalah satu keperluan di bawah Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil daripada Aktiviti Haram 2001 (AMLA). Usaha Wajar Pelanggan akan dilaksanakan terhadap **kedua-dua pembeli dan penjual**, atau **tuan tanah dan penyewa sesuatu harta tanah**. Sila sediakan dokumen pengenalan anda sebelum menjalankan transaksi tersebut.

## **14G Customer Due Diligence: Moneylenders**

### **14G.1 When CDD is required**

**S** 14G.1.1 Moneylenders are required to conduct CDD on the customer and the person conducting the transaction, when giving out financing equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions in a day that appear to be linked.

**S** 14G.1.2 In addition to paragraph 14G.1.1, moneylenders must also conduct CDD on a guarantor when an agreement between a reporting institution and a customer or borrower involves a guarantor.

#### ***Notice to Customers***

**G** 14G.1.3 For the purpose of CDD, moneylenders may display at its business premises (both physical and digital) a notice, in the format provided below, informing its customers of the CDD requirements:

#### **Notice to Customer**

##### **(Moneylenders)**

Customer Due Diligence (CDD) is a requirement under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA). CDD shall be conducted on customers with financing amount equivalent to RM3,000 and above within a day. Please produce your identification document before making the transactions.

#### **Notis kepada Pelanggan**

##### **(Pemberi Pinjam Wang)**

Pelaksanaan Usaha Wajar Pelanggan (*Customer Due Diligence/CDD*) adalah satu keperluan di bawah Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil daripada Aktiviti Haram 2001 (AMLA). Usaha Wajar Pelanggan akan dilaksanakan terhadap pelanggan dengan nilai pembiayaan bersamaan atau melebihi RM3,000 dalam satu hari. Sila sediakan dokumen pengenalan anda sebelum menjalankan transaksi tersebut.

## **14H Customer Due Diligence: Pawnbrokers**

### **14H.1 When CDD is required**

- S** 14H.1.1 Pawnbrokers are required to conduct CDD on the customer and the person conducting the transaction, when the pledge amount is equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions in a day that appear to be linked.

#### ***Notice to Customers***

- G** 14H.1.2 For the purpose of CDD, pawnbrokers may display at its business premises (both physical and digital) a notice, in the format provided below, informing its customers of the CDD requirements:

#### **Notice to Customer**

##### **(Pawnbrokers)**

Customer Due Diligence (CDD) is a requirement under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA). CDD shall be conducted on customers with pawn amount equivalent to RM3,000 and above within a day. Please produce your identification document before making the transactions.

#### **Notis kepada Pelanggan**

##### **(Pemegang Pajak Gadai)**

Pelaksanaan Usaha Wajar Pelanggan (*Customer Due Diligence/CDD*) adalah satu keperluan di bawah Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil daripada Aktiviti Haram 2001 (AMLA). Usaha Wajar Pelanggan akan dilaksanakan terhadap pelanggan dengan nilai pajakan bersamaan atau melebihi RM3,000 dalam satu hari. Sila sediakan dokumen pengenalan anda sebelum menjalankan transaksi tersebut.



## **15 Politically Exposed Persons (PEPs)**

### **15.1 General**

- S** 15.1.1 The requirements set out in this paragraph are applicable to all types of PEPs and family members or close associates of those PEPs.
- S** 15.1.2 In identifying individuals who fall within the definition of a close associate of a PEP, reporting institutions must take reasonable measures to determine the extent to which these individuals are directly engaged or involved in the activity of the PEP.

### **15.2 Foreign PEPs**

- S** 15.2.1 Reporting institutions are required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.
- S** 15.2.2 Upon determination that a customer or a beneficial owner under paragraph 15.2.1 is a foreign PEP, the requirements of enhanced CDD specified in paragraph 14.11 and enhanced on-going due diligence as specified in paragraph 14.12.5 must be conducted.

### **15.3 Domestic PEPs or person entrusted with a prominent function by an international organisation**

- S** 15.3.1 Reporting institutions are required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.
- S** 15.3.2 If the customer or beneficial owner is determined to be a domestic PEP or a person entrusted with a prominent function by an international organisation, reporting institutions are 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.
- S** 15.3.3 The assessment of the ML/TF/PF risks as specified under paragraph 15.3.2, shall take into account the profile of the customer under paragraph 10.6.2 on Risk Profiling.
- S** 15.3.4 The requirements on enhanced CDD as specified under paragraph 14.11 and enhanced on-going due diligence as set out under paragraph 14.12.5 must be conducted in respect of domestic PEPs or persons entrusted with a prominent function by an international organisation who are assessed as higher risk.

- G** 15.3.5 Reporting institutions may apply CDD measures similar to other customers for domestic PEPs or persons entrusted with a prominent function by an international organisation if the reporting institution is satisfied that the domestic PEPs or persons entrusted with a prominent function by an international organisation are not assessed as higher risk.
- G** 15.3.6 In assessing the ML/TF/PF risk level of the customer, beneficial owner or beneficiary identified as a family member or close associate of a domestic PEP or a person entrusted with prominent public function by an international organisation, reporting institutions may consider the following factors:
- (a) the family members or close associates have business interests related to the PEP's public functions (possible 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) country from which the family members or close associates originate or reside; or
  - (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/PF by the PEP.

#### 15.4 Sources of Information

- G** 15.4.1 Reporting institutions may refer to any of the following sources in identifying a PEP, a family member or a close associate of a PEP:
- (a) in-house or commercial database;
  - (b) risk-information or guidance shared by the competent authority, supervisory or regulatory authorities;
  - (c) public or open source information; or
  - (d) customer's self-declaration.
- G** 15.4.2 The examples of sources referred under paragraph 15.4.1 are not exhaustive and reporting institutions are encouraged to develop internal references in identifying PEPs, family members or close associates of PEPs.

## 15.5 Cessation of PEP status

- S** 15.5.1 Reporting institutions shall consider the following factors in determining whether the status of a PEP who no longer holds a prominent public function should cease:
- (a) the level of informal influence that the PEP could still exercise, even though the PEP no longer holds a prominent public function; and
  - (b) whether the PEP's previous and current functions, in official capacity or otherwise, are linked to the same substantive matters.

## **16 Reliance on Third Parties**

### ***Customer Due Diligence***

- G** 16.1 Reporting institutions may rely on third parties to conduct CDD or to introduce business.
- S** 16.2 The ultimate responsibility and accountability for CDD measures shall remain with the reporting institution relying on third parties.
- S** 16.3 Reporting institutions shall have internal policies and procedures in place to mitigate the risks when relying on third parties, including those from jurisdictions that have been identified as having strategic AML/CFT/CPF deficiencies that pose ML/TF/PF risks to the international financial system.
- S** 16.4 Reporting institutions are prohibited from relying on third parties located in higher risk countries that have been identified in accordance with paragraph 17.
- S** 16.5 The relationship between reporting institutions and the third parties relied upon by the reporting institutions to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. In placing reliance on the third party, the reporting institution, at a minimum:
- (a) must be able to obtain immediately the necessary information concerning CDD as required under paragraph 14; and
  - (b) must be reasonably satisfied that the third party:
    - (i) has an adequate CDD process;
    - (ii) has measures in place for record keeping requirements;
    - (iii) can provide the CDD information and provide copies of the relevant documentation immediately upon request; and
    - (iv) is properly regulated and subjected to AML/CFT/CPF supervision by the relevant supervisory authority.
- S** 16.6 Reporting institutions shall obtain an attestation from the third party to satisfy itself that the requirements in paragraph 16.5 have been met.
- G** 16.7 Reporting institutions may obtain written confirmation from the third party that it has conducted CDD on the customer or beneficial owner, as the case may be, in accordance with paragraph 14.

- G** 16.8 The requirements under paragraphs 16.1, 16.3 and 16.5 may be fulfilled if the reporting institution relies on a third party that is part of the same financial and/or DNFBP group, subject to the following conditions:
- (a) the group applies CDD, record keeping and AML/CFT/CPF programmes in line with the requirements in this policy document;
  - (b) the implementation of CDD, record keeping and AML/CFT/CPF programmes is supervised at a group level by the relevant authority; and
  - (c) any higher country risk is adequately mitigated by the group's AML/CFT/CPF policies.

***On-going Due Diligence***

- S** 16.9 Reporting institutions shall not rely on third parties to conduct on-going due diligence of its customers.

## 17 Higher Risk Countries

- S** 17.1 Reporting institutions are required to conduct enhanced CDD proportionate to the risk, on business relationships and transactions with any person from higher risk countries for which this is called for by the FATF or by the Government of Malaysia.
- S** 17.2 Notwithstanding the generality of paragraph 17.1, the enhanced CDD shall include any specific CDD measure as may be imposed by the FATF or by the Government of Malaysia.
- S** 17.3 Reporting institutions are required to apply appropriate countermeasures, proportionate to the risks, when called upon to do so by the FATF or by the Government of Malaysia.
- G** 17.4 For the purpose of paragraph 17.3, the countermeasures may include the following:
- (a) limiting business relationships or financial transactions with the identified country or persons located in the country concerned;
  - (b) maintaining a report with a summary of exposure to customers and beneficial owners from the country concerned and must be made available to the competent authority or relevant supervisory authorities upon request;
  - (c) conducting enhanced external audits, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or group, located in the country concerned; or
  - (d) conducting any other countermeasures as may be specified by the competent authority.
- S** 17.5 In addition to the above, where ML/TF/PF risks are assessed as higher risk, reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from other jurisdictions that have strategic AML/CFT/CPF deficiencies for which they have developed an action plan with the FATF.
- S** 17.6 For the purpose of requirements under paragraphs 17.1, 17.2, 17.3 and 17.5, reporting institutions shall refer to the FATF website:

<https://www.fatf-gafi.org>

## 18 Cash Threshold Report

### 18.1 General

- S** 18.1.1 Where the requirement of cash threshold report applies, reporting institutions are required to submit cash threshold reports to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

### 18.2 Definition

- S** 18.2.1 For the purpose of paragraph 18:
- (a) cash transactions refer to transactions involving physical currencies (domestic or foreign currency) and bearer negotiable instruments such as a bill of exchange, promissory note, bearer bond, traveller's cheque, cash cheque, money order and postal order. However, this does not include bank drafts, cheques, electronic transfers or fixed deposit rollovers or renewals; and
  - (b) cash transactions include transactions involving withdrawal of cash from accounts or exchange of bearer negotiable instruments for cash.

### 18.3 Applicability

- S** 18.3.1 The requirements for cash threshold reports are applicable to customers and person conducting the transaction in single or multiple cash transactions within the same account in a day for the amount equivalent to **RM25,000** and above.
- S** 18.3.2 Reporting institutions shall not offset the cash transactions against one another. Where there are deposit and withdrawal transactions, the amount must be aggregated. For example, a deposit of RM20,000 and a withdrawal of RM10,000 must be aggregated to the amount of RM30,000 and hence, must be reported as it exceeds the amount specified by Bank Negara Malaysia.
- S** 18.3.3 Transactions referred to under paragraph 18.3.1 include cash contra from an account to different account(s) transacted over-the-counter by any customer.

#### 18.4 Reporting of Cash Threshold Report

- S** 18.4.1 Reporting institutions are required to establish a reporting system for the submission of cash threshold reports to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.
- S** 18.4.2 The Compliance Officer of a reporting institution that has been granted access to the Financial Intelligence System (FINS) administered by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia must submit the cash threshold report through the following website:
- <https://fins.bnm.gov.my/>
- S** 18.4.3 Reporting institutions must ensure that the cash threshold report is submitted within five working days, from the date of the transaction.
- S** 18.4.4 Reporting institutions must ensure all required information specified in Appendix 4 are submitted and all submitted information are accurate and complete.
- S** 18.4.5 Submission of a cash threshold report does not preclude the reporting institution's obligation to submit a suspicious transaction report.



## **19 Suspicious Transaction Report**

### **19.1 General**

- S** 19.1.1 Reporting institutions are required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia whenever the reporting institution suspects or has reasonable grounds to suspect that the transaction or activity (including attempted or proposed), regardless of the amount:
- (a) appears unusual;
  - (b) has no clear economic purpose;
  - (c) appears illegal;
  - (d) involves proceeds from an unlawful activity or instrumentalities of an offence; or
  - (e) indicates that the customer is involved in ML/TF/PF.
- S** 19.1.2 Reporting institutions must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.
- S** 19.1.3 Reporting institutions must establish a reporting mechanism for the submission of suspicious transaction reports.

### **19.2 Reporting Mechanisms**

- S** 19.2.1 Reporting institutions are required to ensure that the designated branch or subsidiary compliance officer is responsible for channelling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.
- S** 19.2.2 Reporting institutions are required to have in place policies on the duration upon which internal suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe can be exceeded, where necessary.

- S** 19.2.3 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.
- S** 19.2.4 The Compliance Officer of a reporting institution that has been granted access to the FINS administered by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia must submit the suspicious transaction report through the following website:
- <https://fins.bnm.gov.my/>
- S** 19.2.5 For reporting institutions that have not been granted access to FINS, the Compliance Officer must submit the suspicious transaction report, using the specified reporting form as provided in Bank Negara Malaysia's AML/CFT website: <https://amlcft.bnm.gov.my/aml/cft-policies> through any of the following channels:
- Mail : Director  
Financial Intelligence and  
Enforcement Department  
Bank Negara Malaysia  
Jalan Dato' Onn  
50480 Kuala Lumpur  
(To be opened by addressee only)
- E-mail : [str@bnm.gov.my](mailto:str@bnm.gov.my)
- S** 19.2.6 The Compliance Officer must ensure that the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.
- S** 19.2.7 Reporting institutions must ensure that in the course of submitting the suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.

- S** 19.2.8 Reporting institutions must provide additional information and documentation as may be requested by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and must respond promptly to any further enquiries with regard to any report received under section 14 of the AMLA.
- S** 19.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism, including management of internal suspicious transaction reports, is operated in a secured environment to maintain confidentiality and preserve secrecy.
- G** 19.2.10 Where a suspicious transaction report has been lodged, reporting institutions may update or make a fresh suspicious transaction report as and when a new suspicion arises.

### 19.3 Triggers for Submission of Suspicious Transaction Report

- S** 19.3.1 Reporting institutions are required to establish internal criteria (“red flags”) to detect suspicious transactions.
- S** 19.3.2 Reporting institutions must consider submitting a suspicious transaction report when any of its customer’s transactions or attempted transactions fits the reporting institution’s description of “red flags”.
- G** 19.3.3 Reporting institutions may refer to Part E of this policy document for examples of transactions that may constitute triggers or any other examples that may be issued by the competent authority, regulatory bodies, SRBs and international organisations for the purpose of reporting suspicious transactions.

### 19.4 Internal Suspicious Transaction Reports

- S** 19.4.1 Reporting institutions must ensure that the Compliance Officer maintains a complete file on all internal suspicious transaction reports and any supporting documentary evidence regardless of whether such reports have been submitted.
- S** 19.4.2 Pursuant to paragraph 19.4.1, if no suspicious transaction reports are submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the internal suspicious transaction reports and the relevant supporting documentary evidence must be made available to the competent authority or relevant supervisory authority upon request.

## **20 Disclosure of Suspicious Transaction Reports, Cash Threshold Reports and Related Information**

- S** 20.1 Reporting institutions are prohibited from disclosing any suspicious transaction report, and where applicable, cash threshold reports, as well as any information related to these reports, in accordance with section 14A of the AMLA. This includes any information on the subject or counterparties reported on, such as personal identification, account details, transaction details, the suspected offence or suspicious activities reported on, and any other information contained in the report.
- S** 20.2 The prohibition under paragraph 20.1 does not apply where the exceptions under section 14A(3) of the AMLA apply.
- S** 20.3 Where the exceptions under section 14A(3) of the AMLA apply, reporting institutions must have the following measures in place:
- (a) a set of parameters on:
    - (i) the circumstances where disclosure is required;
    - (i) types of information that can be disclosed; and
    - (ii) to whom it can be disclosed;
  - (b) internal governance procedures to ensure that any disclosure is properly justified, duly authorised and managed in a controlled and secured environment;
  - (c) apprise all employees and intended recipients who are privy to the reports and related information to maintain confidentiality; and
  - (d) an effective audit trail is maintained in respect of the disclosure of such information.
- G** 20.4 For any disclosure of reports and related information pursuant to section 14A(3)(d) of the AMLA, reporting institutions may make a written application to the Director, Financial Intelligence and Enforcement Department, Bank Negara Malaysia for a written authorisation.
- S** 20.5 In making an application under paragraph 20.4, the reporting institution shall provide the following:
- (a) details and justification for the disclosure;
  - (b) details on the safeguards and measures in place to ensure confidentiality of information transmitted at all times;
  - (c) information on persons authorised by the reporting institution to have access to the reports and related information;
  - (d) any other documents or information considered relevant by the reporting institution; and
  - (e) any other documents or information requested or specified by Bank Negara Malaysia.

## 21 Record Keeping

- S** 21.1 Reporting institutions are required to keep the relevant records including any accounts, files, business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and beneficial owners, and the results of any analysis undertaken. The records maintained must remain up-to-date and relevant.
- S** 21.2 Reporting institutions must ensure that all relevant records relating to transactions which are kept are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
- S** 21.3 Reporting institutions are required to keep the records for at least six years following the completion of the transaction, the termination of the business relationship or after the date of the occasional transaction.
- S** 21.4 In situations where the records are subjected to on-going investigation or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.
- S** 21.5 Reporting institutions are required to retain the relevant records in a form that is admissible as evidence in court pursuant to the Evidence Act 1950, and make such records available to the competent authority or supervisory authorities and law enforcement agencies in a timely manner.

## **22 Management Information System**

- S** 22.1 Reporting institutions must have in place an adequate manual or electronic management information system (MIS) to complement its CDD process. The MIS is required to provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect irregularities and/or any suspicious activity.
- S** 22.2 The MIS shall be commensurate with the size, nature and complexity of the reporting institution's business operations and ML/TF/PF risk profile.
- S** 22.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomalies in transaction patterns, customer's risk profile and transactions exceeding any internally specified thresholds.
- S** 22.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems, agents and across all branches of the reporting institution.
- G** 22.5 The MIS may be integrated with the reporting institution's information system that contains its customer's normal transactions or business profile, which is accurate, up-to-date and reliable.

## 23 Targeted Financial Sanctions on Terrorism Financing

### 23.1 Definition and Interpretation

#### 23.1.1 For the purpose of paragraph 23,

“**customer**” includes “beneficial owner” and “beneficiary”.

“**Domestic List**” refers to names and particulars of specified entities as declared by the Minister of Home Affairs under the relevant subsidiary legislation made under section 66B(1) of the AMLA.

“**related party**” refers to:

- (a) a person related to the properties or funds that are wholly or jointly owned or controlled, directly or indirectly, by a specified entity; and
- (b) a person acting on behalf or at the direction of a specified entity.

“**UNSCR List**” refers to names and particulars of persons as designated by the United Nations Security Council (UNSC) or its relevant Sanctions Committee pursuant to the relevant United Nations Security Council Resolutions (UNSCR) and are deemed as specified entities by virtue of section 66C(2) of the AMLA.

### 23.2 General

- S** 23.2.1 Reporting institutions are required to keep updated with the relevant UNSCR relating to combating the financing of terrorism, which includes:
- (a) UNSCR 1267(1999), 1373(2001), 1988(2011), 1989(2011) and 2253(2015) which require sanctions against individuals and entities belonging or related to Taliban, ISIL (Da’esh) and Al-Qaida; and
  - (b) new UNSCR published by the UNSC or its relevant Sanctions Committee as published in the UN website.

### 23.3 Maintenance of Sanctions List

#### ***UNSCR List***

- S** 23.3.1 Reporting institutions are required to maintain a sanctions database on the UNSCR List.

- S** 23.3.2 Reporting institutions must ensure that the information contained in the sanctions database is updated and effected without delay upon the publication of the UNSC or its relevant Sanctions Committee's designation in the UN website.
- G** 23.3.3 Reporting institutions may refer to the Consolidated UNSCR List published in the following UN website:  
<https://www.un.org>
- S** 23.3.4 The UNSCR List shall remain in the sanctions database until the delisting of the specified entities by the relevant Sanctions Committee is published in the UN website.

***Domestic List***

- S** 23.3.5 Reporting institutions are required to keep updated with the Domestic List as and when published in the *Gazette*.
- S** 23.3.6 Reporting institutions are required to maintain a sanctions database on the Domestic List.
- S** 23.3.7 Reporting institutions must ensure that the information contained in the sanctions database is updated and effected without delay upon publication in the *Gazette*.
- G** 23.3.8 Reporting institutions may refer to the Domestic List published in the following website:  
<https://lom.agc.gov.my>
- S** 23.3.9 The Domestic List shall remain in the sanctions database until the delisting of the specified entities is published in the *Gazette*.

***Other requirements***

- S** 23.3.10 Reporting institutions must ensure that the information contained in the sanctions database is comprehensive and easily accessible by its employees at the head office, branch, subsidiary and where relevant, to the outsourced service providers or agents.
- G** 23.3.11 Reporting institutions may monitor and consolidate other countries' unilateral sanctions lists in their sanctions database.
- G** 23.3.12 Reporting institutions may also consider electronic subscription services in ensuring prompt updates to the sanctions database.



## 23.4 Sanctions Screening – Customers

- S** 23.4.1 Reporting institutions are required to conduct sanctions screening on existing, potential or new customers against the Domestic List and UNSCR List. Where applicable, screening shall be conducted as part of the CDD process and on-going due diligence.
- S** 23.4.2 For the avoidance of doubt, sanctions screening obligations apply to all customers and transactions regardless of any thresholds for CDD or features of a product or service.
- S** 23.4.3 Reporting institutions shall ensure reasonable measures are taken to adhere to sanctions screening requirements, including obtaining limited data points of the customers during on-boarding or conducting a transaction, to facilitate screening. At a minimum, reporting institutions shall obtain the following information:
- (a) full name;
  - (b) NRIC number or passport number or reference number of any other official documents; and
  - (c) date of birth of customers.
- S** 23.4.4 Reporting institutions are required to screen its entire customer database (including dormant accounts), without delay, for any positive name match against the:
- (a) Domestic List, upon publication in the *Gazette*; and
  - (b) UNSCR List, upon publication of the UNSC or its relevant Sanctions Committee's designation in the UN website.
- G** 23.4.5 When conducting the sanctions screening process, reporting institutions may perform name searches based on a set of possible permutations for each specified entity to prevent unintended omissions.
- S** 23.4.6 Reporting institutions shall maintain the records on the sanctions screening conducted and make such records available to competent authority or supervisory authority, upon request.

### ***Dealing with False Positives***

- S** 23.4.7 Reporting institutions are required to ascertain potential matches with the UNSCR List or the Domestic List are true matches to eliminate false positives.
- S** 23.4.8 Reporting institutions are required to make further inquiries for additional information and identification documents from the customer, counter-party or credible sources to assist in determining whether the potential match is a true match.

- G** 23.4.9 Reporting institutions may direct any query to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia to ascertain whether or not the customer is a specified entity, in the case of similar or common names.

### 23.5 **Related Parties**

- S** 23.5.1 Reporting institutions shall undertake due diligence on related parties.
- S** 23.5.2 In undertaking due diligence on the related parties, reporting institutions are required to examine and analyse past transactions of the specified entities and related parties, and maintain records on the analysis of these transactions.
- G** 23.5.3 In ascertaining whether an entity is owned or controlled by a specified entity, reporting institutions may refer to the definition of “beneficial owner” in paragraph 6.2, and requirements under paragraph 14 in relation to CDD on beneficial owners.

### 23.6 **Freezing, Blocking and Rejecting – Customers and Related Parties**

- S** 23.6.1 Reporting institutions are required to conduct the following, immediately and without delay, upon determination and confirmation of a customer’s identity as a specified entity and/or related parties:
- (a) freeze the customer’s funds and properties; or
  - (b) block transactions (where applicable), to prevent the dissipation of the funds.
- S** 23.6.2 Reporting institutions are required to reject a potential customer, where there is a positive name match.
- S** 23.6.3 The freezing of funds and properties or blocking of transactions, as the case may be, shall remain in effect until the specified entity is removed from the Domestic List or UNSCR List in accordance with paragraphs 23.3.4 and 23.3.9.

#### ***Allowable Transactions***

- S** 23.6.4 Any dealings with frozen funds or properties, whether by the specified entity, related party or any interested party, requires prior written authorisation from the Minister of Home Affairs.
- S** 23.6.5 The frozen funds and properties, may continue receiving deposits, dividends, interests, bonus or other benefits. However, such funds and benefits must remain frozen as long as the specified entity continues to be listed under the Domestic List and UNSCR List.

### ***Exemption for Basic and Extraordinary Expenditures***

- G** 23.6.6 Reporting institutions may advise the specified entity, a related party or any interested party of the frozen funds or properties, or to the blocked or rejected transactions, to make an application to the Minister of Home Affairs for exemptions on basic and extraordinary expenditures.
- S** 23.6.7 Reporting institutions shall only proceed with payments for basic and extraordinary expenditures upon receiving written authorisation from the Minister of Home Affairs.

## **23.7 Reporting on Positive Name Match**

### ***Reporting upon Determination of a Positive Name Match***

- S** 23.7.1 Reporting institutions are required to immediately report upon determination that they are in possession or in control of funds or properties, of any specified entity and/or related party, using the form attached in Appendix 5A or 5B, where applicable, to the:
- (a) Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and
  - (b) Inspector-General of Police.

### ***Periodic Reporting on Positive Name Match***

- S** 23.7.2 Reporting institutions that have reported positive name matches and are in possession or in control of frozen or blocked funds or properties of any specified entity and/or related party are required to report any changes to those funds, other financial assets and economic resources, using the form and at intervals as specified in Appendix 6A or 6B, where applicable.
- S** 23.7.3 Notwithstanding paragraph 23.7.2, reporting institutions are not required to submit periodic reporting on positive name matches involving customers who conduct one-off transactions and where the customer does not maintain an account with the reporting institution.

## **23.8 Reporting of Suspicious Transaction**

### ***On Related Transactions***

- S** 23.8.1 Reporting institutions are required to submit a suspicious transaction report, upon determination of any positive match or has reason to suspect that the account or transaction is related or linked to, or is used or intended to be used for or by any specified entity or related party.

- S** 23.8.2 Reporting institutions are also required to submit a suspicious transaction report on any attempted transactions undertaken by specified entity or related party.

***On Name Match with Other Unilateral Sanctions Lists***

- S** 23.8.3 Reporting institutions shall submit a suspicious transaction report if there is any positive name match with individuals or entities listed in other unilateral sanctions lists.

## 24 Targeted Financial Sanctions on Proliferation Financing and Other UN-Sanctions Regimes

### 24.1 General

24.1.1 This paragraph applies for the purposes of ensuring compliance with reporting institutions' obligations under Strategic Trade Act 2010 (STA), Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 and Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing<sup>8</sup> (Directive on TFS-PF) issued by the Strategic Trade Controller, Ministry of Investment, Trade and Industry in April 2018, as may be amended or superseded from time to time.

### 24.2 Definition and Interpretation

24.2.1 For the purpose of paragraph 24,

**“customer”** includes “beneficial owner” and “beneficiary”.

**“related party”** refers to:

- (a) a person related to the funds, other financial assets or economic resources that are wholly or jointly owned or controlled, directly or indirectly, by a designated person; and
- (b) a person acting on behalf or at the direction of a designated person.

**“UNSCR List”** refers to names and particulars of persons as designated by the UNSC or its relevant Sanctions Committee and are deemed as designated persons under the relevant STA subsidiary legislation.

### 24.3 Maintenance of Sanctions List

**S** 24.3.1 Reporting institutions are required to keep updated with the list of countries and persons designated as restricted end-users and prohibited end-users under the STA, in accordance with the relevant UNSCR relating to prevention of proliferation of weapons of mass destruction (WMD) as published in the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee.

---

<sup>8</sup> Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF) under the Strategic Trade Act 2010, Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 and Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010

- S** 24.3.2 Reporting institutions are also required to keep updated with the list of designated countries and persons under the STA in accordance with the relevant UNSCRs relating to upholding of peace and security, through prevention of armed conflicts and human rights violations, as published on the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee.
- S** 24.3.3 Reporting institutions are required to maintain a sanctions database on the UNSCR List.
- S** 24.3.4 Reporting institutions must ensure that the information contained in the sanctions database is updated and effected without delay upon publication of the UNSC or its relevant Sanctions Committee's designation in the UN Website.
- G** 24.3.5 Reporting institutions may refer to the Consolidated UNSCR List published in the following UN website:
- <https://www.un.org>
- S** 24.3.6 The UNSCR List shall remain in the sanctions database until the delisting of the designated country or person by the UNSC or its relevant Sanctions Committee is published in the UN website.
- S** 24.3.7 Reporting institutions must ensure that the information contained in the sanctions database is comprehensive and easily accessible by its employees at the head office, branch, subsidiary, and where relevant, to the outsourced service providers or agents.
- G** 24.3.8 Reporting institutions may monitor and consolidate other countries' unilateral sanctions lists in their sanctions database.
- G** 24.3.9 Reporting institutions may also consider electronic subscription services in ensuring prompt updates to the sanctions database.

#### **24.4 Sanctions Screening – Customers**

- S** 24.4.1 Reporting institutions are required to conduct sanctions screening on existing, potential or new customers against the UNSCR List. Where applicable, screening shall be conducted as part of the CDD process and on-going due diligence.
- S** 24.4.2 For the avoidance of doubt, sanctions screening obligations applies to all customers and transactions regardless of any thresholds for CDD or features of a product or service.

- S** 24.4.3 Reporting institutions shall ensure reasonable measures are taken to adhere to sanctions screening requirements, including obtaining limited data points of the customers during on-boarding or conducting a transaction, to facilitate screening. At a minimum, reporting institutions shall obtain the following information:
- (a) full name;
  - (b) NRIC number of passport number or reference number of any other official documents; and
  - (c) date of birth of customers.
- S** 24.4.4 Reporting institutions are required to screen its entire customer database (including dormant accounts), without delay, for any positive name match against the UNSCR List, upon publication of the UNSC or its relevant Sanctions Committee's designation in the UN website.
- G** 24.4.5 When conducting the sanction screening process, reporting institutions may perform name searches based on a set of possible permutations for each designated person to prevent unintended omissions.
- S** 24.4.6 Reporting institutions shall maintain the records on the sanctions screening conducted and make such records available to competent authority or supervisory authority, upon request.

***Dealing with False Positives***

- S** 24.4.7 Reporting institutions are required to ascertain potential matches with the UNSCR List are true matches to eliminate false positives.
- S** 24.4.8 Reporting institutions are required to make further inquiries for additional information and identification documents from the customer, counter-party or credible sources to assist in determining whether the potential match is a true match.
- G** 24.4.9 Reporting institutions may direct any query to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia to ascertain whether or not the customer is a designated person, in the case of similar or common names.

**24.5 Related Parties**

- S** 24.5.1 Reporting institutions shall undertake due diligence on related parties.
- S** 24.5.2 In undertaking due diligence on the related parties, reporting institutions are required to examine and analyse past transactions of the designated persons and related parties, and maintain records on the analysis of these transactions.

- G** 24.5.3 In ascertaining whether an entity is owned or controlled by a designated person, reporting institutions may refer to the definition of “beneficial owner” in paragraph 6.2 and requirements under paragraph 14 in relation to customer due diligence on beneficial owners.

#### **24.6 Freezing, Blocking and Rejecting - Customers and Related Parties**

- S** 24.6.1 Reporting institutions are required to conduct the following, immediately and without delay, upon determination and confirmation of a customer’s identity as a designated person and/or related parties:
- (a) freeze the customer’s funds, other financial assets and economic resources; or
  - (b) block transactions (where applicable), to prevent the dissipation of the funds, other financial assets and economic resources.
- S** 24.6.2 Reporting institutions are required to reject a potential customer, when there is a positive name match.
- S** 24.6.3 The freezing of funds, other financial assets and economic resources or blocking of transactions, as the case may be, shall remain in effect until the designated country or person is removed from the UNSCR List in accordance with paragraph 24.3.6.

#### ***Allowable Transactions***

- S** 24.6.4 Any dealings with frozen funds, other financial assets or economic resources, whether by the designated country, person, identified related party or any interested party, requires prior written authorisation from the Strategic Trade Controller under the STA.
- S** 24.6.5 The frozen funds, other financial assets, or economic resources may continue receiving deposits, dividends, interests, bonuses or other benefits. However, such funds and benefits must remain frozen as long as the countries and persons continue to be listed under the UNSCR List.

#### ***Exemption for Basic and Extraordinary Expenditures***

- G** 24.6.6 Reporting institutions may advise the designated person, a related party or any interested party of the frozen funds, other financial assets or economic resources, or to the blocked or rejected transactions, to make an application to the Strategic Trade Controller under the STA for exemptions on basic and extraordinary expenditures.



- S** 24.6.7 Reporting institutions shall only proceed with the payments for basic and extraordinary expenditures upon receiving written authorisation from the Strategic Trade Controller under the STA.

***Exemption for Payments Due under Existing Contracts***

- G** 24.6.8 Reporting institutions may advise the designated person, related party or any interested party of the frozen funds, other financial assets or economic resources, or to the blocked or rejected transaction, to make an application to the Strategic Trade Controller under the STA to allow payments due under contracts entered into prior to the designation.

- S** 24.6.9 Reporting institutions shall only proceed with the payments due under existing contracts upon receiving prior written authorisation from the Strategic Trade Controller under the STA.

**24.7 Reporting on Positive Name Match**

***Reporting upon Determination of a Positive Name Match***

- S** 24.7.1 Reporting institutions are required to immediately report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia on any detection, freezing, blocking or rejection actions undertaken with regard to any identified funds, other financial assets and economic resources or transactions, using the form attached in Appendix 5A or 5B, where applicable.

***Periodic Reporting on Positive Name Match***

- S** 24.7.2 Reporting institutions that have reported positive name matches and are in possession or in control of frozen or blocked funds, other financial assets or economic resources of any designated person and/or related party are required to report any changes to those funds, other financial assets and economic resources using the form and at intervals specified in Appendix 6A or 6B, which applicable.
- S** 24.7.3 Notwithstanding paragraph 24.7.2, reporting institutions are not required to submit period reporting on positive name matches involving customers who conduct one-off transactions and where the customer does not maintain an account with the reporting institution.

## 24.8 Reporting of Suspicious Transactions

### ***On Related Transactions***

- S** 24.8.1 Reporting institutions are required to submit a suspicious transaction report upon determination of any positive match or has reason to suspect that the account or transaction is related or linked to, or is used or intended to be used for or by any designated country, person or related party.
- S** 24.8.2 Reporting institutions are also required to submit a suspicious transaction report on any attempted transaction undertaken by designated countries, persons or related parties.

### ***On Name Match with Other Unilateral Sanctions Lists***

- S** 24.8.3 Reporting institutions shall submit a suspicious transaction report if there is any positive name match with individuals or entities listed in other unilateral sanctions lists.

### ***Imposition of New Measures***

- S** 24.9 In the event the UNSC or its relevant Sanctions Committee imposes new measures relating to the prevention of PF or proliferation of WMD, reporting institutions are required to adhere to such measures as specified by the Strategic Trade Controller under the STA.

## **25 Other Reporting Obligations**

- S** 25.1 Reporting institutions are required to submit the following reports to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, as and when applicable:
- (a) Data and Compliance Report issued by Bank Negara Malaysia; and
  - (b) any other report as may be specified by Bank Negara Malaysia.

# **PART C**

# **GLOSSARY, TEMPLATES AND**

# **FORMS**

## APPENDIX 1 Glossary

No	Abbreviation	Description
1.	AMLA	Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001
2.	AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
3.	CDD	Customer Due Diligence
4.	CO	Compliance Officer
5.	CRP	Customer Risk Profiling
6.	CSC	Club, Societies and Charities
7.	CTR	Cash Threshold Report
8.	CPF	Counter Proliferation Financing
9.	Directive on TFS-PF	Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing
10.	DNFBPs	Designated Non-Financial Businesses and Professions
11.	DPMS	Dealers in Precious Metals or Precious Stones
12.	EDD	Enhanced Customer Due Diligence
13.	FATF	Financial Action Task Force
14.	FATF Recommendations	FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation
15.	FINS	Financial Intelligence System
16.	FSA	Financial Services Act 2013
17.	GLCs	Government-Linked Companies
18.	MIS	Management Information System
19.	ML/TF	Money Laundering and Terrorism Financing
20.	NCC	National Coordination Committee to Counter Money Laundering
21.	Non-FTF	Non Face-to-Face
22.	NRIC	National Registration Identity Card
23.	ODD	On-going Due Diligence
24.	PEPs	Politically Exposed Persons
25.	PF	Proliferation Financing
26.	RBA	Risk-Based Approach
27.	SRB	Self-Regulatory Body
28.	STA	Strategic Trade Act 2010
29.	STR	Suspicious Transaction Report
30.	TFS	Targeted Financial Sanctions
31.	TFS-PF	Targeted Financial Sanctions Relating to Proliferation Financing
32.	UN	United Nations
33.	UNSC	United Nations Security Council
34.	UNSCR	United Nations Security Council Resolutions
35.	WMD	Weapons of Mass Destruction

## APPENDIX 2 Definition of Small-sized Reporting Institutions

Reporting institutions that satisfy the below criteria are subject to the application of simplification or exemption of Compliance Programme requirements, pursuant to paragraph 11.1 of this policy document.

Sector		Criteria
<ul style="list-style-type: none"> <li>Non-bank Financial Institutions</li> <li>Moneylenders</li> <li>Pawnbrokers</li> <li>Trust Companies</li> </ul>		<ul style="list-style-type: none"> <li>Total annual sales turnover of less than RM 3 million; <b>AND</b></li> <li>Total number of employees less than 30.</li> </ul>
<ul style="list-style-type: none"> <li>Dealers in Precious Metals or Precious Stones (DPMS)</li> </ul>	<ul style="list-style-type: none"> <li>Companies or businesses carrying on retail business</li> </ul>	<ul style="list-style-type: none"> <li>Total annual sales turnover of less than RM 10 million; <b>AND</b></li> <li>Total number of employees less than 30.</li> </ul>
	<ul style="list-style-type: none"> <li>Companies or businesses carrying on wholesale business, i.e. business to business dealings only</li> </ul>	<ul style="list-style-type: none"> <li>All such businesses are subject to the exemptions and simplification of AML/CFT/CPF Compliance Programme.</li> </ul>
<ul style="list-style-type: none"> <li>Lawyers</li> <li>Accountants</li> </ul>		<ul style="list-style-type: none"> <li>Number of practising certificate holders of 5 and below</li> </ul>
<ul style="list-style-type: none"> <li>Company Secretaries</li> </ul>		<ul style="list-style-type: none"> <li>5 members and below of a body prescribed by the Minister under section 235(2)(a) of Companies Act 2016; or</li> <li>5 persons and below licensed as company secretary by the Companies Commission of Malaysia; or</li> <li>5 persons and below with any combination of the above.</li> </ul>
<ul style="list-style-type: none"> <li>Registered Estate Agents</li> </ul>		<ul style="list-style-type: none"> <li>Total annual fees of less than RM 3 million</li> </ul>

## APPENDIX 3 Customer Due Diligence Form

Customer Due Diligence	
Identification and verification of a customer as required under:	
<ul style="list-style-type: none"> <li>Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA); and</li> <li>Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for DNFBPs and NBFIs (AML/CFT/CPF and TFS for DNFBPs and NBFIs) policy document.</li> </ul>	
<b>Disclaimer:</b>	
<ul style="list-style-type: none"> <li>This document is intended for guidance on the implementation of CDD, TFS, CRP and EDD in complying with the AML/CFT/CPF and TFS requirements under the AMLA only. Reporting institutions may develop their own forms or checklists in consideration of the size, nature and complexity of the business operations.</li> <li>This document does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice.</li> <li>In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.</li> </ul>	

Date:

1) INDIVIDUAL			
Full Name			
NRIC/Passport No.			
Date of Birth			
Residential Address			
Town			
State			
Postcode		Country	
Mailing Address (if different from the above address)			
Town			
State			
Postcode		Country	
Nationality			
Occupation Type			
Name of Employer/Nature of Business (if self-employed)			
Contact Number (home/office/mobile)			
Purpose of Transaction			

2) For LEGAL PERSON	
Company/Business Name	
Business Registration No.	
Business Type	<input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Partnership <input type="checkbox"/> Limited Liability Partnership <input type="checkbox"/> Public Company <input type="checkbox"/> Private Limited Company <input type="checkbox"/> Trust <input type="checkbox"/> Club/Society/Charity <input type="checkbox"/> Other: _____

<b>Country of Incorporation/Registration</b>			
<b>Address of Registered Office (trustee for trust)</b>			
<b>Town</b>			
<b>State</b>			
<b>Postcode</b>		<b>Country</b>	
<b>Address of the Principal Place of Business (If different from above)</b>			
<b>Town</b>			
<b>State</b>			
<b>Postcode</b>		<b>Country</b>	
<b>Principle Business</b>			
<b>Contact No.</b>			
<b>Purpose of Transaction</b>			
<b>Name of Directors(s)/Partner(s)</b>			
<b>Name of Shareholder(s)/Beneficial Owner(s)</b>	<b>Name</b>	<b>Types of shares</b>	<b>Percentage</b>
<b>Name of Beneficial Owners through other means (e.g., Nominee shareholders etc.)</b>	<b>Name</b>	<b>Type of ownership/control/relationship</b>	
<b>Name of Senior Management</b>			

3) For LEGAL ARRANGMENT			
<b>Name</b>			
<b>Registration No.</b>			
<b>Type</b>	<input type="checkbox"/> Trust <input type="checkbox"/> Club/Society/Charity <input type="checkbox"/> Others: _____ (please specify)		
<b>Country of Registration</b>			
<b>Address of Registered Office (trustee for trust)</b>			
<b>Town</b>			
<b>State</b>			
<b>Postcode</b>		<b>Country</b>	
<b>Address of the Principal Place of activity (If different from above)</b>			
<b>Town</b>			
<b>State</b>			
<b>Postcode</b>		<b>Country</b>	
<b>Principle activity</b>			
<b>Contact No.</b>			
<b>Purpose of Transaction</b>			
<b>Name of Directors(s)/Partner(s)</b>			
	<b>Name</b>	<b>ID</b>	<b>Address</b>
<b>Settlor</b>			
<b>Trustee</b>			
<b>Protector (if any)</b>			
<b>Beneficiary/class of beneficiary</b>			
<b>Other BO information</b>			



	<b>Relationship with trust:</b>
--	---------------------------------

**PERSON TRANSACTING ON BEHALF OF INDIVIDUAL/LEGAL PERSON/LEGAL ARRANGEMENT**

<b>Full Name</b>			
<b>NRIC/Passport No.</b>			
<b>Date of Birth</b>			
<b>Address</b>			
<b>Town</b>			
<b>State</b>			
<b>Postcode</b>		<b>Country</b>	
<b>Nationality</b>			
<b>Occupation</b>			
<b>Name of Employer/Nature of Business</b>			
<b>Contact Number (home/office/mobile)</b>			

<b>VERIFICATION (For Office Use)</b>	
Individual	Legal Persons/Legal Arrangement
<ul style="list-style-type: none"> <li>To verify and be satisfied with the identity of the customer or beneficial owner <u>through reliable and independent documentation, electronic data or any other measures</u> that the reporting institution deem necessary, for example: <ul style="list-style-type: none"> <li>Identity Card issued by Malaysian government</li> <li>Employee Identity Card issued by ministries and statutory bodies</li> <li>Foreign passport or identity card issued by the United Nations</li> <li>Documents issued by Malaysian government</li> <li>Biometric identification</li> <li>Organisation that maintains reliable and independent electronic data to verify customer's identity</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>To verify the identity of the customer through the following information/documents, for example: <ul style="list-style-type: none"> <li>Constitution/Certificate of Incorporation/Partnership</li> <li>Reliable references to verify the identity of customer;</li> </ul> </li> <li>To verify the identity of directors/shareholders with equity interest of more than twenty five percent/Partners through the following documents, for example, <ul style="list-style-type: none"> <li>Sections 58 and 78 Forms as prescribed by the Companies Commission of Malaysia or equivalent documents for Labuan companies or foreign incorporations</li> <li>Other equivalent documents for other types of legal person</li> <li>Authorisation for any person to represent the</li> <li>Letter of authority or directors' resolution.</li> </ul> </li> </ul>

### Targeted Financial Sanctions (TFS)

TFS as required under:

- Section 14(1)(c) of the AMLA;
- Paragraphs 23 and 24 of the AML/CFT/CPF and TFS for DNFBPs and NBFIs policy document; and
- Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF) under the Strategic Trade Act 2010, Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 and Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010.

Screen the name of customer against the MOHA<sup>9</sup> and UNSCR Sanctions List for Terrorism<sup>10</sup> and for Proliferation<sup>11</sup> and Other UN-Sanctions Lists

☐ **Positive** name match

☐ **Negative** name match

**If POSITIVE name match:**

- ☐ freeze the customer's funds, other financial assets and economic resources OR block the transaction (where applicable), if existing customer;
- ☐ reject a potential customer, if the transaction has not commenced;
- ☐ submit a suspicious transaction report (STR) to Bank Negara Malaysia; and
- ☐ report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and Inspector-General Police using the form attached in Appendix 5A, 5B, 6A or 6B where applicable.

<sup>9</sup> **MOHA: Ministry of Home Affairs**

<http://www.moha.gov.my/index.php/en/maklumat-perkhidmatan/membanteras-pembiayaan-keganasan2/senarai-kementerian-dalam-negeri>

<sup>10</sup> **UNSCR: United Nations Security Council Resolutions (Terrorism)**

[https://www.un.org/sc/suborg/en/sanctions/1267/aq\\_sanctions\\_list](https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list); and  
<https://www.un.org/sc/suborg/en/sanctions/1988/materials>

<sup>11</sup> **UNSCR: United Nations Security Council Resolutions (Proliferation of Weapons of Mass Destruction)**

<https://www.un.org/sc/suborg/en/sanctions/1718/materials>

### Customer Risk Profiling (CRP)

CRP as required under paragraph 10 of the AML/CFT/CPF and TFS for DNFBPs and NBFIs policy document.

In profiling the risk of its customers, reporting institutions must consider the following factors:

a) Customer Risk, e.g.

Is the customer or the beneficial owner a foreign or domestic PEP?	<input type="checkbox"/> Foreign PEP <i>*By default higher ML/TF/PF risks &amp; subject to EDD</i>
	<input type="checkbox"/> Domestic PEP
Nationality (resident or non-resident) of the customer/director/partner and shareholder/beneficial owner	<input type="checkbox"/> Malaysian <input type="checkbox"/> Foreigner
Is the customer/director/partner and shareholder/beneficial owner classified as High Net Worth individual?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Type of customer	<input type="checkbox"/> New customer <input type="checkbox"/> Repeating customer <input type="checkbox"/> Occasional/One-Off
Size and structure customer's business?	<input type="checkbox"/> Large and complex structure <input type="checkbox"/> Small and simple structure
Type of occupation/business	<input type="checkbox"/> Lower risk occupation/business <input type="checkbox"/> Higher risk occupation/business i.e. cash intensive business/occupation
Is there any adverse remark on the customer/company' background from research via public or commercial database such as Google?	<input type="checkbox"/> Yes Please state: _____ <input type="checkbox"/> No
Other consideration	

b) Geographical Risk, e.g.

What is the country of origin of the customer, location of business, branches, beneficial owner, beneficiaries or related parties?	<input type="checkbox"/> Low risk countries <input type="checkbox"/> Countries having strategic AML/CFT/CPF deficiencies <input type="checkbox"/> Countries subject to a FATF call to apply countermeasures
List of higher risk countries is available at: - <a href="http://www.fatf-gafi.org">http://www.fatf-gafi.org</a>	<i>*By default higher ML/TF/PF risk &amp; subject to EDD and countermeasures</i>
Other consideration	

c) Products/Services Risk, e.g.

Does the product/service offered provide anonymity to the customer?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the product/service offered commensurate with the profile of the customer?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the product/service offered involve complex and unusual transaction?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the customer require nominee services?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the company have nominee shareholder(s) or nominee director(s)? (for nominee service dispensed by lawyers, accountants and company secretaries)	<input type="checkbox"/> Yes <input type="checkbox"/> No
	<input type="checkbox"/> Yes

Does the product/service offered involve cross-border transactions?	<input type="checkbox"/> No
Other consideration	

d) Transaction and Delivery Channel Risk, e.g.

Mode of payment	<input type="checkbox"/> Bank transfer or cheques
	<input type="checkbox"/> Physical cash
Delivery Channel	<input type="checkbox"/> Face-to-face
	<input type="checkbox"/> Through agent/intermediaries
	<input type="checkbox"/> Non face-to-face
Other consideration	

Other factors that affect the customer's ML/TF/PF risk rating?
--

<b>Overall risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
---------------------------------	------------------------------	---------------------------------	-------------------------------

EDD as required under:

- ### Circumstances when EDD applies:

- Note:**

Individual name of higher risk customer/PEP

## Customer/PEP's role in Legal Person/Legal Arrangement, where relevant

Source of Fund/  
Source of Wealth

### Additional Information on Customer and Beneficial Owner

**For customer subject to EDD – To be approved by Senior Management of the Firm**

## Approval

- ☐ Approved  
☐ Not approved

Justification: \_\_\_\_\_

Name of Senior Management

**Position/Designation**

Date

## APPENDIX 4 Required Information in CTR

Element of CTR	Required Information
Account Transaction Details	<ul style="list-style-type: none"> <li>i. Transaction Type</li> <li>ii. Transaction Date</li> <li>iii. Transaction Amount (RM)</li> <li>iv. Transaction Amount (FC)*</li> </ul>
Customer Information	<p>Individual:</p> <ul style="list-style-type: none"> <li>i. Name</li> <li>ii. Gender</li> <li>iii. Nationality</li> <li>iv. NRIC/ Passport/Other ID*</li> <li>v. Date of Birth</li> <li>vi. Residential Address</li> <li>vii. Contact Number</li> <li>viii. Occupation</li> </ul> <p>Non-Individual:</p> <ul style="list-style-type: none"> <li>i. Business/ Company Name</li> <li>ii. Country of incorporation</li> <li>iii. BR No</li> <li>iv. Date of Incorporation</li> <li>v. Business Address</li> <li>vi. Contact Number (Office)</li> <li>vii. Nature of Business</li> </ul> <p><u>Signatory/Director/BO/Joint Accountholder</u></p> <ul style="list-style-type: none"> <li>i. Role</li> <li>ii. Name</li> <li>iii. Gender</li> <li>iv. Nationality</li> <li>v. NRIC/ Passport/Other ID*</li> <li>vi. Date of Birth</li> <li>vii. Residential Address</li> <li>viii. Contact Number</li> </ul> <p>Legal Arrangement:</p> <ul style="list-style-type: none"> <li>i. Trustee Name</li> <li>ii. Country of Establishment/Nationality</li> <li>iii. Date of Establishment/ Birth</li> <li>iv. Business/ Residential Address</li> <li>v. Contact Number (Office/Mobile)</li> <li>vi. Nature of Business/Employment Sector</li> </ul> <p><u>Settler/Protector/Beneficiary</u></p> <ul style="list-style-type: none"> <li>i. Role</li> <li>ii. Name</li> <li>iii. Gender</li> <li>iv. Nationality/Place of Incorporation</li> <li>v. NRIC/ Passport/Other ID*</li> <li>vi. Date of Birth/Establishment</li> <li>vii. Residential/Business Address</li> </ul>

	viii. Contact Number
Person Conducting Transaction	i. Name ii. Gender* iii. Nationality* iv. NRIC/Passport/Other ID* v. Date of Birth* vi. Address* vii. Contact Number*
Information of Beneficiaries	i. Name ii. Gender* iii. Nationality* iv. NRIC/Passport/Other ID* v. Date of Birth* vi. Residential Address* vii. Contact Number* viii. Occupation*

\* Field will only become required if the preceding fields are filled up.

## APPENDIX 5A Targeted Financial Sanctions Reporting (NBFIs) – Upon Determination

### REPORTING UPON DETERMINATION: ( ) TERRORISM FINANCING ( ) PROLIFERATION FINANCING ( ) OTHER UN-SANCTIONS REGIMES

Please tick (✓) at the appropriate bracket

ALL Sanctions Regimes		Terrorism Financing	
UNSCR No (If Available)	:	Type of Lists	: Domestic List ( ) UNSCR List ( )
Date of UN Listing	:	Circular/Gazette Reference No.	:
		Circular/Gazette Reference Date	:

No.	UNSCR Permanent Ref No/MOHA Reference No (e.g. KPI.001/KDN.I.01-2014)	Customer Name	Address	NRIC/Passport No.	Reporting Institution Name	Branch maintaining the account and facility	Account no.	Account/Facility/Financial Services Type	Date financial services given (DD/MM/YYYY)	Account/Facility Status (before designation)	Status of Account/facility/financial services status ( <i>after</i> designation) (e.g. frozen, expired/terminated, lapsed, etc.)	Date account/facility/financial services frozen/expire/terminated/lapsed, etc.) (DD/MM/YYYY)	Balance as at (for each account/facility/financial services) :			Related Parties	Remarks
													· Banking (CR)/	· Banking (DR)	Please state the type and value of property for loan accounts		
1.																	
2.																	

#### Reporting Institution Details

Reporting Institution Name : (please state all entities under the group if reporting done on group basis)  
Sector :  
Contact Person :  
Designation :  
Tel No. :  
E-mail :  
Reporting Date :

**Notes:** Please submit the completed form to -

Reporting for ALL sanctions regimes	In addition, reporting for TFS on Terrorism Financing
<b>Email</b>	<b>Address</b>
<b>Financial Intelligence and Enforcement Department, Bank Negara Malaysia</b>	<b>Ketua Polis Negara</b>
• Address : <a href="mailto:amlsanctions@bnm.gov.my">amlsanctions@bnm.gov.my</a>	(a) u/p: Pasukan Siasatan Jenayah Pengubahan Wang Haram dan Pembiayaan Keganasan Urusetia Pejabat Ketua Polis Negara, Tingkat 23, Menara 238, Jalan Tun Razak, 50400, Kuala Lumpur
• Subject : Reporting upon Determination (CTF/CPF/OSR*) *to specify relevant sanctions regime	(b) u/p : Bahagian E8,Cawangan Khas Tingkat 24, Menara 2, Ibu Pejabat Polis, Bukit Aman, 50560, Kuala Lumpur



## APPENDIX 5B Targeted Financial Sanctions Reporting (DNFBPs) – Upon Determination

### REPORTING UPON DETERMINATION: ( ) TERRORISM FINANCING ( ) PROLIFERATION FINANCING ( ) OTHER SANCTIONED REGIMES

Please tick (✓) at the appropriate bracket

ALL Sanctions Regimes				Terrorism Financing			
UNSCR No (If Available)	:			Type of Lists	:	Domestic List ( )	UNSCR List ( )
Date of UN Listing	:			Circular/Gazette Reference No.	:		
				Circular/Gazette Reference Date	:		

No.	UNSCR Permanent Ref No/MOHA Reference No (e.g. KPI.001/KDN.I.01-2014)	Customer Name	Address	NRIC/Passport No.	Reporting Institution Name	Branch providing the product/service/facility (if applicable)	Product/service /facility offered, e.g. pawn, loan	Date of funds received by the reporting institution (DD/MM/YY)	Customer status ( <i>before designation</i> ) e.g. existing/new on-boarding	Status of product/service facility ( <i>after designation</i> ) (e.g. frozen, terminated, etc.)	Date product/service/facility frozen/terminated etc.) (DD/MM/YY)	Value of product/service/facility	Please state the type and value of property for transactions relating to a property	Related Parties	Remarks
1.															
2.															
3.															
4.															

#### Reporting Institution Details

Reporting Institution Name :  
Sector :  
Contact Person :  
Designation :  
Tel No. :  
E-mail :  
Reporting Date :

**Notes:** Please submit the completed form to -

Reporting for ALL sanctions regimes	In addition, reporting for TFS on Terrorism Financing
Email	Address
Financial Intelligence and Enforcement Department, Bank Negara Malaysia	Ketua Polis Negara
• Address : <a href="mailto:sanctions@bnm.gov.my">sanctions@bnm.gov.my</a>	(c) u/p: Pasukan Siasatan Jenayah Pengubahan Wang Haram dan Pembiayaan Keganasan Urusetia Pejabat Ketua Polis Negara, Tingkat 23, Menara 238, Jalan Tun Razak, 50400, Kuala Lumpur
• Subject : Reporting upon Determination (CTF/CPF/OSR*) *to specify relevant sanctions regime	(d) u/p: Bahagian E8,Cawangan Khas Tingkat 24, Menara 2, Ibu Pejabat Polis, Bukit Aman, 50560, Kuala Lumpur

Please tick (✓) at the appropriate bracket

## Type of Lists : Domestic List ( ) UNSCR List ( )

## APPENDIX 6B Targeted Financial Sanctions Reporting (DNFBPs) - Periodic Reporting on Positive Name Match

PERIODIC REPORTING ON POSITIVE NAME MATCH: ( ) TERRORISM FINANCING ( ) PROLIFERATION FINANCING ( ) OTHER SANCTIONED REGIMES

Please tick (✓) at the appropriate bracket

Only for reporting on Terrorism Financing\*

Type of Lists : Domestic List ( ) UNSCR List ( )

No.	UNSCR Permanent Ref No/MOHA Reference No (e.g. KPL001/KDNJ01-2014)	Customer Name	Address	NRIC/Passport No.	Reporting Institution Name	Branch providing the product/service/facility (if applicable)	Product/service/facility offered, e.g. pawn, loan	Date of funds received by the reporting institution (DD/MM/YY)	Account/Facility Status (before designation)	Status of product/service facility (after designation) (e.g. frozen, terminated, etc.)	Date of funds received by the reporting institution (DD/MM/YY)	Value of product/service/facility	Transaction Details (line by line transaction)					New Account Balance as at: (DD/MM/YY)			Related Parties	Remarks
													Transaction No	Date (DD/MM/YY)	Type (CR/DR)	Amount (MYR)	Remarks	Banking (CR)	Banking (DR)	Please state the type and value of property for loan accounts		
1.																						
													1.									
													2.									
2.																						
3.																						

### Reporting Institution Details

Reporting Institution Name : (please state all entities under the group if reporting done on group basis)  
 Sector :  
 Contact Person :  
 Designation :  
 Tel No. :  
 E-mail :  
 Reporting Date :

### Notes:

Please submit the completed form to		Submission dates	
Financial Intelligence and Enforcement Department, Bank Negara Malaysia • Email Address : <a href="mailto:sanctions@bnm.gov.my">sanctions@bnm.gov.my</a> • Subject : Reporting upon Determination (CTF/CPF/OSR*) *to specify relevant sanctions regime		Terrorism Financing:	UNSCR List: Every 5 <sup>th</sup> January and 5 <sup>th</sup> July Domestic List: Every 15 <sup>th</sup> May and 15 <sup>th</sup> November
		Proliferation Financing & Other Sanctioned Regimes:	Only if there is any changes to the frozen funds (after first time reporting on positive name match) and latest by 15 January of the following calendar year

# **PART D GUIDANCE**

## **APPENDIX 7      Guidance on Application of Risk-Based Approach**

### **1.0      Introduction**

- 1.1 The risk-based approach (RBA) is central to the effective implementation of the anti-money laundering, countering financing of terrorism and countering proliferation financing (AML/CFT/CPF) preventive requirements and the FATF Recommendations. The focus on risk is intended to ensure a reporting institution is able to identify, assess and understand the money laundering, terrorism financing and proliferation financing (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) clarify the policy expectations in relation to the assessment of business-based and customer-based ML/TF/PF risk in applying the RBA. In the event a reporting institution has developed its own RBA, the reporting institution is expected to ensure its RBA achieves the outcomes as specified in this policy document and as further clarified in this Guidance.
- 1.3 This Guidance is **not** intended to supersede or replace any of the existing mandatory requirements on RBA that are provided in paragraph 10 of this policy document.
- 1.4 For reporting institutions under a group structure, the requirements on the RBA as provided for in the policy document and this Guidance are applicable to reporting institutions at the entity level, not group level, whether as a parent company in a group of corporations or subsidiary entity.
- 1.5 The RBA—
  - (a) recognises that the ML/TF/PF threats to a reporting institution vary across customers, countries, products and services, transactions and distribution channels;
  - (b) allows the reporting institution to apply appropriate policies, procedures, systems and controls to manage and mitigate the ML/TF/PF risks identified based on the nature, scale and complexity of the reporting institution's business and ML/TF/PF risk profile; and
  - (c) facilitates more effective allocation of the reporting institution's resources and internal structures to manage and mitigate the ML/TF/PF risks identified.
- 1.6 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 Institutional Risk Assessment and Customer Risk Profiling

### 2.1 The RBA entails two (2) assessments:

#### Institutional Risk Assessment (IRA)

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

- **Refer to requirements in paragraphs 10.2, 10.3, 10.4 and 10.5 in this policy document.**

- I. **Perform risk assessment** - A reporting institution is expected to 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 is expected to 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 is expected to establish and implement policies, controls and procedures to manage and mitigate the identified ML/TF/PF risks. Such measures should be sufficiently adequate to manage and mitigate the ML/TF/PF risks identified.

#### Customer Risk Profiling (CRP)

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

- **Refer to requirements in paragraph 10.6 in this policy document.**

- I. **Determine the risk parameters for customer risk profiling** - A reporting institution is expected to identify specific ML/TF/PF 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 IRA.
- II. **Conduct risk profiling on customers** – Based on the Customer Due Diligence (CDD) information obtained at point of on-boarding new customers, or ongoing CDD information obtained from existing customers, as the case may be, a reporting institution is expected to determine the ML/TF/PF risk profile of each customer (e.g. high, medium or low) by applying the risk parameters determined above, in order to determine the appropriate level of CDD (i.e. standard or enhanced) that is applicable in respect of each customer. The resulting ML/TF/PF risk

profile may also have a bearing on the frequency and intensity of on-going CDD that is applicable throughout the duration of the business relationship with the customer.

III. ***Apply customer risk management and mitigation control measures***

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

- 2.2 The RBA is expected to be tailored to the nature, scale and complexity of the reporting institution's business, size, structure and activities.
- 2.3 A reporting institution is expected to incorporate the RBA into its existing policies and procedures. All steps and processes in relation to the RBA for purpose of IRA and CRP are expected to be documented and supported by appropriate rationale and be subject to approval by senior management and/or the Board of Directors, as appropriate.
- 2.4 Recognising that ML/TF/PF risks evolve and are subject to change over time (arising from the emergence of new threats, introduction of new products/services, new technologies, expansion to new customer base etc.) a reporting institution is expected to understand that assessing and mitigating ML/TF/PF risks is not a static exercise. Therefore, a reporting institution is expected to periodically review, evaluate and update the RBA accordingly.
- 2.5 The outcome of the IRA and CRP complement each other. Therefore, to effectively implement the RBA–
  - (a) a reporting institution is expected to determine reasonable risk factors and parameters for the IRA and CRP; and
  - (b) over a period of time, data from the CRP may also be useful in updating the parameters of the IRA.

### **3.0 Institutional Risk Assessment (IRA)**

#### **A. Perform Risk Assessment**

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

- 3.2 The reporting institution is expected to evaluate the likelihood and extent of its ML/TF/PF risks at a macro level. When assessing the ML/TF/PF risks, a reporting institution is expected to consider all relevant risk factors that affect their business and operations, which may include the following:
- (a) Specific risk factors or high risk crimes that the reporting institution may consider for the purpose of identifying its ML/TF/PF risks;
  - (b) Type of customers;
  - (c) Geographic location of the reporting institution;
  - (d) Transactions and distribution channels offered by the reporting institution;
  - (e) Products and services offered by the reporting institution;
  - (f) Structure of the reporting institution; and
  - (g) Findings of the National Risk Assessment (NRA).
- 3.3 The ML/TF/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, a reporting institution is expected to make its own determination as to the risk weightage or materiality for each factor under consideration. These factors either individually or in combination, may increase or decrease potential ML/TF/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 of risk factors:
- (a) **Customers** – in conducting business transactions, the reporting institution is exposed to various types of customers that may pose varying degrees of ML/TF/PF risks. In analysing its customers' risk, a reporting institution may consider the non-exhaustive examples below:
    - *Exposure by type of customer, individuals and non-individuals (companies, businesses, legal arrangements, associations, etc.);*
    - *Exposure by nationality i.e. local or foreign;*
    - *Nature and type of business or occupation of the customers;*
    - *Exposure to foreign PEP customers;*
    - *Exposure to domestic PEP customers assessed as higher risk;*
    - *Exposure to customers related to PEPs assessed as higher risk;*
    - *Exposure to customers that are legal arrangements (e.g. trusts) and legal persons and the level of complexity of such legal structures;*
    - *Exposure to customers that authorise a proxy/agent to represent on their behalf;*
    - *Exposure to companies that have nominee shareholders or shares in bearer form;*
    - *Exposure to legal persons or arrangements that are personal asset holding vehicles;*



- *Exposure to customers originating from or domiciled in, and/or transactions conducted in or through higher risk countries (called by FATF or Government of Malaysia) or tax haven jurisdictions;*
- *Exposure to customers that provide vague or incomplete information about their proposed business activities during onboarding and resistant to provide additional information when queried;*
- *Exposure to customers with their beneficial owners or senior management appear in unilateral sanctions lists or adverse news;*
- *Exposure to customers engage in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding;*
- *Exposure to customers dealing with dual-use goods or goods subject to export control goods or complex equipment for which the person lacks technical background, or which is incongruent with their stated line of activity; and/or*
- *Exposure to customers affiliated with universities or research institutions are involved in the trading of dual-use goods or goods subject to export control.*

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

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

- (c) **Transactions and distribution channels** – A reporting institution has various modes of transaction and distribution of its products and services. Some of the modes of transaction and distribution channels may be more susceptible to ML/TF/PF risks. For example, products sold

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

- *Mode of distribution e.g. direct channel, or via agents, brokers, financial advisors, introducers, online or technology based transaction;*
- *Volume and frequency of non-face-to-face business relationships or transactions;*
- *Mode of payment e.g. cash-based transactions, e-payments;*
- *Cash intensive or other forms of anonymous transactions;*
- *Volume and frequency of transactions carried out in high risk areas or jurisdictions;*
- *Number of distribution channels located in high risk areas or jurisdictions;*
- *Exposure to cross-border transactions and/or transactions in high risk jurisdictions; and/or*
- *Transactions that involve possible companies with opaque ownership structures, front companies, e.g.: companies do not have high level of capitalisation or display other shell company indicators, including long period of dormancy followed by surge of activity.*

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

- *Nature of the products and services;*
- *Level of complexity of the products and services;*
- *Cash intensity related to the products and services;*
- *Market segments of the products and services;*
- *Products that are easily transferable to another party;*
- *Product's ownership not easily traceable to the owner;*
- *Product can be easily converted to cash or exchanged to another form;*
- *Customer can place deposit for a period of time for purchasing a product;*
- *Product can be easily transported or concealed;*
- *Product can be used as an alternative form of currency;*
- *Product that has high value in nature;*
- *Product can be purchased through non face-to-face channel;*
- *Allow use of virtual asset and other anonymous means of payment;*
- *Allow use of unusual means of payment e.g. high value items such as real estate, precious metals and precious stones;*
- *Services that enable clients to move funds anonymously; and/or*
- *Nominee services that may obscure ownership of legal person or legal arrangements;*
- *Transactions involve trading of dual-use goods or goods subject to export control; and/or*
- *Inadequate information and inconsistencies in trade documents and financial flows; such as names, companies, addresses, final destination, etc.*

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

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

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

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

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

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

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

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

**Example 1 for all sectors:**

<b>Risk Factor</b>	<b>Examples</b>	<b>Formulated Parameters</b>
Customer	Higher risk customer	<ul style="list-style-type: none"> <li>Number of higher risk customers more than 20% of total customer base for a year</li> <li>Number of politically exposed person (PEP) customers who are high risk is more than 5% of total customers</li> </ul>
	Local and foreign customers	<ul style="list-style-type: none"> <li>Percentage of local and foreign customer for a year</li> </ul>
	Companies with nominee shareholders or shares in bearer form	<ul style="list-style-type: none"> <li>Percentage of such companies against total non-individual customer base</li> </ul>
Transactions and Distribution Channels	Cash intensive or other forms of anonymous transactions	<ul style="list-style-type: none"> <li>High volume of cash transactions above RM50,000 within a year</li> <li>High volume of anonymous/proxy transactions exceeding RM50,000 per transaction within a year</li> </ul>
	Percentage of non-face-to-face transactions	<ul style="list-style-type: none"> <li>Non-face-to-face transactions exceeding 50% of total transactions</li> </ul>
	Frequency and amount of cash payments	<ul style="list-style-type: none"> <li>Cash transactions above RM10,000</li> </ul>
	Wide array of e-banking products and services	<ul style="list-style-type: none"> <li>More than 30% of new accounts are opened via internet, mail or telephone without prior relationship</li> </ul>
Findings of the NRA or any other risk assessments issued by	Sectors identified as highly vulnerable to ML/TF/PF risks	<ul style="list-style-type: none"> <li>Number of customers with occupation or nature of business from highly vulnerable sectors identified under the NRA or any other risk assessments</li> </ul>

relevant authorities		issued by relevant authorities.
-------------------------	--	------------------------------------

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

- 3.6 By applying all the risk factors and parameters in performing its risk assessment, a reporting institution should be able to determine the extent of ML/TF/PF risks that it is exposed to, on a quantitative and/or qualitative basis.
- 3.7 The outcome of the risk assessment would determine the level of ML/TF/PF risks the reporting institution is willing to accept (i.e. the reporting institution's risk appetite) and its appropriate risk rating. The risk appetite and risk rating will have a direct impact on the proposed risk management and mitigation policies, controls and procedures adopted by the reporting institution.
- 3.8 Apart from ensuring that the risk assessment is reflected in its policies and procedures, a reporting institution is also expected to justify the outcome of the risk assessment conducted. Reporting institutions are reminded of the requirement under the AMLA and this policy document to maintain proper records on any assessments and approvals by senior management and/or the Board of Directors on the ML/TF/PF risk assessments conducted to enable reviews to be conducted as and when it is requested by the competent authority or supervisory authority.

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

- 3.9 Once a reporting institution has identified and assessed the ML/TF/PF risks it faces after performing its risk assessment under paragraph 3A above, a reporting institution is expected to formulate and implement appropriate risk control measures in order to manage and mitigate those risks.
- 3.10 The intended outcome is that the mitigation measures and controls are commensurate with the ML/TF/PF risks that have been identified.
- 3.11 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 operations to other entities or at group level, where relevant.

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

- (a) restrict or limit financial transactions;
- (b) improved on-boarding processes for customers, including beneficial owners;
- (c) require additional internal approvals for certain segment of customers, transactions and products or services;
- (d) conduct regular training programmes for directors and employees on ML/TF/PF risks, typologies or increase resources where applicable;
- (e) improved controls for effective sanctions screening and transaction monitoring, including tailored risk-based measures to mitigate sanctions evasion, employment of technology-based screening, advanced technology to facilitate network analysis or system-based monitoring of transaction; and
- (f) employ biometric system for better customer verification.

## 4.0 Customer Risk Profiling (CRP)

### A. Determine the risk parameters for customer profiling

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

#### Example for all sectors:

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

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

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

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

- 4.2 Where relevant, a reporting institution may adopt similar risk factors and parameters that have been used for the assessment of the ML/TF/PF risks considered under the IRA.
- 4.3 The different CRP parameters considered within the customer, country or geographic, product or service and transaction or distribution channel risk factors, may either individually or in combination impact the level of risk posed by each customer.
- 4.4 Identifying one high risk indicator for a customer does not necessarily mean that the customer is high risk<sup>12</sup>. The CRP ultimately requires a reporting institution to draw together all risk factors, parameters considered, including patterns of transaction and activity throughout the duration of the business relationship to determine how best to assess the risk of such customers on an on-going basis.
- 4.5 Therefore, a reporting institution is expected to ensure that the CDD information obtained at the point of on-boarding and on-going due diligence is accurate and up to date.

<sup>12</sup> Except for high risk customer relationships that have already been prescribed, for example Foreign PEPs or customers from high risk jurisdiction identified by FATF.



## **B. Conduct risk profiling on customers**

- 4.6 Based on the processes under paragraph 4A above, a reporting institution is expected to formulate its own risk scoring mechanism for the purpose of risk profiling its customers, e.g. high, medium or low. This will assist the reporting institution to determine whether to apply standard or enhanced CDD measures in respect of each customer.
- 4.7 A reporting institution is expected to document the reason and basis for each risk profiling and risk scoring assigned to its customers.
- 4.8 Accurate risk profiling of its customers is crucial for the purpose of applying effective control measures. Customers who are profiled as higher risk should be subject to more stringent control measures including more frequent monitoring compared to customers rated as low risk.
- 4.9 While CDD measures and risk profiling of customers are performed at the inception of the business relationship, the risk profile of a customer may change once the customer has commenced transactions. On-going monitoring would assist in determining whether the transactions are consistent with the customer's last known information.

## **C. Apply customer risk management and mitigation control measures**

- 4.10 Based on the risk profiling conducted on customers, a reporting institution is expected to apply the risk management and mitigation procedures, systems and control measures proportionate to the customers' risk profile to effectively manage and mitigate such ML/TF/PF risks.
- 4.11 Non-exhaustive examples of risk management and mitigation control measures for CRP include:

- (a) Develop and implement clear customer acceptance policies and procedures;
- (b) Obtain, and where appropriate, verify additional information on the customer;
- (c) Update regularly the identification of the customer and beneficial owners,
- (d) Obtain additional information on the intended nature of the business relationship;
- (e) Obtain information on the source of funds and/or source of wealth of the customer;
- (f) Obtain information on the reasons for the intended or performed transactions;

- (g) Obtain the approval of senior management to commence or continue business relationship;
- (h) Conduct appropriate level and frequency of ongoing monitoring commensurate with risks identified;
- (i) Scrutinise transactions based on a reasonable monetary threshold and/or pre-determined transaction patterns; and
- (j) Impose transaction limit or set a certain threshold.

## **5.0 Continuous application of RBA**

- 5.1 The application of RBA is a continuous process to ensure that RBA processes for managing and mitigating ML/TF/PF risks are kept under regular review.
- 5.2 A reporting institution is expected to conduct periodic assessment of its ML/TF/PF risks (preferably every two years or sooner if there are any changes to the reporting institution's business model) taking into account the growth of the business, nature of new products/services and latest trends and typologies in the sector.
- 5.3 Through the periodic assessment, a reporting institution may be required to update or review either its IRA or CRP.
- 5.4 A reporting institution is expected to take appropriate measures to ensure that its policies and procedures are updated in light of the continuous risk assessments and ongoing monitoring of its customers.

## **6.0 Documentation of the RBA process**

- 6.1 A reporting institution is expected to ensure the RBA process is properly documented.
- 6.2 Documentation by the reporting institution is expected to include:

- (a) Process and procedures of the RBA;
- (b) Information that demonstrates higher risk indicators have been considered, and where they have been considered and discarded, reasonable rationale for such decision;
- (c) Analysis of the ML/TF/PF risks and conclusions of the ML/TF/PF threats and vulnerabilities to which the reporting institution is exposed to; and

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

- 6.3 In addition, on a case-by-case basis, a reporting institution is expected to document the rationale for any additional due diligence measures it has undertaken compared to the standard CDD approach.
- 6.4 The documented risk assessment is expected to be presented, discussed and deliberated with the senior management (including the CEO) and the Board of Directors of the reporting institution, where applicable.

## APPENDIX 8 Institutional Risk Assessment Template

Risk Assessment Template
<p>As required under:</p> <ul style="list-style-type: none"> <li>Section 19 of the AMLA; and</li> <li>Paragraphs 10.2, 10.3, 10.5 and 10.6 of the AML/CFT/CPF and TFS for DNFBPs and NBFIs.</li> </ul> <p>Please also refer to Guidance on Application of Risk-Based Approach Application.</p> <p><i>Disclaimer:</i></p> <ul style="list-style-type: none"> <li><i>This document is intended for guidance on the implementation of institutional risk assessment to assist the reporting institution to comply with the requirements of the AMLA only. Reporting institutions may develop their own template in consideration of the size, nature and complexity of the business operations.</i></li> <li><i>This document does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice.</i></li> <li><i>In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.</i></li> </ul>

In conducting risk assessment i.e. to identify, assess and understand their ML/TF/PF risks at the institutional level, the reporting institution may consider the following examples of risk factors:

### a) Overall Business Risk

Identifying higher risk business activities:

No	Main Business Activities	ML Risk	TF Risk	PF Risk	% Contribution to Total Business
1	<i>E.g. Selling of gold jewellerys including precious stones e.g. diamonds</i>	<i>E.g. High</i>	<i>E.g. High</i>	<i>E.g. High</i>	<i>E.g. 90%</i>

Firm's structure:

<b>No of Branches</b>	
<b>No of Agents</b>	
<b>No of Employees</b>	

Mapping of AMLA and other related requirements to respective division/department/job-scope:

No	AML Requirements	Responsible/Related Division/Department/Job Scope	Policies and Procedures?	Awareness Level & Training
1	<i>E.g. Customer Due Diligence</i>	<i>E.g. Front Counter Staff</i>	<i>E.g. Yes</i>	<i>E.g. Weak/Inadequate</i>

## b) Product and Services Risk

### i. Product

For each product, reporting institutions may consider the following risk factors:

No	Risk Factor	
1	Product can be easily transferable to another party	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Product's ownership not easily traceable to customer	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Product can be easily converted to cash or exchange to another form	<input type="checkbox"/> Yes <input type="checkbox"/> No
4	Customer can place deposit for a period of time for product purchase	<input type="checkbox"/> Yes <input type="checkbox"/> No
5	Product can easily be transported or concealed	<input type="checkbox"/> Yes <input type="checkbox"/> No
6	Product can be used as an alternative form of currency	<input type="checkbox"/> Yes <input type="checkbox"/> No
7	Product is high value in nature	<input type="checkbox"/> Yes <input type="checkbox"/> No
8	Customer can purchase product through non-face-to-face channel	<input type="checkbox"/> Yes <input type="checkbox"/> No
9	Allow use of virtual asset and other anonymous means of payment.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
10	Allow use of unusual mean of payment e.g. high value items such as real estate, precious metals and stones.	<input type="checkbox"/> Yes <input type="checkbox"/> No
11	Others (Please specify):	

<b>Product risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
---------------------------------	------------------------------	---------------------------------	-------------------------------

### ii. Services

For each service, reporting institutions may consider the following risk factors:

No	Risk Factor	
1	Services that allow deposit/payment from third-party/unknown parties	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Services that allow transfer of fund to third-party/unknown parties	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Services that allow cross-border fund transfer	<input type="checkbox"/> Yes <input type="checkbox"/> No
4	Services allow customer to deposit/transfer fund through the firm's client account	<input type="checkbox"/> Yes <input type="checkbox"/> No
5	Services include creation/setting up of complex legal arrangements	<input type="checkbox"/> Yes <input type="checkbox"/> No
6	Services that are capable of concealing beneficial ownership from competent authorities	<input type="checkbox"/> Yes <input type="checkbox"/> No
7	Services that provide nominee director/shareholders	<input type="checkbox"/> Yes

		<input type="checkbox"/> No
8	Services that provide anonymity in relation to the client's identity	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
9	Services are offered through use of agent or intermediary	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
10	Services that allow the use of shell companies or companies with ownership through nominee shares or bearer shares or control through nominee and corporate directors	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
11	Customer can acquire services through non face-to-face channel	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
12	Services allow use of virtual asset and other anonymous means of payment	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
13	Services allow use of unusual mean of payment e.g. high value items such as real estate, precious metals and stones	<input type="checkbox"/> Yes
		<input type="checkbox"/> No
14	Others (please specify):	

<b>Services risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
----------------------------------	------------------------------	---------------------------------	-------------------------------

<b>Overall product and services risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--	------------------------------	---------------------------------	-------------------------------

### c) Customer Risk

No	Risk Factors		Total	Percentage (%)	
1	Type of customers	Individual customers			
		Legal persons			
		Legal arrangements			
		Clubs, Societies and Charities			
		Others (Please specify):			
2	Type of occupation for individual customers	Salaried			
		Self-employed	Trading		
			Services		
			Others		
3	Nature and type of business of legal persons	Trading			
		Services			
		Cash intensive business (e.g. retail)			
		Others			
4	Risk Level (based on RI's own customer risk profiling)	Low risk			
		Medium risk			
		High risk			

5	Characteristics of customers	High net worth			
		Domestic PEPs			
		Foreign PEPs			
6	Structure/nature of customer	Legal persons which has complex structure or multiple layer of ownership			
		Legal persons which has nominee relationship			
		Customers that are cash intensive businesses			
		Others (please specify):			
7	Geographical location of customer	Domestic	All local customers		
			From within business area		
			Outstation customers		
		Foreign	All foreign customers		
			Customer from higher risk countries*		
8	Other factors (please specify):				

<b>Overall customer risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--	------------------------------	---------------------------------	-------------------------------

#### d) Geographical Location Risk

		Total	Percentage (%)
Local Headquarters and Branch Location	No of branches including headquarters located at/near tourist hotspots		
	No of branches including headquarters located at/near crime hotspots		
	No of branches including headquarters located at/near country's border		
	No of branches including headquarters located at/near country's entry points		
Foreign Branch Location	No of branches located in higher risk countries and/or countries of proliferation concern		

<b>Geographical location risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
---	------------------------------	---------------------------------	-------------------------------

**e) Transactions and Delivery Channel Risk**

No	Risk Factors		Total	Percentage (%)
1	Mode of delivery	Volume of non-face-to-face transactions e.g. online, agents		
		Value of non-face-to-face transactions (RM) e.g. online, agents		
2	Mode of payment	Cash	Volume of cash transaction (no. of cash transaction/total no. of all transaction)	
			Value of cash transaction (total value of cash transaction/total value of all transaction)	
			Average cash transaction (Total value of cash transaction/total no. of cash transaction)	
		Electronic payment	Volume of e-payment (no. of e-payment transaction/total no. of all transaction)	
			Value of e-payment transaction (total value of e-payment transaction/total value of all transaction)	
			Average e-payment transaction (Total value of e-payment transaction/total no. of e-payment transaction)	
3	Transaction location	Local	Fund received from outside your business area	
			Fund transferred to outside your business area	
		Foreign	Fund received from outside Malaysia	
			Fund transferred to outside Malaysia	
			Volume of transactions from/to higher risk countries	
			Value of transactions from/to higher risk countries	

<b>Transaction and delivery channel risk assessment:</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--	------------------------------	---------------------------------	-------------------------------



**f) Total Institutional ML/TF/PF Risk Level**

<b>Total Institutional ML/TF/PF Risk Level</b>	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
--	------------------------------	---------------------------------	-------------------------------

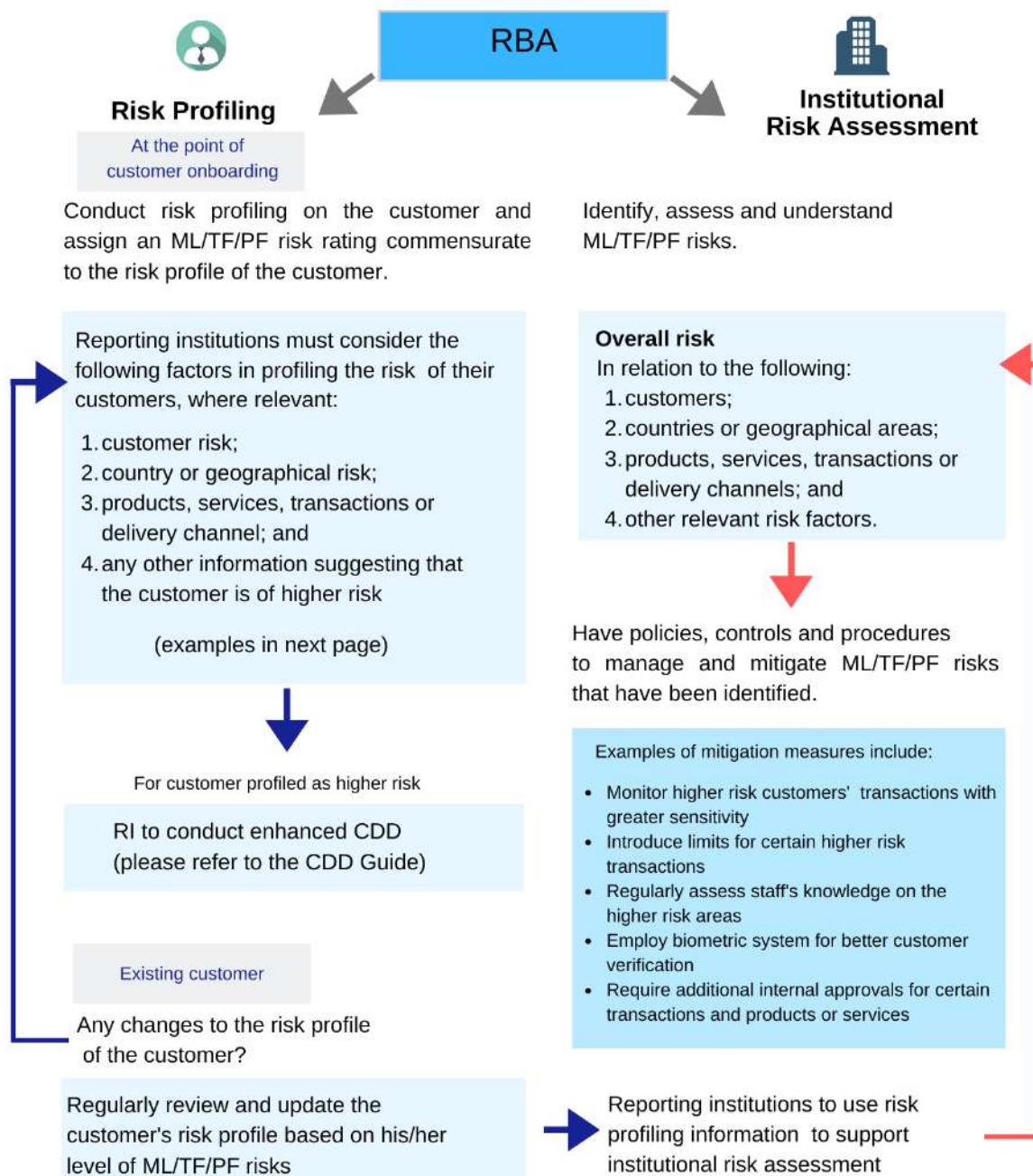
**g) Risk Control and Mitigation**

<b>No.</b>	<b>Identified High Risk ML/TF/PF Areas: Product/Services/Locations/Work- Process/Division/Customer or Group of Customers/Transaction Type/Delivery Channel</b>	<b>Proposed Control Measures – Policies, procedures and controls to manage and mitigate ML/TF/PF risks that have been identified</b>
1	<i>E.g. High exposure to higher risk customers</i>	<i>E.g. monitor higher risk customer's transactions with greater sensitivity</i>
2	<i>E.g. High exposure to politically exposed persons</i>	<i>E.g. employ technology-based screening for effective enhanced due diligence</i>
3	<i>E.g. Identified higher risk transactions</i>	<i>E.g. introduce limit for identified higher risk transactions</i>

## APPENDIX 9 Infographic on Risk Based Approach

### Risk Based Approach (RBA) Guide

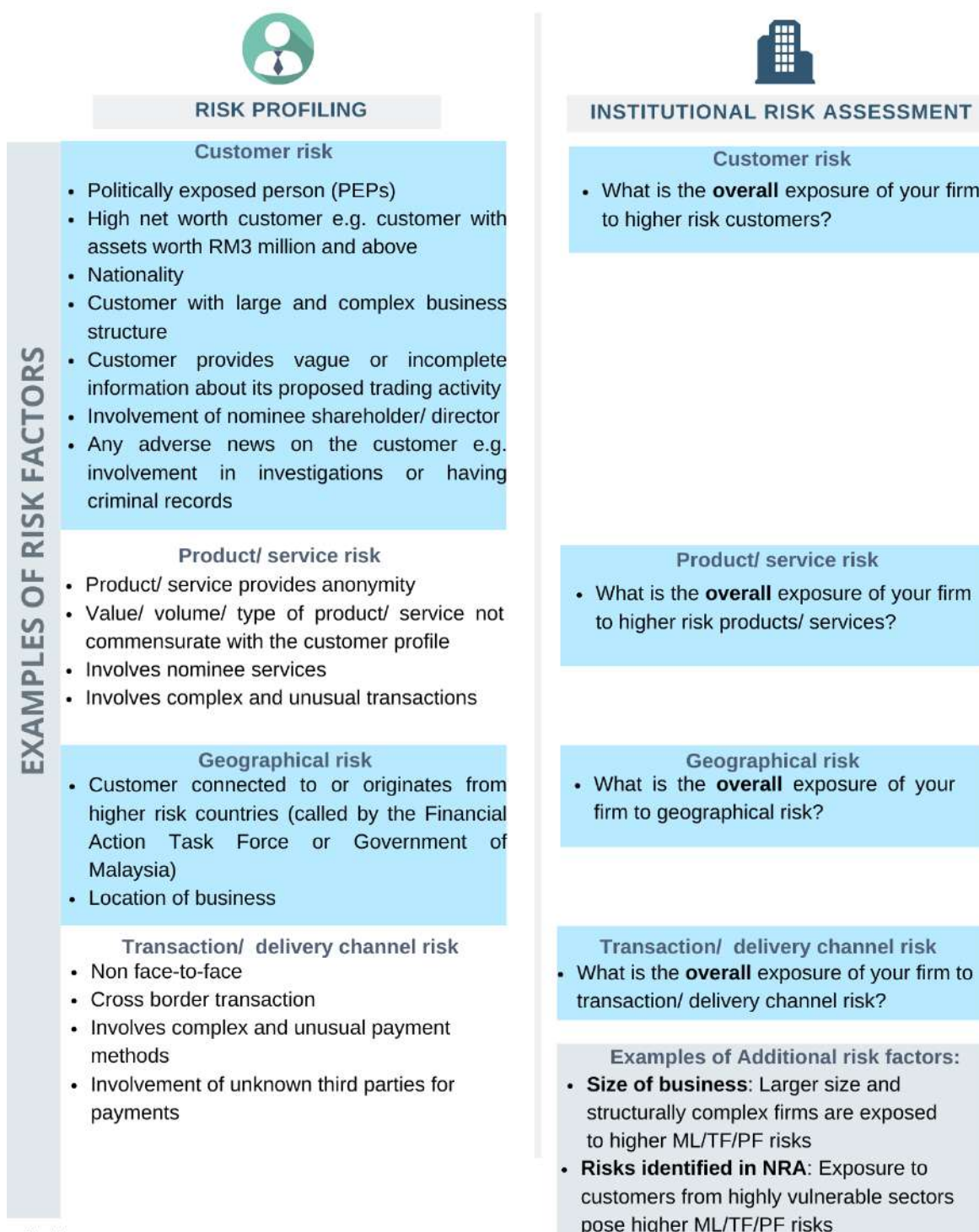
RBA is the process of identifying, assessing and understanding your firm's exposure to the money laundering/ terrorism financing/ proliferation financing (ML/TF/PF) risks and taking reasonable and appropriate anti-money laundering, countering financing of terrorism and countering proliferation financing (AML/CFT/CPF) measures effectively and efficiently to mitigate and manage the risks.



**Note:** Please refer to Paragraph 10 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) (AML/CFT/CPF and TFS for DNFBPs and NBFIs Policy Document)

## Risk Factors for Risk Profiling and Institutional Risk Assessment

The risk factors to be considered for risk profiling and institutional risk assessment are generally similar. The difference lies wherein that risk profiling looks at the individual customer, while institutional risk assessment looks at the risks of the firm/ business as a whole.



**Disclaimer:**

This document is intended for your general information only. It does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.



## APPENDIX 10 Infographic on Compliance Officer's Role and Responsibilities

### Compliance Officer (CO) Guide

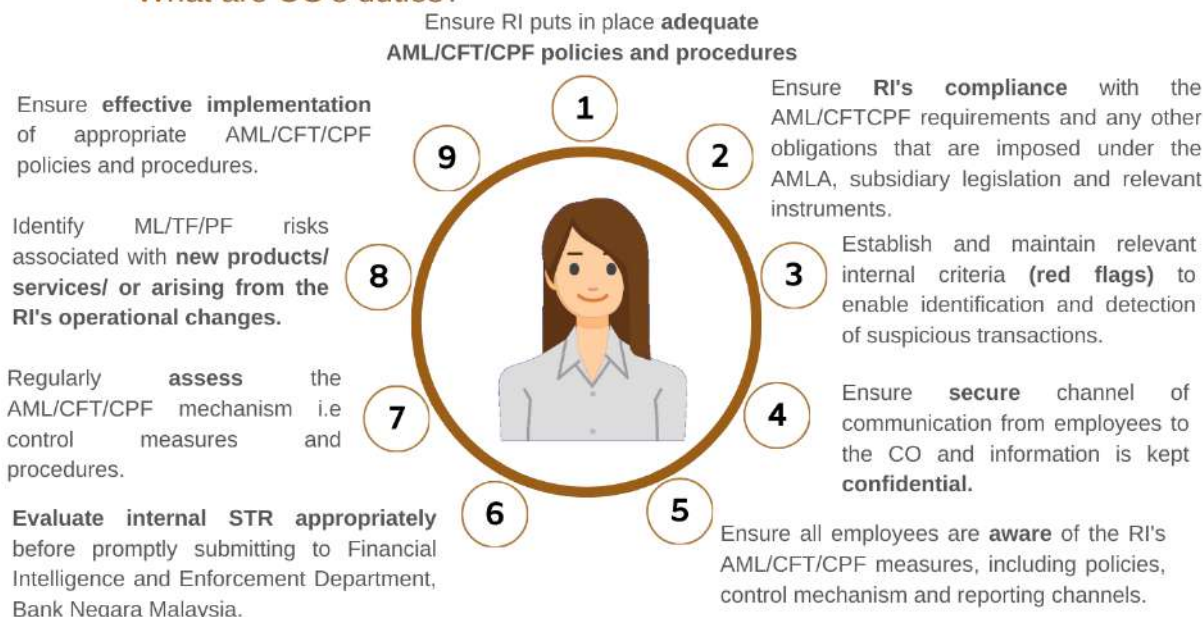
#### What is the role of CO?

- A CO is the **reference point** for anti-money laundering, counter financing, countering proliferation financing of terrorism (AML/CFT/CPF) matters within the reporting institution (RI).
- A CO is legally required to submit suspicious transaction reports (STRs) on behalf of the RI.

#### Criteria of CO

- Have sufficient stature, authority and seniority within the RI to participate and be able to effectively influence decisions relating to AML/CFT/CPF.
- Be fit and proper to carry out AML/CFT/CPF responsibilities effectively.
- Have necessary knowledge and expertise to effectively discharge roles and responsibilities.

#### What are CO's duties?



#### Appointment of CO

RIs are required to inform the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, in writing or by completing the form at <https://amlcft.bnm.gov.my/co> within ten working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, e-mail address and such other information as may be required.

E-mail: [fied@bnm.gov.my](mailto:fied@bnm.gov.my)

Mail: Director

Financial Intelligence and Enforcement Department  
Bank Negara Malaysia  
Jalan Dato' Onn  
50480 Kuala Lumpur

**Note:** Please refer to Paragraph 11 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs and NBFIs Policy Document)

#### Disclaimer:

This document is intended for your general information only. It does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.

## APPENDIX 11 Infographic on Customer Due Diligence

### Customer Due Diligence (CDD) Guide



#### When to conduct CDD?

##### 1. Establishing Business Relations

You are required to conduct CDD at the point of establishing a business relationship with your customer.

##### 2. Carrying Out Any or Occasional Transaction involving the Circumstances or Amount as Specified under Paragraphs 14A to 14H of the Policy Document



###### LICENSED CASINO

Any transaction equivalent to **RM10,000** and above. This includes circumstances where the transaction is carried out in a single transaction or several transactions in a day that appear to be linked.



###### LICENSED GAMING OUTLETS

Customer's winning equivalent to **RM50,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions that appear to be linked.



###### MONEYLENDERS

When giving out financing equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions, in a day that appear to be linked.



###### PAWNBROKERS

Pledge amount equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions, in a day that appear to be linked.



###### DEALERS IN PRECIOUS METALS OR PRECIOUS STONES

Any cash transaction equivalent to **RM50,000** and above with the customer, or any other amount as may be specified by the competent authority. This includes:

- Transaction conducted in a single transaction or through several transactions in a day that appear to be linked and across all branches of the reporting institution; and
- Aggregate payments over a period of time for a single purchase.



###### GATEKEEPERS (lawyers, accountants, company secretaries and trust companies)

When preparing or carrying out any of the Gazetted Activities for their clients (Please refer to the Policy Document for further details)



###### REGISTERED ESTATE AGENTS

To conduct CDD on both purchaser and seller, or landlord and tenant of the property

##### 3. Suspicion of money laundering, terrorism financing or proliferation financing (ML/TF/PF)

When you have any suspicion of ML/TF/PF regardless of the amount or thresholds

##### 4. Doubt

When you have any doubt about the accuracy or adequacy of previously obtained information on a particular customer

**Note:** Please refer to Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) (AML/CFT/CPF and TFS for DNFBPs and NBFIs Policy Document).



## What are specific information needed based on the customer type?

To comply with the CDD requirements, you are required to identify the customer and verify the customer's identity using reliable and independent documentation, electronic data or any other measures that you deem necessary.

1

### INDIVIDUAL CUSTOMER AND BENEFICIAL OWNER

- Name
- NRIC / Passport number
- Residential and mailing address
- Date of birth
- Nationality
- Occupation type
- Name of employer or nature of self-employment / nature of business
- Contact number
- Purpose of transaction

2

### LEGAL PERSON (LP), LEGAL ARRANGEMENT (LA) AND CLUB, SOCIETY AND CHARITY (CSC)

**Step 1** Understand the nature of the customer's business, its ownership and control



**Step 2** Identify the customer and verify its identity through the following information:

#### Legal Person

e.g. company/ business

- Name, legal form and proof of existence;
- Company/ business registration number;
- Powers that regulate and bind the customer, as well as persons having senior management position;
- Business and registered address;
- Any persons authorised to represent the company/ business; and
- Nature of business

#### Legal Arrangement

e.g. trust

- Name, legal form and proof of existence;
- Powers that regulate and bind the customer, as well as persons having senior management position; and
- Business address and address of the trustee's registered office

#### Club, Society and Charity

e.g. persatuan, yayasan

- Conduct CDD applicable for legal persons or legal arrangements, as the case may be; and
- Office bearer or any person authorised to represent the CSC

### Examples of verification documents



Certificate of Incorporation



Unique identifier such as tax identification number



Constitution



Directors' Resolution



Partnership Agreement



Trust Deed



Trust registration or equivalent document



Unique identifier such as tax identification number



Certificate of Registration



Identification Documents of Office Bearers

### Step 3

Identify and take reasonable measures to verify the identity of beneficial owners through the following information:

#### Who is a Beneficial Owner (BO)?

- Refers to any **natural person(s)** who ultimately **OWNS** or **CONTROLS** a customer and/or the natural person on whose behalf a transaction is being conducted.
- Also includes those **natural persons** who exercise **ULTIMATE EFFECTIVE CONTROL** over a legal person or arrangement.

'Ultimately owns or controls' or 'ultimate effective control' refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.

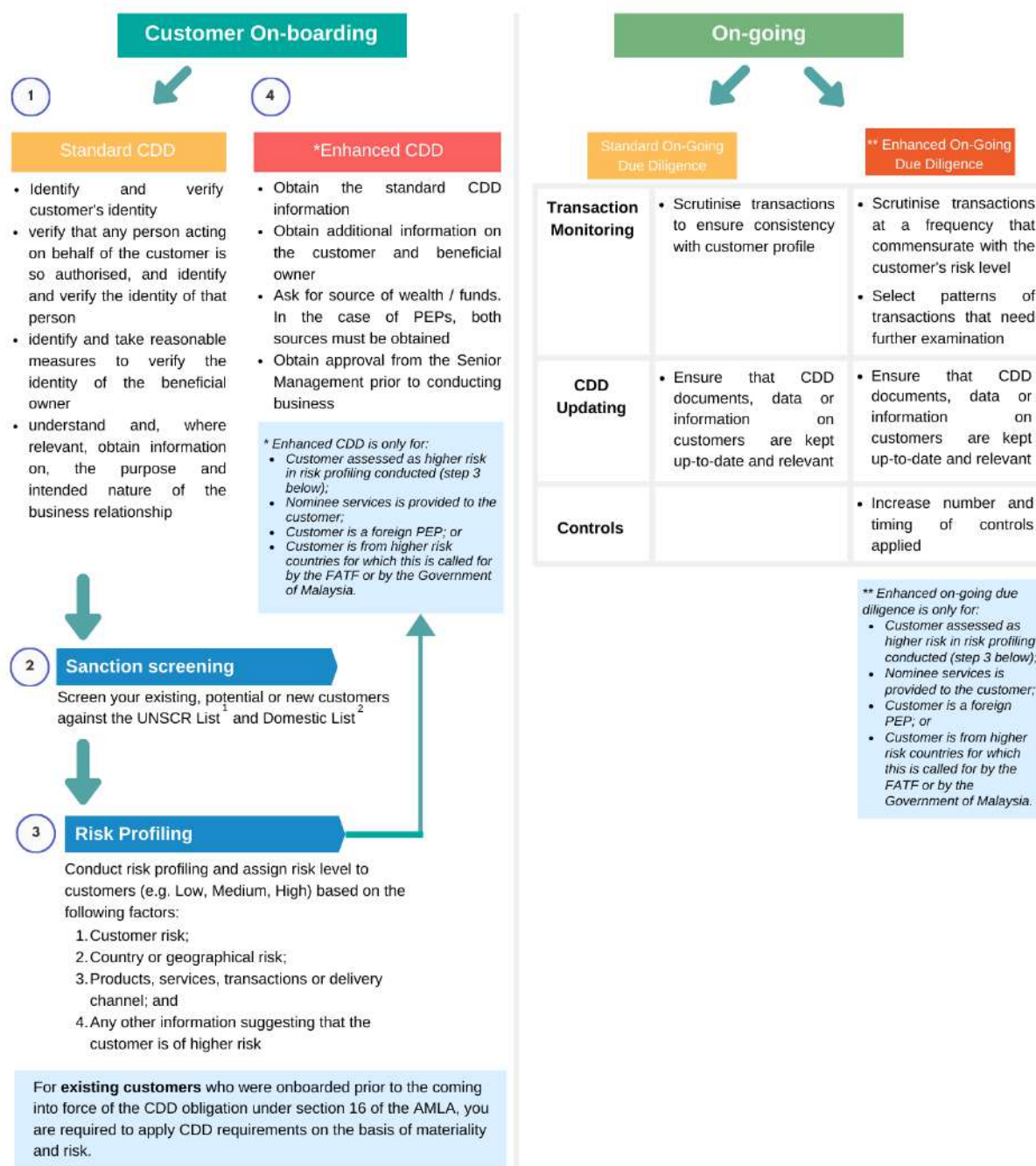
Legal Person	Legal Arrangement	Club, Society and Charity
<p><b>A.</b> Identity of the <b>natural person(s)</b> who ultimately has a controlling ownership interest in a legal person. At a minimum, this includes:</p> <p> Identification of directors/ shareholders with <b>equity interest of more than 25%</b>;</p> <p> <b>B.</b> If there is doubt on the controlling ownership interest - the identity of the <b>natural person</b> exercising control through other means; <b>AND</b></p> <p> <b>C.</b> When there is no <b>natural person</b> identified under <b>A</b> or <b>B</b> above, the identity of the <b>natural person</b> who holds the senior management position.</p> <p><i>If BO is identified at step A, you do not need to pursue steps B and C; or</i> <i>If BO is identified at step B, you do not need to pursue step C</i></p>	<p><b>A.</b> Identity of:</p> <ul style="list-style-type: none"> <li>Settlor;</li> <li>Trustee(s);</li> <li>Protector (if any);</li> <li>Beneficiary or class of beneficiaries; and</li> <li>Any other <b>natural person exercising ultimate effective control over the trust</b> (including through chain of control / ownership).</li> </ul> <p><b>B.</b> For other types of LA, the identity of persons in equivalent or similar positions.</p>	<p><b>A.</b> Pursuant to CDD undertaken on LP or LA, where relevant;</p> <p><b>B.</b> Identity of other members with effective control of the CSC.</p>

#### Examples of Other Means by which Natural Persons Exercise Control on LP, LA or CSC

Contractual associations or personal connections with management or directors	Recipient of loan or other benefit (e.g. tenancy of property / licence to property) having conditions granting control rights	Other ability to exert significant influence on corporate activity (e.g. veto rights, decision rights, right to profit, etc)
Other ownership arrangements (e.g. nominees, joint ownership arrangements)	Management control (the right to appoint or remove majority of directors)	Ownership of voting rights



## Customer Due Diligence (CDD) Process Flow



<sup>1</sup> **Consolidated UNSCR List:** <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

<sup>2</sup> **Domestic List:** <http://www.federalgazette.agc.gov.my>

**Note:** Please refer to Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) (AML/CFT/CPF and TFS for DNFBPs and NBFIs Policy Document).

**Disclaimer:**

This document is intended for your general information only. It does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.



## APPENDIX 12 Infographic on Suspicious Transaction Reports

# Suspicious Transaction Report (STR) Guide



### What is an STR?

STRs are documents that reporting institutions are required to submit when having suspicion that a customer is involved in **money laundering (ML)**, **terrorism financing (TF)**, **proliferation financing (PF)** or other serious crimes

### Why submit STRs?

STRs provide law enforcement agencies valuable information/ intelligence of potential crime activities

## When to submit STRs?

**Regardless of the amount being transacted**, you are required to promptly submit an STR, whenever you suspect or have reasons to suspect that the transaction or an activity (including attempted transactions or activity):

- appears unusual
- has no clear economic purpose
- appears illegal
- involves proceeds from an unlawful activity or instrumentalities of an offence
- indicates that the customer is involved in ML/TF/PF



## How do you recognise suspicious transactions?



1. **Screen** customer account.
2. **Ask** customer appropriate questions.
3. **Find** out customer's record/ review known information.
4. **Evaluate** information gathered and consider to submit an STR.

You are also required to establish **red flags** relevant to your business or service to facilitate the detection of suspicious transactions.

Examples of red flags are provided in the Policy Document.





### DO

- Ensure that STRs are submitted within the next working day, from the date the Compliance Officer establishes the suspicion.
- Establish reporting mechanism for submission of STR.
- Establish policies on the duration for Compliance Officer to review internal STRs.
- Ensure that STR is treated with utmost confidentiality.



### DON'T

- Disclose submission of STRs to anyone else, except under certain circumstances (refer to Section 14A of Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 20 of the Policy Document).
- Tip off the person(s) being reported - do treat them as normal clients so they do not suspect that STRs have been filed on them.

## How to submit STRs?

1. Fill up the STR form, which can be found at [www.amlcft.bnm.gov.my](http://www.amlcft.bnm.gov.my)
2. The Compliance Officer of the reporting institution to submit the STR via any of the following methods:

a) **Mail:** Director

Financial Intelligence and  
Enforcement Department  
Bank Negara Malaysia  
Jalan Dato' Onn  
50480 Kuala Lumpur  
(To be opened by addressee  
only)

b) **Email:** [str@bnm.gov.my](mailto:str@bnm.gov.my)

c) **FINS platform** (where applicable):

<https://fins.bnm.gov.my/>

**Note:** Please refer to Section 14 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 19 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Bank Financial Institutions (NBFIs) (AML/CFT/CPF and TFS for DNFBPs and NBFIs Policy Document)

**Disclaimer:**

This document is intended for your general information only. It does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.

## APPENDIX 13 Infographic on Targeted Financial Sanctions

### Targeted Financial Sanctions on Terrorism Financing, Proliferation Financing and Other UN-Sanctions Regimes Guide





**Targeted financial sanctions** are measures for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of specified entities/ designated persons who are being sanctioned.

**Terrorism financing** is the act of providing financing for terrorist acts, and for terrorists and terrorist organisations, through legitimate or illegitimate sources.

**Proliferation financing** is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

**Other UN-Sanctions Regimes** refer to any other United Nations Sanctions Committee (UNSC) sanctions regimes in relation to upholding of peace and security, and prevention of armed conflicts and human right violations.

#### WHAT DO YOU NEED TO DO?

1 	2 	3 	4 
MAINTAIN & UPDATE SANCTIONS LISTS	NAME SCREENING & DUE DILIGENCE	FREEZE/ REJECT	REPORT
<p>You are required to maintain a sanctions database on the United Nations Security Council Resolutions (UNSCR) List and Domestic List.</p> <p>The UNSCR List and Domestic List contain names and particulars of persons designated as specified entities/ designated persons by the UNSC and the Minister of Home Affairs (MOHA), respectively.</p> <p>You may refer to the lists from the following websites:</p> <ul style="list-style-type: none"> <li>• <b>Consolidated UNSCR List:</b> <a href="https://www.un.org">https://www.un.org</a></li> <li>• <b>Domestic List:</b> <a href="https://lom.agc.gov.my">https://lom.agc.gov.my</a></li> </ul> <p>You are required to update the database upon publication of designation or specification by the UNSC or MOHA.</p>	<p>You are required to conduct sanctions screening on <b>existing, potential or new customers</b> (including beneficial owners and beneficiary) against the sanctions lists.</p> <ul style="list-style-type: none"> <li>• Ensure that potential matches are true matches and not false positives</li> </ul> <p>Conduct due diligence on <b>related parties</b> (refer FAQ).</p>	<p>In the event of positive name match, you are required to, immediately and without delay:</p> <ul style="list-style-type: none"> <li>• Reject transactions for <b>new/ potential</b> customers</li> <li>• Freeze funds/ properties for <b>existing</b> customers</li> <li>• Block transactions (where applicable)</li> </ul>	<p>In the event of positive name match, you are required to immediately:</p> <ul style="list-style-type: none"> <li>• Report to the Financial Intelligence and Enforcement Department (FIED), Bank Negara Malaysia and Inspector-General of Police (Domestic List)</li> <li>• Submit Suspicious Transaction Report (STR) to FIED</li> </ul> <p>You should also submit STRs when suspecting that an account or transaction (including attempted transaction) is linked to a specified entity / designated person / related party.</p>



## WHAT TO DO WITH FUNDS/ PROPERTIES BELONGING TO SANCTIONED INDIVIDUALS?

The funds and properties may continue receiving deposits, dividends, interests, bonuses or other benefits. However, such funds and benefits must remain frozen as long as the specified entities / designated persons continue to be listed under the UNSCR List and Domestic List.

Where the freezing is made in relation to **terrorism financing**,

- Any dealings with the frozen funds or properties, whether by the specified entity, related parties or any interested party, requires prior written authorisation from the Minister of Home Affairs.
- You may advise the customer, a related party or any interested party of the frozen funds or properties to make an application to the Minister of Home Affairs to allow exemption for basic and extraordinary expenditures e.g. rent, medicine, etc.
- You shall only proceed with the payments upon receiving written authorisation from the Minister of Home Affairs.

Where the freezing is made in relation to **proliferation financing and other UN-sanctions**,

- Any dealings with frozen funds, other financial assets, or economic resources, whether by the designated country, person, identified related parties or interested parties, require prior written authorisation from the Strategic Trade Controller (STC) under the Strategic Trade Act (STA).
- You may advise the customer, a related party or any interested party of the frozen funds, other financial assets or economic resources, or to the blocked or rejected transaction to make an application to the STC under the STA to allow exemptions on basic and extraordinary expenditures and to allow payments due under contracts entered into prior to the designation.
- You shall only proceed with the payment only upon receiving the prior written authorisation and confirmation of the STC under the STA.




## WHO SHOULD YOU REPORT TO AND HOW?

### Terrorism Financing

(Upon determination of name match against **Domestic List, UNSCR 1988 and 1267 lists**)




#### 1 Upon Determination

#### 2 Periodic Reporting

Frequency	Terrorism Financing	
	1 Upon Determination	2 Periodic Reporting
 <b>Frequency</b>	Immediately after determination of a positive name match	For positive name match against: <ul style="list-style-type: none"> <li><b>UNSCR Lists</b> Every 5 January and 5 July</li> <li><b>Domestic List</b> Every 15 May and 15 Nov</li> </ul> Not required for customers who conduct one-off transactions and where the customers do not maintain an account with the reporting institution
	 <b>Recipient</b>	FIED, Bank Negara Malaysia & Inspector-General of Police
	 <b>Form</b>	Appendix 6A or 6B, where applicable
	Appendix 5A or 5B, where applicable	Appendix 6A or 6B, where applicable

## Proliferation Financing and Other UN-Sanctions Regimes

(Upon determination of name match against **UNSCR 1718 list**)

	1 Upon Determination	2 Periodic Reporting
 <b>Frequency</b>	Immediately after determination of a positive name match	Only if there is any change to the frozen funds (after first time reporting on positive name match) and latest by 15 January of the following calendar year.  Not required for customers who conduct one-off transactions and where the customers do not maintain an account with the reporting institution
 <b>Recipient</b>	FIED, Bank Negara Malaysia	FIED, Bank Negara Malaysia
 <b>Form</b>	Appendix 5A or 5B, where applicable	Appendix 6A or 6B, where applicable

## FREQUENTLY ASKED QUESTIONS (FAQ)

<p><b>1 Who are "related parties"?</b></p> <p>Related parties refer to:</p> <ul style="list-style-type: none"> <li>• person related to the funds, other financial assets or other economic resources that are wholly or jointly owned or controlled, directly or indirectly, by a designated person; and</li> <li>• a person acting on behalf or at the direction of a designated person.</li> </ul> <p>Based on the above, it may extend to shareholders, directors, authorised person, senior management and also the beneficial owner.</p>	<p><b>2 Can the RI accept loan repayments from specified entities/ designated persons?</b></p> <p>If the loan agreement was made prior to the listing of the specified entity/ designated person on the sanction lists, you may continue to receive the loan repayments on the agreement</p>
---	--

**Note:** Please refer to paragraphs 23 and 24 of the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT/CPF and TFS for DNFBPs & NBFIs Policy Document)

### Disclaimer:

This document is intended for your general information only. It does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.

# **PART E**

# **RED FLAGS**

## **APPENDIX 14      Examples of Red Flags**

### **Examples of Red Flags/Triggers for suspicion**

*Disclaimer:*

*These examples of red flags are intended as guidance in complying to the AMLA only. Reporting institutions are required to establish internal red flags to detect suspicious transactions.*

#### **Generic red flags**

##### **A. Red Flags involving Customers who are Individuals**

1. Customer refuses to provide information required by the reporting institutions, attempts to minimise the level of information provided or provides information that is misleading or difficult to verify.
2. Client who avoids personal contact without logical explanation.
3. Financial activities and transactions of the customer are inconsistent with the customer profile.
4. Unexplained inconsistencies arising from the process of identifying or verifying the customer.
5. Customer insists on the use of an intermediary (either professional or informal) without logical justification.
6. Customer who has previously been convicted for any serious crime.
7. Customer who is under investigation or has known connections with criminals.
8. Customer uses multiple bank accounts (from domestic or foreign jurisdiction) to complete a transaction without logical explanation.
9. Customer provides falsified records or counterfeit documentation.
10. Customer conducts large or frequent transactions using foreign currency without any economic rationale.
11. Customer is unusually concerned and/or makes inquiries about the AML/CFT/CPF requirements and internal compliance policies, procedures or controls.

##### **B. Red Flags involving Customers who are Legal Persons or Legal Arrangements**

1. Legal person which demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in activities.
2. Legal person which is registered under a name that indicates that the company performs activities or services that it does not provide without good reason.

3. Legal person or legal arrangement which is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations without good reason.
4. Legal person or legal arrangement which is registered at an address that does not match the profile of the company without good reason.
5. Legal person or legal arrangement which is registered at an address that is also listed for numerous other companies or legal arrangements, indicating the use of a mailbox service without good reason.
6. Where the director or controlling shareholder(s) cannot be located or contacted.
7. Where the director or controlling shareholder(s) do not appear to have an active role in the company without logical explanation.
8. Where the director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees.
9. Legal arrangement or trust which declared an unusually large number of beneficiaries or controlling interests.
10. Legal person, legal arrangement or trust which authorised numerous signatories without logical explanation or business justification.
11. Legal person or legal arrangement which is incorporated/formed in a jurisdiction that is considered to pose high ML/TF/PF risk.
12. Legal person which conducts financial activities and transactions inconsistent with its corporate profile.
13. Legal person which involves multiple shareholders who each hold an ownership interest just below the identification of beneficial ownership threshold.
14. Legal person which has indication of being used as a shell company e.g. use of informal nominees, no real business activities undertaken, does not have physical presence.
15. Media or other reliable sources suggest that the customer may be linked to criminal activity.

### **C. Red Flags involving Transactions**

1. Transactions conducted are questionable, or generate doubts that cannot be sufficiently explained by the client.
2. Transaction involves the use of multiple large cash payments without logical explanation.
3. Customer regularly conducts transactions with international companies without sufficient corporate or trade justification.



4. Frequent and cumulatively large transactions without any apparent or visible economic or lawful purpose.
5. Payments received for products/services from a third party who is not the owner of the funds, without any apparent reasons.
6. Transactions that require the use of complex and opaque legal entities or legal arrangements without logical explanation.
7. Transactions or instructions involve unnecessary complexity or which do not constitute the most logical, convenient and secure way to do business.
8. High volume of transactions within short period of time without economic purpose or commercial justification.
9. Unnecessary routing of funds or payments from/to/through third party account without logical explanation.
10. Transactions conducted via multiple payments from the same or different accounts/mode of payment which are broken down into smaller amounts without logical explanation.
11. Transactions which are conducted hastily or without due consideration a person would normally give to such transactions.

#### **D. Red Flags involving Geographical Location**

1. Large numbers of incoming or outgoing fund transfers take place for no logical business or other economic purpose, to or from locations of ML/TF/PF concern.
2. Legal persons or legal arrangements are incorporated/formed in a jurisdiction that has ML/TF/PF concern.
3. Customer has unexplained geographic distance from the reporting institutions.

#### **E. Red Flags involving Delivery Channel**

1. Use of a third party to avoid personal contact without logical explanation.

### **Sector Specific Red Flags**

#### **A. Licensed Gaming Outlets**

1. Transaction conducted indicates that the same punter frequently wins and the amount is above the threshold set.
2. Punter requests the winning amount to be paid using separate cheques for different individuals.
3. Punter presents multiple winning tickets.
4. Different punters requesting for the winning cheques to be issued to the same individual.

5. Punters requesting the winning amount to be paid using multiple methods e.g. cheques, cash, bank transfer.

## **B. Lawyers and Accountants**

1. “Structuring” a down payment or escrow money transaction in order to conceal the true source of the funds used or split transfers without logical explanation.
2. Transactions aborted after funds are received in client account, where subsequently client requests for the deposited funds to be sent to a third party and avoids personal contact without logical explanation.
3. Use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries situated in locations of ML/TF/PF concern.
4. Receive large sums of capital funding quickly following incorporation or formation, which is spent or transferred elsewhere in a short period of time without commercial justification.
5. Client has multiple shareholders who each hold an ownership interest just below the identification of beneficial ownership threshold.
6. Make frequent payments to foreign professional intermediaries without apparent economic or logical reasons.
7. Transactions occurring between two or more parties that are connected without an apparent business rationale.
8. Business transaction that involves family members of one or more of the parties without a legitimate business rationale.
9. Transactions executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company’s profile.
10. Transaction executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is inconsistent with the company’s profile.
11. Request for formation of complex trusts or legal arrangements involving complex structure or multiple offshore financial centres.

### **Additional for Lawyers**

12. Transfer of real estate between parties in an unusually short time period with no logical explanation.
13. Payment of deposits via multiple transactions below cash threshold reporting into the firm’s client account.
14. Client who offers to pay extraordinary fees for services that would not warrant such a premium with no logical explanation.

15. Funds deposited into the firm's client account which do not match with the client's profile.
16. Purchase of real estate property without end financing and logical explanation.
17. Depositing payment into the firm's client account from various locations without logical explanation.
18. Purchase of property below or beyond market value without reasonable explanation.

#### **Additional for Accountants**

19. Clients having history or tendency in changing accountants frequently without logical explanation.
20. Creation of fictitious employees under payroll list.
21. Company instructs to transfer sum of money to offshore companies via the clients' account without logical explanation.
22. Funds deposited into client account is relatively larger than the client's modest income or income generated from the underlying business activity, whereby the surplus fund is remitted to a third party instead of returned to the client.
23. Repeat transaction between parties over a contracted period of time without economic purpose.
24. Large or repeat transaction, and the executing customer is a signatory to the account, but is not identified as having a controlling interest in the company or assets.

#### **C. Company Secretaries**

1. A significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company.
2. Receipt by the company of an injection of capital or assets that is high in comparison with the business, size or market value of the company.
3. A large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, the activity of the client or its group companies.
4. Provision of nominee director or shareholder services without a clear and legitimate commercial purpose or some reasonable justification.
5. Use of shell companies where foreign ownership is spread across multiple jurisdictions.
6. Request for the establishment of shell companies for unclear purposes or for the sole purpose to open bank accounts.

7. Family members with no role or involvement in the running of the business are identified as beneficial owners of legal persons.
8. Client receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification.
9. Client has multiple shareholders who each hold an ownership interest just below the identification of beneficial ownership threshold.
10. Client makes frequent payments to foreign professional intermediaries without any logical reasons or without commercial justification.
11. Clients are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without commercial explanation.
12. Company with complex structures or multiple layers of shareholders, i.e. intertwining with multiple legal persons or legal arrangements without logical explanation.
13. Transactions occurring between two or more parties that are connected without an apparent business rationale.
14. Business transaction that involves family members of one or more of the parties without a business rationale.
15. Large or repeat transaction, and the executing customer is a signatory to the account, but is not identified as having a controlling interest in the company or assets.
16. Transactions executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile.
17. Transaction executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is inconsistent with the company's profile.
18. Clients are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without commercial explanation.

#### **D. Trust Companies**

1. Client declared an unusually large number of beneficiaries.
2. Withdrawal of trust assets immediately after being settled into the trust account without plausible reason.
3. Previously inactive trust account is now used intensively without any plausible reason.
4. Activities of the trust are unclear or different from the stated purposes under trust deeds.

5. Management of any trustee appears to be acting according to instructions of unknown or inappropriate person(s).
6. Transactions relating to the trust account are conducted with countries or entities that are reported to be associated with terrorist activities or with persons that have been designated as terrorists.
7. Trust structure or transactions relating to the trust account utilise complex and opaque legal entities and arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws, wherein the trust company is unable to fully understand the purpose or activities of their usage.
8. Discrepancy between the supposed wealth of the settlor and the object of the settlement.

## **E. Dealers in Precious Metals or Precious Stones**

### **Risk associated with customer and customer behaviour:**

1. Customer does not consider the value, size, quality and/or colour of the precious metal, precious stone metal or jewellery when making purchases.
2. Frequent transactions by a customer over a short period of time below the threshold for customer due diligence.
3. Established customer dramatically increasing his purchase of gold bullion for no apparent reason.
4. Previously unknown customer requesting a refiner to turn gold into bullion for no apparent reason.
5. Customer cancels the order after making large down payment amount and seeks for a refund in the form of cheques or telegraphic transfer for no apparent reason.
6. Frequent purchases by a PEP which do not commensurate with his or her profile.
7. Purchases that involve significant amount of cash without apparent reason.

### **Risk associated with business counter parties:**

8. Business counter parties appear to have no business knowledge of the industry in which he proposes to deal in.
9. Business counter parties do not have a place of business, equipment or finances necessary to support the business activities.

## **F. Registered Estate Agents**

1. Purchaser titles the property in the name of a nominee.

2. Customer substitutes the purchasing party's name at the last minute without reasonable explanation.
3. Purchaser resells the property within a short period of time without a reasonable explanation.
4. Purchase of multiple properties within a short period of time and it is inconsistent with the profile of the purchaser.
5. Payment for purchase of property does not come from customer's country of origin without logical explanation.
6. Purchase made without viewing the property without logical explanation.
7. Seller or property owner sells the property for significantly less than the purchase price without logical explanation.
8. There is a significant and unexplained geographic distance between the buyer and the location of the property.
9. Purchase of property without end financing.
10. Purchases which are not consistent with customers' profiles.
11. Deposits for property are paid in a significant amount of cash.
12. Purchases by legal persons/legal arrangements which obscure the true beneficial owner of the customer.
13. Payments or deposits are paid by third parties without logical explanation.
14. Payments or deposits are paid by multiple parties.

#### **G. Moneylenders, Pawnbrokers, Leasing and Factoring**

1. Customer is reluctant to provide the purpose of the loan, or that the stated purpose is ambiguous.
2. Customer suddenly repays a problem loan unexpectedly without logical explanation.
3. Customer makes a large, unexpected loan payment with unknown source of funds, or with the source of funds that does not match with the known profile of the client.
4. Customer repays a long term loan within a relatively short time period without logical explanation.
5. Customer shows income from foreign sources on loan application and is reluctant to provide details.
6. Customer's documentation to ascertain identification, support income or verify employment is provided by an intermediary who has no apparent reason to be involved.

7. Customer offers large deposits or some other form of incentive in return for favourable treatment of loan request without commercial justification.
8. Customer asks to borrow against its assets as collaterals to apply the loan where the origin of the assets is not known.
9. Customer asks to borrow against high value goods or real estate provided by unrelated third party as collaterals or guarantees to apply the loan without reasonable justification.
10. The loan transaction does not make economic sense e.g. the client has significant asset, hence does not appear to have a sound business reason for the transaction.
11. Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
12. Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business of the client.
13. Frequent default or intentionally default on loan secured by high value items or assets that can be easily converted into cash.
14. Customer making multiple pledges in close successions for an aggregated loan of a substantial value without commercial justification.
15. Customer uses notes in denominations that are unusual for the customer when making repayments.
16. Customer applies for a loan of an amount that is unusual compared with amounts of past transactions.
17. Application for financial leasing does not seem reasonable in terms of the intended use of the equipment or the client's business activity (e.g. obvious inconsistency between size of investment and lessee's business activity, or inadequacy of the equipment in comparison to the business activity the lessee engages in or intends to engage in).
18. The client repays debt under leasing contract, using funds transferred from countries known for highly secretive banking and corporate law.
19. Customer is found to produce fictitious invoice with an overstated amount to obtain factoring services.
20. Customers who frequently pawn items in a large quantity.
21. Customers who indicate disinterest in redeeming pawned items.
22. Customers who reveal that funds from pawned items will be used for travelling to conflict areas.