



**GUIDELINES ON  
ANTI-MONEY LAUNDERING AND COUNTER  
FINANCING OF TERRORISM (AML/CFT)  
  
INSURANCE AND TAKAFUL SECTORS**

## TABLE OF CONTENTS

### PART A OVERVIEW

1.	Introduction.....	3
2.	Objective .....	4
3.	Scope.....	4
4.	Legal Provisions .....	4
5.	Applicability .....	5
6.	Effective Date .....	5
7.	Compliance Date.....	6
8.	Guidelines Superseded.....	6
9.	Relationship with Existing Policies.....	6
10.	Definition and Interpretation.....	6

### PART B AML/CFT REQUIREMENTS

11.	Applicability to Branches, Subsidiaries and Offices of Labuan Home Grown Entities .....	13
12.	Risk-Based Approach Application .....	14
13.	Customer Due Diligence (CDD) .....	17
14.	Politically Exposed Persons (PEPs) .....	30
15.	New Products and Business Practices.....	32
16.	Reliance on Third Parties.....	32
17.	Non Face-to-Face Business Relationship .....	34
18.	Higher Risk Countries .....	35
19.	Failure to Satisfactorily Complete CDD .....	36
20.	Management Information System .....	36
21.	Financial Group (Labuan Home Grown Entities) .....	37
22.	Record Keeping .....	38
23.	AML/CFT Compliance Programme.....	38
24.	Suspicious Transaction Report.....	49
25.	Combating the Financing of Terrorism.....	54
26.	Non-Compliance .....	55
	Appendix I.....	56
	Appendix II.....	57

## **PART A      OVERVIEW**

### **1.      Introduction**

- 1.1      Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate which may lead to economic and social consequences. The globalisation of the financial services industry and advancement in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in utilizing reporting institutions to launder illicit funds and use them as conduits for ML/TF activities.
  
- 1.2      Since the formation of the National Coordination Committee to Counter Money Laundering (NCC), efforts have been undertaken to effectively enhance the AML/CFT compliance framework of reporting institutions resulting in the introduction of the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism AML/CFT and the relevant Sectoral Guidelines. While these efforts have addressed the ML/TF risks and vulnerabilities, there is a need to continuously assess the effectiveness of our AML/CFT framework to ensure that it continues to evolve in line with developments in international standards and the global environment.
  
- 1.3      Besides bringing the recommendation up to date in addressing new and emerging threats, the 2012 revision of the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks, which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

- 1.4 This Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Insurance and Takaful Guidelines is based on the principle that reporting institutions must conduct their business in conformity with high ethical standards and be on guard against undertaking any business transaction that is or may be connected with or may facilitate ML/TF. This is aim to ensure the integrity and soundness of Labuan International Business and Financial Centre (IBFC) and Malaysian financial systems are safeguarded.

## **2. Objective**

- 2.1 This guidelines is formulated in accordance with the provisions of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and the FATF 40 Recommendations and is intended to ensure that reporting institutions understand and comply with the requirements and obligations imposed on them.

## **3. Scope**

- 3.1 This guidelines sets out the:
- (a) obligations of reporting institutions with respect to the requirements imposed under the AMLATFA;
  - (b) requirements imposed on reporting institutions in implementing a comprehensive risk based approach in managing ML/TF risk; and
  - (c) roles of the reporting institutions' Board of Directors and Senior Management in putting in place the relevant AML/CFT measures.

## **4. Legal Provisions**

- 4.1 This guidelines is issued pursuant to:
- (a) Section 13, 14, 15, 16, 17, 18, 19, 20, 66E and 83 of the AMLATFA; and
  - (b) Section 4B of the Labuan Financial Services Authority Act 1996 (LFSAA).

## **5. Applicability**

- 5.1 This guidelines is applicable to:
- (a) Reporting institutions carrying on the following activities listed in the First Schedule of the AMLATFA:
    - (i) Labuan insurance and Labuan insurance related companies licensed under Part VII of the Labuan Financial Services and Securities Act 2010 (LFSSA);
    - (ii) Takaful and Labuan Takaful related operators licensed under Part VII of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA); and
    - (iii) any other persons as specified by Labuan FSA;
  - (b) branches and subsidiaries of reporting institutions referred to Paragraph 5.1(a) which carries out any activity listed on the First Schedule of the AMLATFA; and
  - (c) all products and services offered by reporting entities referred to Paragraph 5.1(a).
- 5.2 The requirements of this AML/CFT – Insurance and Takaful Sectors Guidelines is also applicable to Labuan licensees operating as foreign branches, subsidiaries and offices, wherein they are required to comply with the policies and procedures as implemented by their head office. However, if policies and procedures as implemented by their head office are inconsistent with the requirements of this document or less stringent than stated on this document, the requirements prescribed herein on this document shall prevail.
- 5.3 Where the reporting institutions are subject to more than one document relating to AML/CFT matters issued pursuant to Section 83 of the AMLATFA, the more stringent requirement shall apply.

## **6. Effective Date**

- 6.1 This AML/CFT – Insurance and Takaful Sectors will be effective from 30 December 2013.

## **7. Compliance Date**

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

## **8. Guidelines Superseded**

- 8.1 This guidelines supersedes:
- (a) The Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) issued on 4 January 2007; and
  - (b) The Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 2 for Offshore Insurance and Insurance Related Companies issued on 4 January 2007.

## **9. Relationship with Existing Policies**

- 9.1 This guideline shall be read together with other relevant policy documents, circulars and directives issued by Labuan FSA relating to compliance with AML/CFT requirements.

## **10. Definition and Interpretation**

- 10.1 The terms and expression used in this document shall have the same meanings assigned to it in the AMLATFA, LFSSA, and LIFSSA as the case may be, unless otherwise defined in this document.

- 10.2 For the purpose of this AML/CFT – Insurance and Takaful Guidelines, the following definitions and interpretations apply:

“accurate”	Refers to information that has been verified for accuracy.
“Bank”	Refers to Bank Negara Malaysia.
“beneficial owner”	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. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement.

	<p>Reference to “ultimately owns or control” or “ultimate effective control” refers to situation in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.</p>
<p>“beneficiary”</p>	<p>Depending on the context:</p> <p>In relation to insurance and takaful sectors, beneficiary refers to the natural or legal persons, or a legal arrangement, or category of person, who will be paid the policy proceeds when or if an insured event occurs, which is covered by the insurance policy.</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. This 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 wire transfer, refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.</p> <p>In clubs, societies and charities, refers to the natural persons or groups of natural persons who receive charitable, humanitarian or other types of services of the clubs, societies and charities.</p>

<p>“Board of Directors”</p>	<p>Refers to a governing body or a group of directors. A director includes any person who occupies a position of a director, however styled, of a body corporate or unincorporated.</p> <p>(a) a corporation, the same meaning assigned to it in subsection 2(1) of the Labuan Companies Act 1990;</p> <p>(b) a sole proprietorship, means the sole proprietor; and</p> <p>(c) a partnership, means the senior or equity partners.</p>
<p>“customer”</p>	<p>Refers to both account holder and non-account holder, and the term also refers to a client.</p>
<p>“customer due diligence”</p>	<p>Refers to any measures undertaken pursuant to section 16 of the AMLATFA.</p>
<p>“family members”</p>	<p>Refers to legal spouse, children (including legally adopted or step child), parents, siblings, in-laws, or relatives that might benefit from the relationship.</p>
<p>“financial group”</p>	<p>Refers to a group that consists of a holding company incorporated in Labuan or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with offices, branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.</p>
<p>“Government-linked company”</p>	<p>Refers to a corporate entity that may be private or public (listed on a stock exchange) where the government owns an effective controlling interest, or is owned by any corporate entity where the government is a shareholder.</p>
<p>“higher risk”</p>	<p>Refers to circumstances where the reporting institutions assess the ML/TF 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 (e.g. significant unexplained geographic distance between the</li> </ul>



	<p>reporting institution and the customer);</p> <ul style="list-style-type: none"> <li>• non-resident customer;</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>• business 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> <li>• persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling);</li> <li>• businesses or activities identified by the FATF as having higher risk for ML/TF;</li> <li>• legal arrangements that are complex (e.g. trust, nominee); and</li> <li>• persons who match the red flags criteria of the reporting institutions.</li> </ul> <p>(b) Country or geographic risk factors:</p> <ul style="list-style-type: none"> <li>• countries having inadequate AML/CFT systems;</li> <li>• countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;</li> <li>• countries having significant levels of corruption or other criminal activity; and</li> <li>• countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.</li> </ul>
--	---

	<p>In identifying countries and geographic risk factors, reporting institutions may refer, to credible sources such as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports published by international organisations such as the United Nations.</p> <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 fit into the person’s nature of business and risk profile; and</li> <li>• payment received from unknown or un-associated third parties.</li> </ul>
“higher risk countries”	Refers to countries that are listed by FATF or the Government of Malaysia with either on-going or substantial ML/TF risks or strategic AML/CFT deficiencies that pose a risk to the international financial system.
“home supervisor”	Refers to the Bank Negara Malaysia, Securities Commission and Labuan Financial Services Authority and any other person as defined under Section 28A of Labuan Financial Services Authority Act 1996.
“international organisations”	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>(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>
“legal arrangement”	Refers to express trusts or other similar legal arrangements.
“legal person”	Refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, foundations, partnerships, or associations and other similar entities.
“Labuan FSA”	Refers to Labuan Financial Services Authority.
“LIBFC”	Refers to Labuan International Business and Financial Centre.
“person”	Includes a body of persons, corporate or unincorporated.
“politically exposed persons (PEPs)”	<p>Refers to:</p> <p>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 of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials;</p> <p>b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or of</p>

	<p>government, senior politicians, senior government, judiciary or military officials, senior executives of state owned corporations and important political party officials; or</p> <p>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.</p> <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foreign countries.</p>
“requirements”	Refers to requirements that are issued pursuant to substantive provisions in the relevant laws administered by Labuan FSA and are binding. In the event of non-compliance, Labuan FSA may take enforcement actions.
“satisfied”	Where reference is made to a reporting institution being “satisfied” as to a matter, that reporting institution must be able to justify its assessment to the supervisory authority.
“Self-Regulatory Body (SRB)”	Refers to a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), 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 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 practicing the profession.
“senior management”	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a reporting institution (Labuan Entity) including Principal Officer.
“ third parties”	Refers to reporting institutions that are supervised and

	<p>monitored by a relevant competent authority and that meet the requirements under Paragraph 16 on Reliance of 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 or by another financial institution. It may also occur in business relationships between insurance companies and insurance brokers or between mortgage providers and brokers. Those third parties include foreign regulated financial institutions, insurance companies and brokers.</p>
--	---

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

### **11. Applicability to Branches, Subsidiaries and Offices of Labuan Home Grown Entities**

- 11.1 Reporting institutions are required to closely monitor the reporting institution's foreign branches, subsidiaries or offices operating in jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF or the Government of Malaysia.
  
- 11.2 Reporting institutions are required to ensure that their foreign branches, subsidiaries and offices apply AML/CFT measures consistent with the home country requirements. Where the minimum AML/CFT requirements of the host country are less stringent than those of the home country, the reporting institution must apply the home country requirements, to the extent that host country laws and regulations permit.
  
- 11.3 If the host country does not permit the proper implementation of AML/CFT measures consistent with the requirement in Malaysia, the

reporting institution and financial group are required to apply appropriate additional measures to manage the ML/TF risks, and report to Labuan FSA or any of their supervisors in Malaysia on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

- 11.4 In addition, the reporting institution may consider ceasing the operations of the said branch, subsidiary or office that unable to put in place the necessary mitigating control as required under Paragraph 11.3.

## **12. Risk-Based Approach Application**

### **12.1 Risk Management Functions**

12.1.1 In the context of “Risk-Based Approach”, the intensity and extensiveness of risk management functions shall be proportionate to the nature, scale and complexity of the reporting institution’s activities and ML/TF risk profile.

12.1.2 The reporting institution’s AML/CFT risk management function must be aligned and integrated with their overall risk management control function.

### **12.2 Risk Assessment**

12.2.1 Reporting institutions are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels.

12.2.2 In assessing ML/FT risks of their customers, reporting institutions are required to establish internal policies and procedures by having the following processes:

- (a) documenting their risk assessments and findings;

- (b) considering all the relevant risk factors before determining what is 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 mechanisms to provide risk assessment information to the supervisory authority.

12.2.3 Reporting institutions are required to conduct additional assessment as and when required by Labuan FSA and other supervisory authorities.

12.2.4 Reporting institutions may be guided by the results of the National Risk Assessment issued by Bank Negara Malaysia or Labuan FSA in conducting their own risk assessments.

### 12.3 Risk Control and Mitigation

12.3.1 Reporting institutions are required to:

- (a) have policies, controls and procedures, to manage and mitigate ML/TF risks that have been identified;
- (b) monitor the implementation of those policies, controls, procedures and to enhance them if necessary; and
- (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

12.3.2 Reporting institutions shall conduct independent control testing on their policies, controls and procedures for the purpose of monitoring the implementation thereof under Paragraph 12.3.1(b).

### 12.4 Risk Profiling

12.4.1 Reporting institutions are required to conduct risk profiling on their customers.

12.4.2 A risk profile must consider to include the following factors:

- (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) geographical location of business or country of origin of customers;
- (c) products, services, transactions or delivery channels (e.g. cash-based, face or non face-to-face, cross border); and
- (d) any other information suggesting that the customers is of higher risk.

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

12.4.4 Upon 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/FT risk.

## 12.5 **AML/CFT Risk Reporting**

12.5.1 Reporting institutions shall provide timely reporting of the risk assessment, ML/TF risk profile and the effectiveness of risk control and mitigation measures to the Board and Senior Management. The frequency and intensity of reporting shall commensurate with the level of risks involved and the reporting institution's operating environment.



12.5.2 The report referred to under Paragraph 12.5.1 may include, the following:

- (a) results of AML/CFT monitoring activities carried out by the reporting institution such as level of the reporting institution's exposure to ML/TF risks, break-down of ML/TF risk exposures based on key activities or customer segments, trends of suspicious transaction reports and trends of orders received from law enforcement agencies;
- (b) details of recent significant risk events, that occur either internally or externally, modus operandi and its impact or potential impact to the reporting institution; and
- (c) recent developments in AML/CFT laws and regulations, and its implication to the reporting institution.

## **13. Customer Due Diligence (CDD)**

### **13.1 General**

13.1.1 For any business transactions made through its agents, reporting institutions must enforce on their agents the requirements of CDD as required under this document.

13.1.2 Reporting institutions are required to set out processes that must be undertaken by the agents in conducting CDD as well as appropriate enforcement action by reporting institutions in its arrangement or agreement with agents.

### **13.2 When CDD is required**

13.2.1 Reporting institutions are required to conduct CDD on the customer and the person conducting the transaction, when:

- (a) establishing business relations;
- (b) it has any suspicion of ML/TF, regardless of amount; or
- (c) it has any doubt about the veracity or adequacy of the previously obtained information.

13.2.2 In establishing business relations, reporting institutions may conduct simplified CDD under paragraph 13.6 on its customer, beneficial owner and beneficiary for any insurance policy sold with insurance premiums involving an amount of foreign currency equivalent to below RM5,000 per annum, or foreign currency equivalent to below RM10,000 for any single premium insurance policy.

### 13.3 What is required

13.3.1 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 purporting to act on behalf of the customer is so authorized, 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.

13.3.2 In conducting CDD, reporting institutions are required to comply with the requirements on combating the financing of terrorism under Paragraph 25.

### 13.4 When verification is required

13.4.1 Reporting institutions are required to verify the identity of the customer and beneficial owner for any insurance sold with insurance premiums foreign currency equivalent to RM5,000

and above per annum or foreign currency equivalent to RM10,000 and above for any single premium insurance policy.

13.4.2 In addition to the CDD measures required under Paragraph 13.3.1, institutions are required to conduct the following CDD measures on the beneficiary, as soon as the beneficiary is identified/designated:

- (a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;
- (b) for beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information (e.g. under a will of testament) concerning the beneficiary to satisfy the reporting institutions that it will be able to establish the identity of the beneficiary at the time of the payout; and
- (c) for the purposes of Paragraphs 13.4.2(a) and (b), the verification of the identity of the beneficiary must occur latest at the time of the payout.

13.4.3 Reporting institution are not required to conduct verification on insurance policy owners of policies sold via any banking institution if it is satisfied that prior verification has been conducted by the banking institution in accordance with reliance on third parties under Paragraph 16 of this document.

13.4.4 Reporting institution may not conduct further verification on previously conducted CDD in the following circumstances:

- (a) for renewal and reinstatement of policies with no significant changes to the term and conditions or the insurance policy (including benefits under the insurance policy); or

- (b) for application of pure insurance covers which do not provide for payment of surrender values, including hospital and surgical insurance, critical illness insurance and pure term life insurance covers.

13.4.5 Reporting institutions may refer to **Appendix I** for the illustration of the timing of identification and verification process.

### 13.5 **Specific CDD Requirements**

#### *Individual Customer and Beneficial Owner*

13.5.1 In conducting CDD on an individual customer and beneficial owner, the reporting institution is required to obtain at least the following information:

- (a) full name;
- (b) National Registration Identity Card (NRIC) number or valid passport number or reference number of any other official documents bearing the photograph 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/nature of business;
- (h) the purpose of transaction;
- (i) source of wealth (i.e. if the income does not match with the occupation); and
- (j) contact number (home, office or mobile).

13.5.2 Reporting institutions shall verify the documents referred to under Paragraph 13.5.1(b) by requiring the customer or beneficial owner, as the case may be, to furnish the original document and make a copy of the said document. However,

where biometric identification method is used, verification is deemed to be satisfied.

13.5.3 Where there is any doubt, reporting institutions are required to request the customer and beneficial owner, as the case may be, to produce other supporting official identification documents bearing their photographs, issued by an official authority or an international organisation, to enable their identity to be ascertained and verified.

#### *Legal Persons*

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

13.5.5 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 Memorandum/Article/Certificate of Incorporation/ Partnership (certified true copies/duly notarised copies, may be accepted) 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, from the principal place of business.

13.5.6 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- (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 the following:
  - (i) identification document of Directors/Shareholders with equity interest of more than twenty five percent/Partners (certified true copy/duly notarised copies or the latest Form 24 and 49 as prescribed by the Companies Commission of Malaysia or Form 13 and Form 25 as prescribed by the Registrar of Companies, Labuan FSA or foreign incorporation, or any other equivalent acceptable documents for other types of legal person are acceptable);
  - (ii) authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and
  - (iii) relevant documents such as NRIC for Malaysian/permanent resident or passport for foreigner, to identify the identity of the person authorised to represent the company or business in its dealing with the reporting institution;
- (b) to the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) under Paragraph 13.5.6(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 13.5.6(a) or (b) above, the identity of the relevant natural person who holds the position of Senior Management.

13.5.7 Where there is any doubt to comply with the requirements under Paragraphs 13.5.5 and 13.5.6, 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 Labuan Financial Services Authority, Companies Commission of Malaysia or any other relevant agencies.

13.5.8 Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or certificate of incorporation and from identifying and verifying the directors and shareholders of the legal person which fall under the following categories:

- (a) public listed companies or corporations listed in Labuan International Financial Exchange and 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) government-linked companies in Malaysia;
- (e) state-owned corporations and companies in Malaysia;
- (f) an authorized person, an operator of a designated payment system, a registered person, as the case may be, under the Financial Services Act (FSA) and Islamic Financial Services Act (IFSA);
- (g) persons licensed or registered under the Capital Markets and Services Act 2007;

- (h) licensed entities under the Labuan Financial Services and Securities Act 2010 and Labuan Islamic Financial Services and Securities Act 2010; or
- (i) prescribed institutions under the Development Financial Institutions Act 2002.

13.5.9 Reporting institutions may refer to the Directives in relation to Recognised Stock Exchanges (R/R 6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

#### *Legal Arrangements*

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

13.5.11 Reporting institutions are required to identify the customer and verify its identity through the following information:

- (a) name, legal form and proof of existence, 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 in the customer; and
- (c) the address of the registered office, and if different, a principal place of business.

13.5.12 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 beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ ownership); or



(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

13.5.13 For the purpose of identifying beneficiaries of trusts that are designated by characteristics or by class under Paragraph 13.5.12, reporting institutions are required to obtain sufficient information concerning the beneficiary in order to be satisfied that it would be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

13.5.14 Reporting institutions may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.

13.5.15 Where reliance is placed on third parties under Paragraph 13.5.14, reporting institutions are required to comply with Paragraph 16 on Reliance on Third Parties.

#### *Clubs, Societies and Charities*

13.5.16 For customers that are clubs, societies or charities, reporting institutions shall conduct CDD and require the customers to furnish the relevant identification and constituent documents (or other similar documents) including certificate of registration and the identification and verification of the office bearer or any person authorised to represent the club, society or charity, as the case may be.

13.5.17 Reporting institutions are required to take reasonable measures to identify and verify the beneficial owners.

### *Reinsurance Arrangement*

13.5.18 Under a reinsurance arrangement, reporting institutions are required to carry out verification only on the ceding company, and not their ceding company's customers. The following verification procedure applies:

- (a) verification is not required where the ceding company is licensed under the FSA, Takaful Operator licensed under the IFSA, licensed entities under the Labuan Financial Services and Securities Act 2010 or a Takaful Operator licensed under the Labuan Islamic Financial Services and Securities Act 2010; and
- (b) reinsurers are required to take necessary steps to verify that the ceding company is authorised to carry on insurance business in its home jurisdiction which enforces AML/CFT standards equivalent to those in the AMLATFA.

### *Group Customers*

13.5.19 Identification and verification of group insurance policies owners are required to be carried out at the point of sale.

## **13.6 Simplified CDD**

13.6.1 Reporting institutions may undertake the following measures for simplified CDD where the requirements under paragraph 13.2.2 apply.

13.6.2 Reporting institutions are required to identify the customers and beneficial owners when establishing business relationship.

13.6.3 The verification of the individual customers, beneficial owners must take place latest at the time of payout.

13.6.4 Where simplified CDD apply, reporting institution may adopt the following measures:

- (a) reducing the frequency of customer identification updates;
- (b) reducing the degree of on-going due diligence; or
- (c) not obtaining specific information but inferring from the type of transaction or business relation established on the purpose and intended nature of business relationship as required under Paragraph 13.3.1(d).

13.6.5 Notwithstanding the above, reporting institution must have in place measures to prevent transaction from being artificially split to avoid the threshold of insurance premium of foreign currency equivalent to RM5,000 per annum or foreign currency equivalent to RM10,000 for single premium. Therefore, the accumulated premium size of multiple policies per policy holder must be taken into consideration.

13.6.6 Simplified measures are not applicable where there is a suspicion of ML/TF, or where specific higher risk scenarios apply.

## 13.7 **Enhanced CDD**

13.7.1 Reporting institutions are required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include at least, the following:

- (a) obtaining CDD Information under Paragraph 13.5;
- (b) obtaining additional information on the customer and beneficial owner (e.g. volume of assets, occupation, and other information from reliable public database);
- (c) inquiring 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 or any other person(s)<sup>1</sup> referred by the head office.

13.7.2 Reporting institutions are required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If the reporting institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, reporting institutions are required to take enhanced measures to identify and verify the identity of the beneficial owner of the beneficiary, latest at the time payout.

13.7.3 In addition to Paragraph 13.7.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

- (a) obtaining additional information on the beneficial owner of the beneficiaries (for example occupation, volume of assets, information available through public databases or internet); and
- (b) requiring the first payment to be carried out through an account in the beneficial owner's name with a financial institution subject to similar CDD standards.

13.7.4 Where the beneficiaries or the beneficial owner of the beneficiaries are politically exposed persons (PEPs) and assessed as higher risk at the latest, at the time of payout, reporting institutions are required to:

- (a) Inform senior management at the head office before the payout of the policy proceeds;

---

<sup>1</sup> Officers delegated by the Senior Management who have primary or significant responsibility for the management and performance of the business activities of the Labuan Entity including the Principal Officer.

- (b) updating conduct enhanced scrutiny on the whole business relationship with the policyholder; and
- (c) consider lodging a suspicious transaction report.

## 13.8 On-Going Due Diligence

13.8.1 Reporting institutions are required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:

- (a) scrutinizing 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.

13.8.2 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 transaction, especially with regard to complex and large transactions or higher risk customers.

13.8.3 The frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall commensurate with the level of ML/TF risks posed by the

customer based on the risk profiles and nature of transactions.

13.8.4 Reporting institutions are required to increase the number and timing of controls applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

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

13.9.1 Reporting institutions are required to apply CDD requirements to existing customers on the basis of materiality and risk.

13.9.2 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.

13.9.3 In assessing materiality and risk of the existing customer under Paragraph 13.9.1, 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, transaction or business relationship is operated; or
- (c) insufficient information held on the customer or change in customer's information.

## **14. Politically Exposed Persons (PEPs)**

### **14.1 General**

14.1.1 The requirements set out under this Paragraph are applicable to family members or close associates of all types of PEPs.

## 14.2 Foreign PEPs

14.2.1 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.

14.2.2 Reporting institutions are required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are foreign PEPs.

14.2.3 Upon determination that a customer/beneficial owner/beneficiary/beneficial owner of beneficiary is a foreign PEP, the requirements of enhanced CDD as set out under Paragraph 13.7 must be conducted.

## 14.3 Domestic PEPs or Persons entrusted with a prominent function by an international organization

14.3.1 Reporting institutions are required to take reasonable measures to determine whether a customer/beneficial owner/beneficiary is a domestic PEP or a person entrusted with a prominent function by an international organisation.

14.3.2 If the customer/beneficial owner/beneficiary is assessed as 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 risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function by an international organisation.

14.3.3 The assessment of the ML/TF risks, as specified under Paragraph 14.3.2, shall take into account the profile of the

customer under the profile of the customer under Paragraphs 12.4.2 on Risk Profiling.

14.3.4 The requirements of enhanced CDD as set out under Paragraph 13.7 must be conducted in respect of domestic PEPs or person entrusted with a prominent function by an international organisation who are assessed as higher risk.

14.3.5 Reporting institutions may apply CDD measures similar to other customer for domestic PEPs or person 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.

## **15. New Products and Business Practices**

15.1 Reporting institutions are required to identify and assess the ML/TF 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.

15.2 Reporting institutions are required to:

- (a) undertake the 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.

## **16. Reliance on Third Parties**

### **Customer Due Diligence**

16.1 Reporting institutions may rely on third parties to conduct CDD or to introduce business.

16.2 The ultimate responsibility and accountability of CDD measures shall remain with the reporting institution relying on the third parties.



- 16.3 Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties, including those from foreign jurisdictions that have been identified as having strategic AML/CFT deficiencies that pose a ML/FT risk to the international financial system.
- 16.4 Reporting institutions are prohibited from relying on third parties located in the higher risk countries that have been identified as having on-going or substantial ML/TF risks.
- 16.5 The relationship between reporting institutions and their 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. At the minimum, reporting institutions must be satisfied that the third party:
- (a) can obtain immediately the necessary information concerning CDD as required under the Paragraph 13.5;
  - (b) has an adequate CDD process;
  - (c) has measures in place for record keeping requirements;
  - (d) can provide the CDD information and provide copies of the relevant documentation immediately upon request; and
  - (e) is properly regulated and supervised by the respective authorities.
- 16.6 Reporting institutions may obtain an attestation from the third party to satisfy themselves that the requirements in Paragraph 16.5 have been met.
- 16.7 Reporting institutions may obtain written confirmation from the third party that they have conducted CDD on the customer or beneficial owner, as the case may be, in accordance with Paragraph 13.

- 16.8 The requirements under Paragraphs 16.1, 16.3 and 16.5 may be fulfilled if the reporting institution rely on a third party that is part of the same financial group subject to the following conditions:
- (a) the group applies CDD and record keeping requirements and AML/CFT programmes against in line with the requirements in this document;
  - (b) the implementation of those CDD and record keeping requirements and AML/CFT programmes are supervised at a group level by a competent authority; and
  - (c) any higher country risk is adequately mitigated by the financial group's AML/CFT policies.
- 16.9 Reporting institutions are prohibited from relying on a third party located in the countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

### **On-Going Due Diligence**

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

## **17. Non Face-to-Face Business Relationship**

- 17.1 Reporting institutions may establish non face-to-face business relationships with its customers.
- 17.2 Non face-to-face relationships can only be established if the reporting institutions have in place policies and procedures to address any specific risks associated with non face-to-face business relationships.
- 17.3 Reporting institutions are required to be vigilant in establishing and conducting business relationships via information communication technology.

- 17.4 Reporting institutions are required to establish appropriate measures for identification and verification of customer's identity that shall be as effective as that for face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.
- 17.5 Reporting institutions may use the following measures to verify the identity non face-to-face customer such as:
- (a) requesting additional documents to complement those which are required for face-to-face customer;
  - (b) developing independent contact with the customer; or
  - (c) verifying customer information against databases maintained by the authorities.

## **18. Higher Risk Countries**

- 18.1 Reporting institutions are required to conduct enhanced CDD for business relationships and transaction with any person from countries identified by the FATF or the Government of Malaysia as having on-going or substantial ML/TF risks.
- 18.2 Where ML/TF risks are assessed as higher risk, reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.
- 18.3 In addition to the enhanced CDD requirement under Paragraph 18.1 reporting institutions are required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:
- (a) limit business relationship or financial transactions with identified countries or persons located in the country concerned;

- (b) review and amend, or necessary terminate, correspondent banking relationship with financial institution in the country concerned;
- (c) conduct enhanced audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned;
- (d) submit a report with summary exposure to customers and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia as the Competent Authority and Supervision and Enforcement Department, Labuan FSA on an annual basis; and
- (e) conduct any other measures as specified by Labuan FSA.

## **19. Failure to Satisfactorily Complete CDD**

- 19.1 Reporting institutions shall not commence business relations or perform any transaction in relation to potential customer, or shall terminate business relations in the case of existing customer, if the reporting institution is unable to comply with the CDD requirements.
- 19.2 In the event of failure to comply with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report under paragraph 24.

## **20. Management Information System**

- 20.1 Reporting institutions must have in place an adequate management information system (MIS), either electronically or manually, 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 irregularity and/or any suspicious activity.
- 20.2 The MIS shall commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

- 20.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomaly in transaction pattern, customer's risk profile and transactions exceeding any internally specified threshold.
- 20.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems.
- 20.5 The MIS may be integrated with the reporting institution's information system that contains its customer's normal transaction or business profile, which is accurate, up-to-date and reliable.

## **21. Financial Group (Labuan Home Grown Entities)**

- 21.1 A parent company incorporated in Labuan is required to implement group-wide programme against ML/TF which is required to be applicable, and appropriate to, all branches and subsidiaries of the group. These shall include the following measures:
- (a) framework for AML/CFT 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 risk management;
  - (d) the provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and
  - (e) safeguards on the confidentiality and use of information exchanged.
- 21.2 A group compliance officer is responsible for creating, coordinating and making a group-wide assessment for the implementation of a single AML/CFT strategy, including mandatory policies and procedures and the authorisation to give orders to all branches and subsidiaries.

## **22. Record Keeping**

- 22.1 Reporting institutions are required to keep the relevant records including any account, files, business correspondence and documents relating to transactions, in particular, those obtained during CDD process. This includes documents used to verify the identity of customers, beneficial owners, beneficiaries, beneficial owners of beneficiaries and results of any analysis undertaken. The records maintained must remain up-to-date and relevant.
- 22.2 Reporting institutions are required to keep the records for at least six years following the completion of the transaction, the termination of business relationship or after the date of occasional transaction.
- 22.3 In situations where the records are subjected to on-going investigations 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.
- 22.4 Reporting institutions are required to retain the relevant records in the form that is admissible as evidence in court and make such available to the supervisory authorities and law enforcement agencies in a timely manner.

## **23. AML/CFT Compliance Programme**

### **23.1 Policies, Procedures and Controls**

- 23.1.1 Reporting institutions are required to implement programmes to mitigate against ML/TF, which correspond to its ML/TF risks and the size of its business.

## 23.2 Board of Directors

### 23.2.1 General

- (a) Members of Board of Directors (Board members) shall understand their roles and responsibilities in managing ML/TF risks faced by the reporting institution;
- (b) Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services; and
- (c) Board members must understand the AML/CFT measures required by laws including the AMLATFA, subsidiary legislation and instruments issued under the AMLATFA, and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the reporting institution from being abused by money launderers and financiers of terrorism.

### 23.2.2 Roles and Responsibilities

The Board of Directors (Board) have the following roles and responsibilities:

- (a) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;
- (b) approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- (c) establish appropriate mechanisms to ensure the AML/CFT 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;

- (d) establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by reporting institutions;
- (e) define the lines of authority and responsibility for implementing the AML/CFT 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;
- (g) assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and
- (h) establish 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.

### 23.3 Senior Management

23.3.1 Senior Management is accountable for the implementation and management of AML/CFT compliance programmes in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

#### 23.3.2 *Roles and Responsibilities*

The Senior Management have the following roles and responsibilities:

- (a) be aware of and understand the ML/TF 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 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 mechanism and formulate procedures to effectively implement AML/CFT 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 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 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 which may have an impact on the reporting institution;
- (f) allocate adequate resources to effectively implement and administer AML/CFT compliance programmes that are reflective of the size and complexity of the reporting institution's operations and risk profiles;
- (g) appoint a compliance officer at management level at head office and designate a compliance officer at management level at each branch or subsidiary;
- (h) provide appropriate levels of AML/CFT training for its employees at all level throughout the organisation;

- (i) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;
- (j) ensure that AML/CFT issues raised are addressed in a timely manner; and
- (k) ensure the integrity of its employees by establishing appropriate employee assessment system.

## 23.4 **Compliance Management Arrangements**

23.4.1 The Compliance Officer acts as the reference point for AML/CFT matters within the reporting institution.

23.4.2 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.

23.4.3 The Compliance Officer is required to be “fit and proper” to carry out his AMLCFT responsibilities effectively.

23.4.4 For the purposes of Paragraph 23.4.3, “fit and proper” may include minimum criteria relating to:

- (a) probity, personal integrity and reputation; and
- (b) competency and capability.

23.4.5 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.

23.4.6 Reporting institutions may encourage the Compliance Officer to pursue professional qualifications in AML/CFT so that they are able to carry their obligation effectively.

23.4.7 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

23.4.8 The Compliance Officer has a duty to ensure the following:

- (a) the reporting institution's compliance with the AML/CFT requirements;
- (b) proper implementation of the AML/CFT policies;
- (c) the appropriate AML/CFT procedures, including CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism, are implemented effectively;
- (d) the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;
- (e) the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;
- (f) all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;
- (g) internal generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and Anti-Money Laundering Compliance Unit, Labuan FSA; and
- (h) the identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

23.4.9 Reporting institutions are required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and Anti-Money Laundering Compliance Unit, Labuan FSA 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, fax number, e-mail address and such other information as may be required.

23.4.10 The Compliance Officer or any designated person as Compliance Officer needs to ensure and check any latest information or announcement in relation to AML Compliance on Labuan FSA website on frequent basis. The person also responsible to take necessary action (if any) within reasonable time.

## **23.5 Employee Screening Procedures**

23.5.1 For the purpose of this Paragraph, reference to employees includes agents.

23.5.2 The screening procedures shall apply upon hiring the employee and throughout the course of employment.

23.5.3 Reporting institutions are required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of reporting institutions to ML/TF.

23.5.4 The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.

## 23.6 Employee Training and Awareness Programmes

- 23.6.1 Reporting institutions are required to conduct awareness and training programmes on AML/CFT practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher course.
- 23.6.2 The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.
- 23.6.3 The reporting institution must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must at least contain at least the following:
- (a) the relevant documents on AML/CFT issued by Labuan FSA or relevant supervisory authorities; and
  - (b) the reporting institution's internal AML/CFT policies and procedures.
- 23.6.4 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting institutions.
- 23.6.5 Employees who deal directly with the customer shall be trained on AML/CFT prior to dealing with customers.
- 23.6.6 Training for all employees may provide a general background on ML/TF, the requirement and obligation to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

23.6.7 In addition, training may be provided to specific categories of employees:

(a) **Front-Line Employees**

Front-line employees may be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customer transacting in large amount of transactions, PEPs, higher risk customers and the circumstances where enhanced CDD is required.

(b) **Employees that Establishing Business Relationship**

The training for employees who establish business relationship may focus on customer identification, verification and CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with new customer until CDD is completed satisfactorily.

(c) **Supervisors and Managers**

The training on Supervisors and Managers may include overall aspects of AML/CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customer, enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing of terrorism.

## 23.7 **Training for Insurance and Takaful Agents**

23.7.1 Reporting institutions are required to ensure their insurance and takaful agents received initial and on-going training on relevant AML/CFT.

23.7.2 In addition to Paragraph 23.7.1 above, the training programme for the insurance and takaful agents shall include the following:

- (a) its legal responsibilities;
- (b) AML/CFT policies and procedures of reporting institutions;
- (c) customer due diligence;
- (d) the requirements of verification and records;
- (e) the recognition and reporting of transactions suspected to involve in ML/TF; and
- (f) the requirements all other relevant policies and procedures.

23.7.3 The insurance and takaful agents are required to be aware that suspicious transaction must be reported to the AML/CFT Compliance Officer at the reporting institution in accordance with the reporting mechanism.

## 23.8 **Independent Audit Function**

23.8.1 The Board is responsible to ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFA, its regulations, subsidiary legislations and relevant policies, circulars and directives on AML/CFT issued by Labuan FSA as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

23.8.2 The Board is required to 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, and effectiveness of the AML/CFT policies, procedures and controls; and
- (b) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.

23.8.3 The scope of independent audit shall include, at a minimum:

- (a) compliance with AMLATFA, its subsidiary legislation and instrument issued under the AMLATFA;
- (b) compliance with the reporting institution's internal AML/CFT policies and procedures;
- (c) adequacy and effectiveness of the AML/CFT compliance programme; and
- (d) reliability, integrity and timeliness of the internal and regulatory reporting and management information systems.

23.8.4 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT measures and any inadequacy in internal controls and procedures.

23.8.5 Reporting institutions are to ensure that independent audits are carried out at the institution level at least on an annual basis.

23.8.6 Reporting institutions must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Supervision and Enforcement Department, Labuan FSA within three months after the completion of the internal audit and within ten working days after submission to Board.



## 24. Suspicious Transaction Report

### 24.1 General

24.1.1 Reporting institutions are required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to Anti-Money Laundering Compliance Unit, Labuan FSA whenever the reporting institution suspect or have reason to suspect that the transaction (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
- (e) indicates that the customer is involved in ML/TF.

24.1.2 Reporting institutions must provide the required and relevant information that giving rise to suspicion 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.

24.1.3 Reporting institutions must establish a reporting system for the submission of suspicious transaction reports.

24.1.4 Reporting institutions may refer to **Appendix II** of this document which provides examples of transactions that may constitute triggers for the purposes of reporting suspicious transactions.

### 24.2 Reporting Mechanisms

24.2.1 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.

24.2.2 Reporting institutions are required to have in place policies on the duration upon which internally generated suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe can be exceeded, where necessary.

24.2.3 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.

24.2.4 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report form through the following modes:

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

Fax : +603-2693 3625  
E-mail : [str@bnm.gov.my](mailto:str@bnm.gov.my)

AND

Mail : Director  
Supervision and Enforcement Dept  
Labuan Financial Services Authority  
Level 17, Main Office Tower  
Financial Park Complex  
Jalan Merdeka  
87000 Labuan F.T.  
Attention to : Anti-Money Laundering  
Compliance Unit  
(To be opened by addressee only)

Fax : +6087-411496  
E-mail : [aml@labuanfsa.gov.my](mailto:aml@labuanfsa.gov.my)

24.2.5 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and/or Anti-Money Laundering Compliance Unit, Labuan FSA, the compliance officer of a reporting institution must submit its suspicious transaction reports on-line:

Website : <https://bnmapp.bnm.gov.my/fins2>

24.2.6 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.

24.2.7 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.

24.2.8 Reporting institutions must provide additional information and documentations as may be requested by Labuan FSA and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.

24.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in secured environment to maintain confidentiality and preserve secrecy.

24.2.10 Where a suspicious transaction report has been lodged, reporting institutions are not precluded from making a fresh suspicious transaction report when a new suspicion arises.

### 24.3 **Tipping Off**

24.3.1 In cases where the reporting institution form a suspicion of ML/TF and reasonably believe that performing the CDD process would tip off the customer, the reporting institution is permitted not to pursue the CDD process. In such circumstances, the reporting institution shall proceed with the transaction and immediately file a suspicious transaction report.

24.3.2 Tipping off in relation to suspicious transaction report is not applicable if :

- (a) the purpose of the disclosure is made to inform the ML/TF risks involved in dealing with the customer within the financial group; or
- (b) such disclosure is made to a supervisory authority of the reporting institution.

24.3.3 Provisions under Paragraph 24.3.2 will not come into effect until such date as specified by Labuan FSA.

#### **24.4 Triggers for Submission of Suspicious Transaction Report**

24.4.1 Reporting institutions are required to establish internal criteria (“red flags”) to detect suspicious transactions.

24.4.2 Reporting institutions may be guided by examples of suspicious transactions provided by Labuan FSA or other corresponding competent authorities, supervisory authorities and international organisations.

24.4.3 Reporting institutions must consider submitting a suspicious transaction report when any of its customer’s transaction or attempted transaction fits the reporting institution’s list of “red flags”.

#### **24.5 Internally Generated Suspicious Transaction Reports**

24.5.1 Reporting institutions must ensure that the Compliance Officer maintain a complete file on all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. If there is no suspicious transaction reports submitted to Financial Intelligence and Enforcement Department, Bank Negara Malaysia, and also to AML Compliance of Labuan FSA, the internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities upon request.

## 25. Combating the Financing of Terrorism

- 25.1 Where relevant, the references to a customer in this Paragraph include a beneficial owner and beneficiary.
- 25.2 Reporting institutions are required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1888 (2011) and 1989 (2011) which require sanctions against individuals and entities belonging or related to the Taliban, Osama bin Laden and the Al-Qaida organisation.
- 25.3 Reporting institutions are required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at:  
[http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml)
- 25.4 Reporting institutions are required to maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLATFA by the Minister of Home Affairs.
- 25.5 Reporting institutions shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.
- 25.6 Reporting institutions are required to conduct regular checks on the names of new, potential and existing customers, against the names in the database. If there is any name match, reporting institutions are required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, reporting institutions must immediately:
- (a) freeze the customer's funds or block the transaction (where applicable), if it is an existing customer;

- (b) reject the potential customer, if the transaction has not commenced;
  - (c) submit a suspicious transaction report; and
  - (d) inform the relevant supervisory authorities.
- 25.7 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the Consolidated List or orders made by the Minister of Home Affairs under section 66B or 66C of the AMLATFA.
- 25.8 Reporting institutions are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate “false positive”. The reporting institutions are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.
- 25.9 Reporting institutions may also consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

## **26. Non-Compliance**

- 26.1 Enforcement action can be taken against the reporting institutions including its Directors, Officers, and Employees for any non-compliance with provision under:
- (a) In Sections 22, 66E, 86, 87, 88, 92 and 93 of the AMLATFA; and/or
  - (b) Section 4B of the Labuan Financial Services Authority Act 1996 (LFSAA).

## Appendix I

CDD for Insurance				
	Normal		Simplified	
	Premium > Threshold i. Foreign currency equivalent to RM5,000 and above for annual premium; or ii. Foreign currency equivalent to RM10,000 and above for single premium		Premium < Threshold i. Foreign currency equivalent to RM5,000 and above for annual premium; or ii. Foreign currency equivalent to RM10,000 and above for single premium	
On who?	Customer and its Beneficial Owner	Beneficiary	Customer and its Beneficial Owner	Beneficiary
What is required? Identification*	When establishing business relationship	At the point of nomination	When establishing business relationship	At the point of nomination
Verification**	When establishing business relationship	Latest at the point of payout	Latest at the point of layout	

\* Identification – refer paragraph 13.5.1 of this document

\*\* Verification – refer paragraph 13.5.2 of this document



## Appendix II

### Examples of Transactions that May Trigger Suspicion

#### (A) Brokerage and Sales

##### (i) New Business

1. A personal lines customer for whom verification of identity proves unusually difficult, who is evasive or reluctant to provide full details or a customer whose source of funds is not clear.
2. A corporate/trust customer where there are difficulties and delays in obtaining a copy of the statements of accounts or other documents of incorporation.
3. A customer with no discernible reason for using the insurer's service, e.g. customers with distant addresses who could find the same service nearer their home base, or customers whose requirements are not in the normal pattern of or inconsistent with the insurer's business and could be more easily serviced elsewhere.
4. A customer introduced by an overseas broker, affiliate or other intermediary, when both customer and introducer are based in countries where production of drugs or drug trafficking may be prevalent.
5. Any transaction in which the insured is unknown.
6. Customer purchases products with termination features without concern for the product's investment performance.
7. Customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.

8. Customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.
  9. Customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
  10. Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include second hand endowment and bearer insurance policies.
  11. A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
  12. Payment to unrelated third party.
- (ii) Transactions which are abnormal or do not make economic sense
1. Proposals from an intermediary not in accordance with the normal business introduced.
  2. Proposals not in accordance with an insured's normal requirements, the markets in which the insured or intermediary is active and the business which the insured operates.
  3. Early cancellation of policies with return of insurance premium, for no discernible purpose or in circumstances which appear unusual.
  4. A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time.

5. Any transaction in which the nature, size or frequency appears unusual, e.g. early termination or cancellation, especially where cash had been tendered and/or the refund cheque is to a third party or a sudden purchase of a lump sum contract from an existing customer whose current contracts are small and with regular payments only.
6. Assignment of policies to apparently unrelated third parties.
7. Transactions not in accordance with normal practice in the market to which they relate, e.g. with reference to the size or class of business.
8. Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

**(B) Settlement**

**(i) Payment**

1. A number of policies taken out by the same insured for low insurance premiums, each purchased for cash and then cancelled with return of insurance premium to a third party.
2. Large or unusual payment of insurance premiums or transaction settlement by cash.
3. Overpayment of insurance premiums with a request to refund the excess to a third party or different country.
4. Payment by way of third party cheque or money transfers where there is a variation between the account holder, the signatory and the prospective insured.
5. A customer uses multiple currency equivalents (e.g. cashier's cheques and money orders) from different banks and money

services businesses to make insurance policy or annuity payments.

(ii) Disposition

1. Payment of claims to a third party without any apparent connection to the insurance policy owner.
2. Abnormal settlement instructions, including payment to apparently unconnected parties or to countries in which the insured is not known to operate.

(iii) Claims and Reinsurances

1. Strong likelihood of risks occurring, resulting in substantial claims, with consequently high insurance premiums.
2. Claims which, while appearing legitimate, occur with abnormal regularity.
3. Regular small claims within insurance premium limit.
4. Treaty reinsurances with high incidence of small claims.
5. Regular reinsurance claims paid overseas to third parties.
6. Recent change of ownership/assignment of policies just prior to a loss.
7. Abnormal loss ratios for the nature and class of risk bound under a binding authority.