GUIDELINES ON ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, COUNTERING PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS FOR LABUAN KEY REPORTING INSTITUTIONS (AML/CFT/CPF AND TFS FOR LABUAN KRIs)

PART A	**OVERVIEW**		
1	**Introduction**		**6**
2	**Legal Provisions and Scope**		**7**
3	**Applicability**		**8**
4	**Effective Date**		**10**
5	**Definition and Interpretation**		**11**
PART B	**AML/CFT/CPF/TFS REQUIREMENTS**		**29**
B.1	**Application of Risk-Based Approach**		**29**
	B.1.1	**Risk Management Functions**	**29**
	B.1.2	**ML/TF Risk Assessment**	**29**
	B.1.3	**ML/TF Risk Control and Mitigation**	**30**
	B.1.4	**PF Risk Assessment**	**31**
	B.1.5	**PF Risk Mitigation**	**32**
	B.1.6	**Customer Risk Profiling**	**32**
	B.1.7	**AML/CFT/CPF Risk Reporting**	**33**
B.2	**AML/CFT/CPF Compliance Programme**		**35**
	B.2.1	**Policies, Procedures and Controls**	**35**
	B.2.2	**Board**	**35**
	B.2.3	**Senior Management**	**36**
	B.2.4	**Compliance Management Arrangements**	**38**
	B.2.5	**Employee Screening Procedures**	**40**
	B.2.6	**Employee Training and Awareness Programme**	**40**
	B.2.7	**Independent Audit Function**	**41**
B.3	**New Products and Business Practices**		**44**
B.4	**Applicability to Labuan Financial Group, Foreign Branches & Subsidiaries**		**45**
	B.4.1	**Labuan Financial Group**	**45**
	B.4.2	**Foreign Branches and Subsidiaries**	**46**
B.5	**Customer Due Diligence (CDD)**		**47**
	B.5.1	**Standard CDD**	**50**
	B.5.2	**Simplified CDD**	**58**
	B.5.3	**Specific CDD**	**60**

	B.5.4	Enhanced CDD	60
	B.5.5	Ongoing Due Diligence	62
	B.5.6	Existing Customer – Materiality and Risk	63
	B.5.7	Non-Face-to-Face Business Relationship	63
	B.5.8	Failure to Satisfactorily Complete CDD	64
	B.5.9	CDD and Tipping-Off	64
B.6		Electronic Know-Your-Customer (e-KYC)	66
	B.6.1	Identification and Verification Through e-KYC	66
	B.6.2	Use of Artificial Intelligence, Machine Learning or Other Forms of Predictive Algorithms	67
	B.6.3	Reliance on Human Representative	68
	B.6.4	Addressing Ongoing Vulnerabilities	68
	B.6.5	Additional Safeguards to Facilitate Deployment	69
	B.6.6	Reporting Requirements	69
B.7		Politically Exposed Persons (PEPs)	70
	B.7.1	General	70
	B.7.2	Foreign PEPs	70
	B.7.3	Domestic PEPs or Person Entrusted with Prominent Function by and International Organisation	71
	B.7.4	Cessation of PEP Status	72
B.8		Reliance on Third Parties	73
	B.8.1	Customer Due Diligence	73
	B.8.2	Ongoing Due Diligence	74
B.9		Higher Risk Countries	75
B.10		Wire Transfers	77
	B.10.1	General	77
	B.10.2	Ordering Institutions	77
	B.10.3	Intermediary Institutions	79
	B.10.4	Beneficiary Institutions	80
B.11		Correspondent Banking	81
B.12		Suspicious Transaction Report	83
	B.12.1	General	83

	B.12.2 Reporting Mechanisms	84
	B.12.3 Triggers for Submission of Suspicious Transaction Report	86
	B.12.4 Internal Suspicious Transactions Report	86
B.13	Disclosure of Suspicious Transaction Report and Related Information	87
B.14	Record Keeping	89
B.15	Management Information System	90
B.16	Enforcement Orders	91
B.17	Targeted Financial Sanctions on Terrorism Financing, Proliferation Financing and under Other UN-Sanctions Regimes	92
	B.17.1 General	92
	B.17.2 Maintenance of Sanctions List	93
	B.17.3 Sanctions Screening – Customers	94
	B.17.4 Related Parties	95
	B.17.5 Freezing, Blocking and Rejecting – Customers and Related Parties	96
	B.17.6 Reporting on Positive Name Match	99
	B.17.7 Periodic Reporting on Positive Name Match	100
	B.17.8 Reporting on Suspicious Transaction	100
B.18	Submission of Regulatory Reports	102

APPENDICES

Appendix I	**List of Policy Documents to be Read Together with the Guidelines and List of Superseded Guidelines**
Appendix II	**Guidance on Application of Risk-Based Approach**
Appendix III	**Appointment of Designated Compliance Officer Form**
Appendix IV	**Methods to Identify and Verify Beneficial Owner**
Appendix V	**False Acceptance Rate and Sampling**
Appendix VI	**Reporting Template for e-KYC**
Appendix VII	**Annual Summary Report of Exposure to Customers and Beneficial Owners from High Risk Countries**
Appendix VIII	**Template for Application of Financial Intelligence Network System**
Appendix IX	**List of Transactions That May Trigger Suspicion**
Appendix X	**Relevant UNSCR and UNSC Sanctions Committee for Targeted Financial Sanctions on Proliferation Financing**
Appendix XI	**Relevant UNSCR and UNSC Sanctions Committee for Targeted Financial Sanctions on Other UN-Sanctions Regimes**
Appendix XII	**Template for Reporting upon Determination of A Positive Name Match**
Appendix XIII	**Template for Periodic Reporting on Positive Name Match**

PART A: OVERVIEW

1.0 Introduction

1.1 Money laundering, terrorism financing and proliferation financing (ML/TF/PF) remain as threats that can undermine the credibility of international financial systems. The growth in international trade, inter-linkages of the global financial system and advancement in technology have presented both the risks and opportunities to the business community. The global Anti-Money Laundering (AML) compliance has changed tremendously due to rapid digitalisation and sophisticated means over the past few years. This resulted in increasing layers of cross-border regulations being implemented to strengthen the fight against money laundering, terrorist financing, proliferation financing and other financial crimes.

1.2 In 2012, the Financial Action Task Force (FATF), had revised its Global Anti-Money Laundering, Counter-Terrorism Financing and Counter Proliferation Financing Standard (the international standards) for effective implementation by member countries to combat ML/TF as well as the financing of proliferation of weapons of mass destruction.

1.3 To uphold Labuan International Business and Financial Centre's (Labuan IBFC) commitment as a well-regulated and supervised jurisdiction, Labuan Financial Services Authority (Labuan FSA) as supervisory authority and law enforcement agency under the National Coordination Committee to Counter Money Laundering (NCC) established the *Guidelines on Anti-Money Laundering, Countering Financing Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Labuan Key Reporting Institutions* (the Guidelines) that is in line with the international standards as well as addressing the results of risk assessments undertaken by Labuan FSA. In addition, all Labuan Key Reporting Institutions (Labuan KRIs) are required to continuously assess the effectiveness of their AML/CFT/CPF Compliance Programme to ensure that it continues to remain relevant in line with the developments of Global Anti-Money Laundering, Counter-Terrorism Financing and Counter Proliferation Financing Standard.

2.0 Legal Provisions and Scope

2.1 The Guidelines are issued under Section 4A of the Labuan Financial Services Authority Act 1996 (LFSAA) and pursuant to the following provisions:

(i) In relation to AML/CFT/CPF provisions:

(a) Sections 8, 13, 14, 14A, 15, 16, 17, 18, 19, 20, and 83 of the Anti-Money Laundering, Anti-Terrorism Financing, and Proceeds of Unlawful Activities Act 2001 (AMLA);

(b) Section 28B(1) of the Labuan Financial Services Authority Act 1996;

(c) Sections 98(2), 99, 111, 175, and 176 of the Labuan Financial Services and Securities Act 2010 (LFSSA);

(d) Sections 73(2), 74, 87 and 137 of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA); and

(e) Section 109B(6) of the Labuan Companies Act 1990.

(ii) In relation to targeted financial sanctions on terrorism financing requirements:

(a) Sections 14(1)(c), 66B, 66E, and 83 of the AMLA.

(iii) In relation to targeted financial sanctions on proliferation financing requirements:

The Guidelines also serve to monitor and supervise compliance with the obligations and restrictions under the Strategic Trade Act 2010 (STA), the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010, and the Directive on Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF) issued by the Strategic Trade Controller, Ministry of Investment, Trade and Industry in June 2024, as amended or superseded from time to time.

2.2 The Guidelines set out the:

(i) Obligations of Labuan KRIs with respect to the requirements imposed under the AMLA;

(ii) Requirements imposed on Labuan KRIs in implementing a comprehensive risk-based approach in managing ML/TF/PF risks;

(iii) Requirements imposed on Labuan KRIs in implementing targeted financial sanctions relating to terrorism financing, proliferation financing and other applicable United Nations sanctions regimes; and

(iv) Roles of the Labuan KRIs' Board of Directors and Senior Management in putting in place the relevant AML/CFT/CPF measures.

2.3 Any person who fails to comply with the Guidelines may be subject to enforcement actions including an administrative penalty under Section 36G of the LFSAA and/or any other enforcement actions provided under the LFSAA and AMLA.

3.0 Applicability

3.1 The Guidelines are applicable to the following entities:

(i) Labuan banks and Labuan investment banks licensed under Part VI of the LFSSA;

(ii) Labuan Islamic banks and Labuan Islamic investment banks licensed under Part VI of the LIFSSA;

(iii) Labuan (re)insurers, including Labuan captive (re)insurers, carrying on life insurance business or life reinsurance business licensed under Part VII of the LFSSA;

(iv) Labuan (re)takaful operators, including Labuan captive (re)takaful operators, carrying on family takaful business or family retakaful business licensed under Part VII of the LIFSSA;

(v) Labuan insurance brokers arranging life insurance business or life reinsurance business licensed under Part VII of the LFSSA;

(vi) Labuan takaful brokers arranging family takaful business or family retakaful business licensed under Part VII of the LIFSSA;

(vii) Labuan trust companies and Labuan managed trust companies licensed under Part V of the LFSSA;

(viii) Labuan money-broking business and Islamic money-broking business licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively;

(ix) Labuan fund managers managing public funds and Islamic public funds licensed under Part III of the LFSSA and Part IV of the LIFSSA, respectively;

(x) Labuan securities licensees and Islamic securities licensees licensed under Part IV of the LFSSA and Part V of the LIFSSA, respectively;

(xi) Labuan exchanges established under Part IX of the LFSSA;

(xii) Labuan leasing companies and Labuan Islamic leasing companies licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively; and

(xiii) Labuan development finance business and Labuan Islamic development finance business licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively.

3.2 A Labuan KRI specified in paragraph 3.1 that undertakes digital financial services shall also comply with the applicable requirements for Labuan digital financial services (LDFS) under these Guidelines and any other relevant requirements issued by Labuan FSA.

3.3 The targeted financial sanctions requirements to combat TF, PF and to suppress other forms of armed conflict, are applicable to all Labuan financial institutions regulated or supervised by Labuan FSA.

3.4 The Guidance Note on Anti-Money Laundering and Counter Financing of Terrorism for Labuan Specified Entities sets out proportionate AML/CFT requirements and recommended best practices for entities other than Labuan KRI that are identified in the Guidance Note as Labuan Specified Entities.

3.5 The Guidelines are also intended to complement and be read together with other applicable Guidelines, Directives or Circulars issued by Labuan FSA as set out in **Appendix I**. In addition, Labuan KRIs may refer to the list of superseded Guidelines under **Appendix I**.

3.6 The requirement of this Guidelines are 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.

3.7 Where the Labuan KRIs are subject to more than one AML/CFT/CPF matters issued pursuant to Section 83 of the AMLA, the more stringent requirements shall apply.

4.0 Effective Date

4.1 The Guidelines shall come into effect on **28 October 2026** and would remain effective and applicable unless amended or revoked.

4.2 Compliance to the requirements outlined in this policy document shall take effect immediately, unless otherwise specified by Labuan FSA.

5.0 Definition and Interpretation

5.1 The terms and expressions used in the Guidelines shall have the same meaning as provided in the AMLA, LFSSA and LIFSSA, as the case may be, unless otherwise defined in the Guidelines or the context requires otherwise.

5.2 For the purpose of the Guidelines, the following definitions and interpretations apply:

Definition and Interpretation	
"accurate information"	Refers to information that has been verified for accuracy. 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.
"beneficial owner"	In the context of legal person, 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. 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. 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. In insurance and takaful sectors, this also refers to any natural person(s) who ultimately owns or controls a beneficiary, as specified in the Guidelines.

Definition and Interpretation	
	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 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. Reference to "ultimate effective control" over trusts or similar legal arrangements includes situations in which ownership or control is exercised through a chain of ownership or control.
"beneficiary"	This is dependent on the context of which the term is used as follows: (a) In trust law, beneficiary refers to the person or persons who are entitled to 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

Definition and Interpretation	
	trust. 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; (b) In foundation law, beneficiary refers to the person or persons who are entitled to benefit of any foundation arrangement. A beneficiary can be a natural or legal person or arrangement. All foundations (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While foundations must always have some ultimately ascertainable beneficiary, foundations 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 council member's discretion in the case of a discretionary foundation. The accumulation period is normally co-extensive with the foundation's perpetuity period which is usually referred to in the charter as the foundation's period. (c) For wire transfers, this refers to the natural or legal person or legal arrangement identified by the originator as the receiver of the requested wire transfer; (d) In relation to clubs, societies and charities, this 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; or

Definition and Interpretation	
	(e) In the context of insurance and takaful business, a beneficiary refers to the natural or legal persons, or a legal arrangement, or insured person under an insurance policy or takaful certificate, or nominees, 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 or takaful certificate.
"beneficiary account"	Includes trust accounts, nominee accounts, fiduciary accounts, accounts opened for companies with nominee shareholders, accounts for mutual fund and fund managers, accounts for personal asset holding vehicles, pooled accounts, accounts opened by professional third parties and other relevant accounts.
"beneficiary institutions"	Refers to the institution which receives the wire transfer from the ordering institution directly or through an intermediary institution and makes the funds available to the beneficiary.
"Board"	This refers to the board of directors of the Labuan KRI, including a committee of the boards to which responsibilities of the board set out in the Guidelines to oversee the AML/CFT/CPF functions have been delegated. In relation to the Labuan KRI of a branch status, the 'Board' shall refer to the Labuan KRI's regional/parent company or any equivalent person or body with the authority to oversee the branch, whichever is relevant.
"close associate of PEP"	Refers to any individual closely connected to a politically exposed person (PEP), either socially or professionally. A close associate in this context includes:

Definition and Interpretation	
	(a) extended family members, such as relatives (biological and 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 (f) close friends.
"Competent Authority"	Refers to Bank Negara Malaysia.
"Core Principles"	Refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Core Principles issued by the International Association of Insurance Supervisors.
"correspondent bank"	Refers to a Labuan KRI that provides or intends to provide correspondent banking services.
"cover payment"	Refers to a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution where the routing of the funding instruction (the cover) is carried out or performed through one or more intermediary institutions.
"cross-border wire transfer"	Refers to any wire transfer where the ordering institution and beneficiary institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the institutions involved is located in a different country.

Definition and Interpretation	
"customer"	Refers to both account holder and non-account holder. The term also refers to a client. For insurance and takaful business, refers to parties related to an insurance/takaful contract including potential parties such as proposer/policyholder/policy owner, payor, assignee and company representative. In the case of group policies, "customer" refers to the master policy holder, that is, the owner of the master policy issued or intended to be issued. In the context of Targeted Financial Sanctions on Terrorism Financing, Proliferation Financing and under Other UN-Sanctions Regimes, this includes beneficiary and beneficial owner.
"customer due diligence (CDD)"	Refers to any measure undertaken pursuant to section 16 of the AMLA.
"director"	Refers to any person, by whatever name called, who: (a) occupies the position of director of a body corporate; (b) is a person in accordance with whose directions or instructions the directors of such a body corporate accustomed to act on; or (c) an alternate or substitute director.
"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.
"domestic wire transfers"	Refers to any wire transfer where the ordering institution and beneficiary institution are located in Malaysia. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of Malaysia, even

Definition and Interpretation	
	though the system used to transfer the payment message may be located outside Malaysia.
"electronic Know Your Customer (e-KYC)"	Refers to establishing business relationships and conducting Customer Due Diligence (CDD) by way of electronic means, including online and mobile channels.
"expatriate"	Refers to a foreign national who meets the eligibility criteria for expatriate employment and is approved by the Immigration Department of Malaysia (Ministry of Home Affairs) to be employed in Malaysia.
"external service arrangement"	This refers to an arrangement in which a service provider performs an activity on behalf of the Labuan KRI on a continuing basis[1], where the activity would otherwise be undertaken by the Labuan KRI.
"family members of PEP"	Refers to individuals who are related to a PEP either directly (consanguinity) or through marriage. A family member in this context, includes: (a) parent; (b) sibling; (c) spouse; (d) child; or (e) spouse's parent, for both biological or non-biological relationships.
"financial group"	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 branches and/or subsidiaries that are subjected to AML/CFT/CPF policies and procedures at the group level.

[1] For the avoidance of doubt, an agreement which is time-bound does not preclude the activity from being considered as being performed on a continuing basis.

Definition and Interpretation	
"financing of proliferation" or "proliferation financing"	Refers to the act of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purpose of weapons of mass destruction (WMD) proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purpose).
"G"	Denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted by the Labuan KRI.
"higher risk"	Refers to circumstances where the Labuan KRI assesses the ML/TF/PF risks as higher, taking into consideration, but not limited to the following factors: (i) Customer risk factors: (a) the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Labuan KRI and the customer); (b) non-resident customers; (c) legal persons or arrangements that are personal asset-holding vehicles; (d) companies that have nominee shareholders or shares in bearer form; (e) businesses that are cash-intensive; (f) the ownership structure of the company appears unusual or excessively complex given the nature of its business; (g) high net worth individuals;

Definition and Interpretation	
	(h) persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling); (i) businesses or activities identified by the FATF as having higher risk for ML/TF/PF; (j) legal arrangements that are complex (e.g. nominee relationships or layering with legal persons); and (k) persons who match the red flag criteria of the Labuan KRI. (ii) Country or geographic risk factors: (a) countries identified by credible sources, such as mutual evaluation or published follow-up reports, as having inadequate AML/CFT/CPF systems; (b) countries subject to sanctions, embargos or similar measure issued by, for example, the United Nations; (c) countries identified by the FATF, other FATF style regional bodies or other international bodies as having higher ML/TF/PF risk; (d) countries identified by credible sources as having significant levels of corruption or other criminal activities; and (e) 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. (iii) Product, services, transaction or delivery channel risk factors:

Definition and Interpretation	
	(a) anonymous transactions (which may include cash); (b) non-face-to-face business relationships or transactions; (c) payment received from multiple persons and/or countries that do not match the person's nature of business and risk profile; and (d) payment received from unknown or unrelated third parties.
"higher risk countries"	Refers to countries identified by FATF or Government of Malaysia that pose a risk to the international financial system.
"intermediary institution"	Refers to the institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.
"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: (a) United Nations and its affiliated international organisations; (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;

Definition and Interpretation	
	(c) military international organisations such as the North Atlantic Treaty Organization; and (d) economic organisations such as the World Trade Organization.
"Labuan financial institution"	Refers to a Labuan financial institution as defined in paragraph (a) of the definition of "Labuan financial institution" in subsection 2(1) of the LFSAA.
"Labuan Key Reporting Institution" or "Labuan KRI"	Refers to a reporting institution under the First Schedule of AMLA that falls within the categories specified in paragraph 3.1 and is subject to the Guidelines.
"law enforcement agencies (LEAs)"	Refers to government agencies responsible for enforcing the law.
"LDFS"	Refers to a Labuan KRI undertaking digital financial business including dealing with digital assets.
"legal arrangement"	Refers to a contractual arrangement between the person who provides the funds or other assets and specifies the terms (the settlor) and the person with control over the funds or other assets (the trustee) for the benefit of those who benefit the trust (the beneficiaries). This relates to express trusts or other similar legal arrangements.
"legal person"	Refers to any entity other than a natural person that can establish a permanent customer relationship with a firm or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLC), foundations, partnerships, or associations and other similar entities. GLC refers to an entity where the government is the majority shareholder or single largest shareholder and

Definition and Interpretation	
	has the ability to exercise and/or influence major decisions such as appointment of board members and senior management.
"mobile channel"	Refers to conducting transactions through any electronic device using a mobile application provided by the Labuan KRI.
"National Risk Assessment (NRA)"	Reference to NRA under section B.1 of this policy document is not limited to the National ML/TF/PF Risk Assessment and includes any sectoral, thematic or emerging risk assessments undertaken by the NCC.
"nominator"	Refers to an individual (or group of individuals) or legal persons that issues instructions (directly or indirectly) to a nominee to act on its behalf in the capacity of a director or a shareholder, also sometimes referred to as a "shadow director" or "silent partner'.
"nominee director and shareholder"	Refers to an individual or legal person instructed by another individual or legal person ("the nominator") to act on its behalf in a certain capacity regarding a legal person. A Nominee 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 and indirect instructions of the nominator. A Nominee Director is never the beneficial owner of a legal person. 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.

Definition and Interpretation	
"occasional transaction"	Refers to transactions carried out by non-account holder or account holder who conducts transactions that are not normal and customary to the account profile of the customer.
"online channel"	Refers to conducting transactions through any electronic device other than transactions conducted via the mobile channel.
"ordering institution"	Refers to the institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
"originator"	Refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering institution to perform the wire transfer.
"payment instrument"	Refers to any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services, or to make payment.
"payable through account"	Refers to correspondent accounts that are used directly by a third party to transact business on their own behalf.
"person"	Includes a body of persons, corporate or unincorporate.
"person conducting the transaction"	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.
"politically exposed persons (PEPs)"	Refers to: (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

Definition and Interpretation	
	state-owned corporations and important political party officials; (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), judicial or military officials, senior executives of state-owned corporations and important political party officials; or (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. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
"registered persons"	Refers to the registered persons specified under Financial Services Act 2013 and Islamic Financial Services Act 2013.
"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 designated person; and (b) a person acting on behalf or at the direction of a designated person. Based on the above, it may extend to shareholders, directors, authorised person, senior management and also the beneficial owner.

Definition and Interpretation	
"related party"	For Targeted Financial Sanction on Terrorism Financing, this 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. For Targeted Financial Sanctions on Proliferation Financing and Under UN-Sanctions Regime, this 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.
"remittance account"	Refers to a customer account which contains customer information including personal details and remittance transaction records of the customer that is maintained by a Labuan KRI.
"respondent institution"	Refers to financial institutions outside Malaysia to which correspondent banking services in Malaysia are provided.
"satisfied"	Where reference is made to a Labuan KRI being "satisfied" as to a matter, the Labuan KRI must be able to justify its assessment to the Labuan FSA.
"Senior Management"	Refers to the principal officer, any officer(s) or committee performing a senior management function who reports to the Board of the Labuan KRI and is principally accountable for: (a) Making decisions that affect the whole, or a substantial part of, the Labuan KRI's business;

Definition and Interpretation	
	(b) Implementing and enforcing policies and strategies approved by the Board including Head of Department or any equivalent designated person; or (c) Internal controls and processes of the Labuan KRI which include a compliance officer, designated compliance officer, shariah adviser, member of Internal Shariah Advisory Board, chief internal auditor, appointed actuary and head of risk management.
"serial payment"	Refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution directly or through one or more intermediary institutions (e.g. correspondent banks).
"shell bank"	Refers to a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
"straight - through processing"	Refers to payment transactions that are conducted electronically without the need for manual intervention.
"targeted financial sanctions"	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 the Minister of Home Affairs.

Definition and Interpretation	
"third parties"	Refers to reporting institutions that are supervised by a relevant competent authority and that meet the requirements under section B.8 on Reliance on Third Parties, namely persons or businesses who are relied upon by the Labuan KRI to conduct the customer due diligence process. Reliance on third parties often occurs through introductions made by another member of the same financial group or by another financial institution. This definition does not include external service arrangements or agency relationships because the external service provider or agent is regarded as synonymous with the Labuan KRI.
"unique transaction reference number"	Refers to a combination of letters, numbers, or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
"UNSCR List"	(i) For Targeted Financial Sanction on Terrorism Financing, this 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. (ii) For Targeted Financial Sanctions on Proliferation Financing, this refers to names and particulars of persons as designated by the UNSC or its relevant Sanction Committee and are deemed as designated

Definition and Interpretation	
	persons under the relevant Strategic Trade Act 2010 (STA) subsidiary legislation. (iii) For Targeted Financial Sanctions under Other UN-Sanctions Regime, this 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 Central Bank of Malaysia Act 2009 (CBA) Regulations.
"up-to-date information"	Refers to information which is as current and up-to-date as possible, and is updated within a reasonable period following any change.
"wire transfer"	Refers to any transaction carried out on behalf of an originator through an institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

PART B AML/CFT/CPF/TFS REQUIREMENTS

B.1 Application of Risk-Based Approach

FATF Recommendation 1:

Risk-Based Approach (RBA) is to be applied to ensure that measures to prevent or mitigate money laundering, terrorist financing and proliferation financing commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering, countering the financing of terrorism and countering proliferation financing (AML/CFT/CPF) regime and the implementation of risk-based measures throughout the FATF Recommendations.

B.1.1 Risk Management Functions

6.1 A Labuan KRI shall implement appropriate risk-based approach in managing ML/TF/PF risks and targeted financial sanctions requirements.

6.2 In the context of a "Risk-Based Approach", the intensity and extensiveness of risk management function shall be proportionate to the nature, scale and complexity of the Labuan KRI's activities and its ML/TF/PF risk profile.

6.3 The Labuan KRI's AML/CFT/CPF risk management function must be aligned and integrated with its overall risk management control function.

B.1.2 ML/TF Risk Assessment

6.4 A Labuan KRI is required to take appropriate steps to identify, assess and understand their ML/TF risks, in relation to its customers, countries or geographical areas and products, services, transactions or delivery channels, and other relevant risk factors.

6.5 In assessing ML/TF risks, Labuan KRI is required to have the following processes in place:

(i) documenting its risk assessments and findings;

(ii) 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;

(iii) keeping the assessment up-to-date through a periodic review; and

(iv) having appropriate mechanisms to provide risk assessment information to Labuan FSA upon request.

6.6 A Labuan KRI is required to conduct additional assessment as and when required by Labuan FSA.

6.7 A Labuan KRI shall be guided by the results of the National Risk Assessment (NRA) issued by the NCC in conducting its own risk assessments and shall take enhanced measures to manage and mitigate the risks identified in the NRA.

G 6.8 In conducting the risk assessment in paragraph 6.4, a Labuan KRI may consider whether:

(i) it is susceptible to the key and emerging crimes as well as higher risk sectors identified in the NRA when assessing its institutional ML/TF risk; and

(ii) enhancements to the AML/CFT Compliance Programme are warranted to ensure any areas of higher ML/TF risk are appropriately mitigated.

B.1.3 ML/TF Risk Control and Mitigation

6.9 A Labuan KRI is required to:

(i) have policies, procedures and controls to manage and mitigate ML/TF risks that have been identified;

(ii) monitor the implementation of those policies, controls, procedures and enhance them where necessary; and

(iii) take enhanced measures to manage and mitigate risks where higher risks are identified and where specified by the competent authority or Labuan FSA.

6.10 A Labuan KRI shall conduct independent control testing on the policies, procedures and controls for the purpose of monitoring the implementation of paragraph 6.9(ii) requirements.

B.1.4 PF Risk Assessment

6.11 A Labuan KRI is 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 section B.17 of this policy document.

G 6.12 In conducting the risk assessment, a Labuan KRI 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.

6.13 For the purpose of paragraph 6.11, a Labuan KRI is 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.

6.14 In assessing the PF risks, a Labuan KRI is required to have the following processes in place:

(i) documenting their PF risk assessments and findings;

(ii) keeping the assessment up-to-date through a periodic review; and

(iii) having appropriate mechanisms to provide PF risk assessment information to the supervisory authority.

6.15 A Labuan KRI shall be guided by the results of the NRA and related thematic risk assessment issued in conducting their own risk assessment and shall take enhanced measures to manage and mitigate the risks identified in the NRA.

B.1.5 PF Risk Mitigation

6.16 A Labuan KRI is required to:

(i) have policies, procedures and controls to manage and mitigate PF risks that have been identified;

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

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

(a) where higher PF risks are identified, a Labuan KRI shall introduce enhanced controls to detect possible breaches, non-implementation or evasion of targeted financial sanctions on PF under section B.17 of this policy document; and

(b) where lower PF risks are identified, a Labuan KRI 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 section B.17 of this policy document.

6.17 A Labuan KRI shall ensure full implementation of the targeted financial sanctions on PF under section B.17 of this policy document irrespective of the institutional PF risk level.

B.1.6 Customer Risk Profiling

6.18 A Labuan KRI is required to conduct risk profiling on its customers and assign ML/TF/PF risk rating that commensurate with their risk profile.

6.19 Risk profiling must consider the following factors:

(i) customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of politically exposed persons (PEPs), types of occupation);

(ii) country or geographic risk (e.g. location of business, origin of customers);

(iii) products, services, transactions or delivery channels (e.g. cash-based, face-to-face or non-face-to-face, cross-border); and

(iv) any other information suggesting that the customer is of higher risk.

G 6.20 In identifying countries and geographic risk factors under paragraph 6.19(ii), a Labuan KRI 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.

6.21 The risk control and mitigation measures implemented by a Labuan KRI shall commensurate with the risk profile of type or particular of customer.

6.22 After the initial acceptance of the customer, a Labuan KRI is required to regularly review and update the customer's risk profile based on their level of ML/TF/PF risks.

B.1.7 AML/CFT/CPF Risk Reporting

6.23 A Labuan KRI shall provide timely reporting of the risk assessment, ML/TF/PF risk profile and the effectiveness of risk control and mitigation measures to the Board and Senior Management. The reporting frequency shall commensurate with the level of risks involved and the Labuan KRI's operating circumstances.

G 6.24 The report referred to under paragraph 6.23 may include the following:

(i) results of AML/CFT/CPF monitoring activities carried out by the Labuan KRI such as the level of its exposure to ML/TF/PF risks, break-down of the ML/TF/PF risk exposures based on key activities or customer segments, trends of suspicious transaction reports, trends of orders received from law enforcement agencies (LEAs);

(ii) details of recent significant risk events, that occur either internally or externally, modus operandi and its impact or potential impact to the Labuan KRI; and

(iii) recent developments in AML/CFT/CPF laws and regulations, and its implications to the Labuan KRI.

G 6.25 A Labuan KRI may refer to the guidance in **Appendix II** and the FATF guidance papers on the application of RBA.

B.2 AML/CFT/CPF Compliance Programme

B.2.1 Policies, Procedures and Controls

7.1 A Labuan KRI is required to implement AML/CFT/CPF programmes which correspond to its ML/TF/PF risks as well as the size and nature of its business.

B.2.2 Board

General

7.2 The Board must understand their roles and responsibilities in managing ML/TF/PF risks identified by the Labuan KRI.

7.3 The Board must be cognisant of the ML/TF/PF risks associated with the business strategies or activities, delivery channels and geographical coverage of the Labuan KRI's business products and services.

7.4 The Board must understand the AML/CFT/CPF measures required by the relevant laws and instruments issued under the AMLA, as well as industry's standards and best practices in implementing AML/CFT/CPF measures.

Roles and Responsibilities

7.5 The Board has the following roles and responsibilities:

(i) Maintain accountability and oversight for establishing AML/CFT/CPF policies and minimum standards;

(ii) approve policies regarding AML/CFT/CPF measures within the Labuan KRI, including those required for risk assessment, mitigation and profiling, customer due diligence (CDD), record keeping, enhanced CDD and ongoing due diligence, suspicious transaction report and targeted financial sanctions;

(iii) approve appropriate mechanisms to ensure the AML/CFT/CPF policies are periodically reviewed and assessed in line with changes and developments in the Labuan KRI's products and services, technology as well as trends in ML/TF/PF;

(iv) approve an effective internal control system for AML/CFT/CPF and maintain adequate oversight of the overall AML/CFT/CPF measures undertaken by the Labuan KRI;

(v) 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;

(vi) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF/PF;

(vii) assess the implementation of the approved AML/CFT/CPF policies through regular reporting and updates by the Senior Management and Audit Committee; and

(viii) establish a Management Information System (MIS) that is reflective of the nature of the Labuan KRI's operations, size of business or activities, complexity of business operations or activities and structure, risk profiles of products and services offered as well as geographical coverage.

B.2.3 Senior Management

7.6 The Senior Management is accountable for implementing and managing AML/CFT/CPF compliance programmes in accordance with policies and procedures established by the Board, as well as the requirements of the applicable legislations, regulations and industry's standards and best practices.

Roles and Responsibilities

7.7 The Senior Management has the following roles and responsibilities:

(i) be aware of and understand the ML/TF/PF risks associated with business strategies or operations, delivery channels and geographical coverage of its business products or activities and services offered and to be offered. This includes new products or activities, new delivery channels and new geographical coverage;

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

(iii) 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;

(iv) undertake review of AML/CFT/CPF policies and propose to the Board the necessary enhancements to them in order to reflect changes in the Labuan KRI's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

(v) provide timely periodic reporting to the Board on the level of ML/TF/PF risks facing by the Labuan KRI, 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 Labuan KRI;

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

(vii) appoint a Compliance Officer at management level at the parent company and designate a Compliance Officer at management level at each branch or subsidiary. In this regard, a Labuan KRI is required to submit the application on the appointment of Designated Compliance Officer to Labuan FSA using the format as set out in **Appendix III;**

(viii) provide appropriate levels of AML/CFT/CPF training for its employees at all levels within the organisation;

(ix) 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;

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

(xi) ensure the integrity of its employees by establishing appropriate employee assessment system.

B.2.4 Compliance Management Arrangements

7.8 The Compliance Officer acts as the reference point for AML/CFT/CPF matters within the Labuan KRI.

7.9 The Compliance Officer must have sufficient stature, authority and seniority within the Labuan KRI to participate and be able to effectively influence decisions relating to AML/CFT/CPF.

7.10 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT/CPF responsibilities effectively.

7.11 For the purpose of paragraph 7.10, "fit and proper" shall include minimum criteria relating to:

(i) probity, personal integrity and reputation;

(ii) competency and capability; and

(iii) financial integrity.

7.12 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 7.13 The Compliance Officer is encouraged to have professional qualifications, certified AML/CFT/CPF Compliance Officer qualification or any relevant certification to carry out his responsibilities effectively.

G 7.14 In addition to formal qualifications, the Compliance Officer should have at least two (2) years of relevant experience with regard to the respective Labuan KRI's business.

7.15 The Compliance Officer must not be placed in a position or situation of potential conflict of interest vis-à-vis his responsibilities. In addition, the Compliance Officer should not be susceptible to undue influence regarding the manner and extent to which they are expected to perform their compliance duties. A Labuan KRI is required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

7.16 The Compliance Officer is responsible for ensuring the following matters:

(i) compliance with the AML/CFT/CPF requirements;
(ii) proper implementation of AML/CFT/CPF policies by the Labuan KRI;
(iii) effective implementation of appropriate AML/CFT/CPF procedures, including CDD, record-keeping, ongoing due diligence, suspicious transaction report and targeted financial sanctions;
(iv) regular assessment of AML/CFT/CPF mechanism such that it is effective and sufficient to address any change in ML/TF/PF trends;
(v) channels of communication from the respective employees to the branch or subsidiary Compliance Officer and subsequently to the Compliance Officer is secured and information is kept confidential;
(vi) all employees are aware of the Labuan KRI's AML/CFT/CPF measures, including policies, control mechanisms and reporting channels;
(vii) establish and maintain relevant internal criteria (red-flags) to enable identification and detection of suspicious transactions;
(viii) evaluate internal generated suspicious transaction reports appropriately before being promptly reported to the Financial Intelligence Department (FInD), Bank Negara Malaysia and AML Policy Unit of Labuan FSA;
(ix) proper identification of ML/TF/PF risks associated with new products or services or risks arising from the Labuan KRI's operational changes, including the introduction of new technology and processes; and
(x) compliance with any other obligations that are imposed under the Guidelines.

7.17 In the event where the compliance officer's role was left vacant, the Labuan KRI shall notify Labuan FSA within ten working days on the vacancy and shall identify the replacement officer within thirty days from the date of vacancy. In the case where that vacancy was due to the dismissal of the Compliance Officer by the

Labuan KRI, the notification to Labuan FSA shall also be accompanied by an explanation for the compliance officer's dismissal.

B.2.5 Employee Screening Procedures

7.18 A Labuan KRI is required to establish an employee assessment system or procedures that commensurate with the nature, size and complexity of its business operations and ML/TF/PF risk exposure.

7.19 The screening procedures under the employee assessment system or procedures shall apply upon hiring the employee and throughout the course of employment.

7.20 The employee assessment under paragraph 7.18 shall include:

(i) an evaluation of an employee's personal information, including criminal records, employment and financial history; and

(ii) clear parameters or circumstances to trigger re-screening of employees during the course of their employment.

G 7.21 In conducting financial history assessment, a Labuan KRI may require employees to submit relevant credit reports or to complete self-declarations on the required information.

7.22 A Labuan KRI shall maintain comprehensive records of documents and information relating to, or relied on in, the employee screening process.

7.23 For a Labuan KRI that employs a Trust Officer, the employee is to adhere to the roles and responsibilities outlined under the Guidelines for Labuan Trust Officers issued by Labuan FSA.

B.2.6 Employee Training and Awareness Programmes

7.24 A Labuan KRI 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.

7.25 The employees must be made aware that they can be held personally liable for any failure to observe the AML/CFT/CPF requirements.

7.26 A Labuan KRI 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:

(i) the relevant documents on AML/CFT/CPF issued by Labuan FSA; and

(ii) the Labuan KRI's internal AML/CFT/CPF policies and procedures.

7.27 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 a Labuan KRI.

7.28 Employees who deal directly with customers shall be trained on AML/CFT/CPF prior to dealing with the customer.

G 7.29 Training to all employees may need to include a general background on ML/TF/PF, the requirements of CDD as well as obligations to monitor and report suspicious transactions to the Compliance Officer.

G 7.30 In addition, training may be provided to specific categories of employees depending on the nature and scope of their functions:

(i) employees who deal directly with customers or establish business relationships may be trained to conduct CDD and ongoing due diligence, including circumstances where enhanced CDD is required in higher risk situations. This includes detecting suspicious transactions and taking necessary measures upon determining a transaction to be suspicious; and

(ii) employees who are supervisors and managers may be trained on the overall aspects of AML/CFT/CPF procedures and the appropriate risk-based approach to CDD. This includes consequences of non-compliance with requirements set out under the Guidelines.

B.2.7 Independent Audit Function

7.31 The Board shall ensure regular independent audits of the internal AML/CFT/CPF measures to determine their effectiveness and compliance against:

(i) The AMLA and its subsidiary legislations and instruments issued under the AMLA; and

(ii) Guidelines and circulars on AML/CFT/CPF or other relevant requirements issued by Labuan FSA.

7.32 In this regard, the Board would need to determine and ensure that the frequency and scope of independent audits conducted by the Labuan KRI commensurate with its ML/TF/PF risks and vulnerabilities.

7.33 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:

(i) checking and testing the compliance with the AML/CFT/CPF policies, procedures and controls, and effectiveness thereof; and

(ii) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT/CPF requirements.

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

(i) compliance with the AMLA, its subsidiary legislation and instruments issued under the AMLA as well as guidelines and circulars on AML/CFT/CPF or other relevant requirements issued by Labuan FSA;

(ii) compliance with the Labuan KRI's internal AML/CFT/CPF policies and procedures;

(iii) adequacy and effectiveness of the AML/CFT/CPF compliance programme; and

(iv) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

G 7.35 In determining the frequency of the independent audit under paragraph 7.32, a Labuan KRI may be guided by the following circumstances:

(i) structural changes to the business of the Labuan KRI such as mergers and acquisitions;

(ii) changes to the number or volume of transactions reported to Labuan FSA;

(iii) introduction of new products and services or new delivery channels; or

(iv) previous non-compliance in relation to AML/CFT/CPF requirements.

7.36 Notwithstanding paragraph 7.34 and 7.35, a Labuan KRI shall comply with additional requirements on the frequency and scope of the independent audit as specified by Labuan FSA.

7.37 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.

7.38 A Labuan KRI must ensure that such audit findings and the necessary corrective measures undertaken are made available to Labuan FSA and relevant supervisory authorities upon request.

B.3 New Products and Business Practices

FATF Recommendation 15:

Financial institutions should identify and assess the money laundering, terrorist financing or proliferation financing risks that may arise in relation to:

(i) the development of new products and new business practices, including new delivery mechanisms; and

(ii) the use of new or developing technologies for both new and pre-existing products.

8.1. A Labuan KRI is required to identify and assess the ML/TF/PF risks that may arise in relation to the development of new products, services and business practices, including new digital assets, delivery mechanisms, and the use of new or developing technologies whether for new or existing solutions.

8.2. A Labuan KRI is required to:

(i) undertake the risk assessment prior to the launch or adoption of such new products, services, business practices and technologies;

(ii) take appropriate measures to manage and mitigate the risks; and

(iii) document the risk assessment in writing.

B.4 Applicability to Labuan Financial Group, Foreign Branches & Subsidiaries

FATF Recommendation 18:

Financial groups should be required to implement group-wide programmes against money laundering, terrorist financing and proliferation financing, including policies and procedures for sharing information within the group for AML/CFT/CPF purposes.

B.4.1 Labuan Financial Group

9.1 A parent company incorporated in Labuan is required to implement group-wide programmes against ML/TF/PF.

9.2 These programmes must be applicable and appropriate to all branches and subsidiaries of the group. These shall include the following measures:

(i) framework for AML/CFT/CPF Compliance programme at the group level;

(ii) appoint a Group Compliance Officer at management level of the Labuan parent company;

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

(iv) the provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes; and

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

9.3 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 necessary authorisation to issue directions to the branches and subsidiaries within the Group.

B.4.2 Foreign Branches and Subsidiaries

9.4 A Labuan KRI is required to closely monitor its foreign branches or subsidiaries operating in jurisdictions with strategic deficiency in AML/CFT/CPF laws and regulations as highlighted by the FATF or the Government of Malaysia.

9.5 A Labuan KRI shall ensure that its foreign branches and subsidiaries apply AML/CFT/CPF measures which at the minimum should meet the more stringent of:

(i) AML/CFT/CPF requirements in jurisdictions where they are operating in; or

(ii) requirements under the Guidelines.

9.6 If the host country does not permit the proper implementation of AML/CFT/CPF measures that are consistent with the AML/CFT/CPF requirements in Labuan, the Labuan KRI and its financial group are required to apply additional measures to manage the ML/TF/PF risks. In addition, they are also required to report to Labuan FSA on the AML/CFT/CPF gaps including additional measures implemented to address them.

G 9.7 The Labuan KRI and its financial group may consider ceasing operations of its branch or subsidiary should they be unable to effect the necessary mitigating controls as required under paragraph 9.6.

B.5 Customer Due Diligence (CDD)

FATF Recommendation 10:

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when establishing business relations, carrying out occasional transactions, suspicion of money laundering, terrorist financing or proliferation financing and has doubt about the veracity or adequacy of previously obtained customer identification data.

Paragraph 10.1 (ii) and (iii) are only applicable to Labuan Banks and LDFS

10.1 A Labuan KRI is required to conduct CDD on customers and persons conducting the transaction, when:

(i) establishing business relations;

(ii) providing wire transfer services;

(iii) providing electronic-money (e-money);

(iv) it has any suspicion of ML/TF/PF, regardless of amount; or

(v) it has any doubt about the veracity or adequacy of previously obtained information.

10.2 A Labuan KRI shall refer to section B.5.3 on specific CDD measures in relation to paragraphs 10.1 (ii) and (iii).

10.3 When conducting CDD, a Labuan KRI is required to:

(i) identify the customer and verify the identity using reliable, independent source documents, data or information;

(ii) identify and verify the identity of the authorised person whom acting on behalf of the customer;

(iii) 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 Labuan KRI is satisfied that it knows who the beneficial owner is; and

(iv) understand, and where relevant, obtain information on the purpose and intended nature of the business relationship.

10.4 When a Labuan KRI conducts CDD on a customer which is a Labuan financial institution, a Labuan KRI is also required to:

(i) take into consideration the relevant results of the NRA in line with paragraphs 6.7 and 6.15, where applicable, and any relevant sectoral or thematic risk assessments issued or communicated by Labuan FSA; and

(ii) assess the ML/TF/PF risks associated with the customer and business relationship in accordance with the applicable requirements under section B.1, taking into consideration all relevant risk factors.

10.5 Based on the assessments conducted under paragraphs 10.4 (i) and (ii), a Labuan KRI shall:

(i) Refrain from blanket de-risking, and ensure that any decision to decline, restrict or terminate a business relationship on ML/TF/PF risk grounds is supported by an assessment of the individual customer and business relationship, taking into consideration whether the identified risks can be effectively mitigated, except where such action is required under these Guidelines or applicable law;

(ii) determine and apply CDD measures commensurate with the risks identified; and

(iii) document the assessment and reasons for the decision.

A Labuan KRI may refer to paragraph 4.11 of **Appendix II** for further guidance.

10.6 Where information or record obtained during CDD process are in foreign language, the Labuan KRI is required to have and maintain a translation of the same in National or English language. The translation shall be made available to Labuan FSA upon request.

10.7 In conducting CDD, a Labuan KRI is required to comply with requirements on targeted financial sanctions, specified under section B.17, in relation to:

(i) terrorism financing;

(ii) proliferation financing of weapons of mass destruction; and

(iii) other UN-sanctions.

Verification

10.8 A Labuan KRI 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 Labuan KRI deem necessary.

10.9 A Labuan KRI shall determine the extent of verification method that commensurate with the identified ML/TF/PF risks.

10.10 A Labuan KRI must be satisfied with the veracity of the information referred to in paragraph 10.7 when verifying the identity of customer or beneficial owner.

10.11 A Labuan KRI shall verify the identity of the customer or beneficial owner before, or during, the course of establishing a business relationship or conducting a transaction for an occasional customer.

Verification on Insurance Policy/Takaful Certificate

10.12 A Labuan KRI is not required to conduct verification on insurance policy/takaful certificate owners sold via any banking institutions if they are satisfied that prior verification has been conducted by the said banking institution. Such reliance is permitted provided it is made in accordance to section B.8 of the Guidelines.

G

10.13 A Labuan KRI may choose not to conduct further verification on previously conducted CDD in the following circumstances:

Paragraph 10.12-10.14 are only applicable to Labuan (re)insurers and Labuan (re)takaful operators

(i) for renewal and reinstatement of policies or certificates with no significant changes to the terms and conditions of the insurance policy/takaful certificate (including benefits under the insurance policy/takaful certificate); or

(ii) for applications of pure insurance/takaful covers which do not provide for payment of surrender values, including hospital and surgical insurance, critical illness insurance and pure term life insurance/family takaful covers.

G 10.14 A Labuan KRI may use the following measures to verify the identity of non-face-to-face customer such as:

(i) requesting additional documents to complement the requirements within section B.5.1;

(ii) developing independent contact with customer; or

(iii) verifying customer information against any database maintained by any relevant authority.

B.5.1 Standard CDD

Individual Customer and Beneficial Owner

10.15 In conducting CDD, the Labuan KRI is required to identify an individual customer and beneficial owner, by obtaining at least the following information:

(i) full name;

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

(iii) residential and mailing address;

(iv) date of birth;

(v) nationality;

(vi) occupation type;

(vii) name of employer or nature of self-employment or nature of business;

(viii) contact number and/or any contact details including email address; and

(ix) purpose of the transaction.

10.16 A Labuan KRI shall identify and verify the identity of the customer and the beneficial owner. For this purpose, the Labuan KRI may refer to the guidance provided in **Appendix IV**.

Beneficiaries

10.17 In addition to the CDD measures required under paragraph 10.3, a Labuan KRI is also required to conduct the following CDD measures on the beneficiary, as soon as the beneficiary is identified or designated:

Paragraph 10.17-10.19 are only applicable to Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

(i) for a beneficiary that is identified as a specifically named natural person, the following needs to be ascertained:

(a) full name;

(b) NRIC number or passport number or reference number of any other official documents of the beneficiary;

(c) date of birth;

(d) address (type of address i.e. mailing/office); and

(e) contact number and/or any contact details including email address

(ii) for a beneficiary that is identified as a specifically named legal person or legal arrangement, the following needs to be ascertained:

(a) name, legal form and proof of existence;

(b) date of incorporation;

(c) address (type of address i.e. registered office); and

(d) contact number and/or any contact details including email address.

(iii) for a beneficiary that is designated by characteristics, class or other means; the Labuan KRI shall obtain sufficient information (e.g. under a will of testament) concerning the beneficiary so as to satisfy itself that it will be able to establish the identity of the beneficiary at the time of the payout.

10.18 For the purposes of paragraphs 10.17 (i), (ii) and (iii), the verification of the identity of the beneficiary must take place latest at the time of the payout.

G 10.19 A Labuan KRI may rely on a third party to verify the identity of the beneficiaries.

Group Customers

Paragraph 10.20-10.22 are only applicable to Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

10.20 A Labuan KRI is required to identify and verify the customer (i.e. master policy/certificate owner) at the point of sale.

10.21 A Labuan KRI is required to establish the necessary mechanisms to identify the beneficiaries (i.e. insured members) of group policies/group takaful certificates at the point of sale, either from the master policy/certificate owner or directly from the insured members, to ensure compliance with CDD obligations and requirements on targeted financial sanctions under section B.17.

10.22 A Labuan KRI is required to verify the identity of beneficiaries of group policies/group takaful certificates latest at the time of payout.

Legal Persons

10.23 For a customer that is a legal person, the Labuan KRI is required to understand the nature of the customer's business, ownership and control structure.

10.24 A Labuan KRI is required to identify the customer and verify its identity through the following information:

(i) the name, legal form and proof of existence, such as Memorandum/Article/Certificate of Incorporation/Constitution/Partnership Agreement (certified true copies /duly notarised copies, may be accepted) or any other reliable references to verify the identity of the customer;

(ii) 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

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

10.25 A Labuan KRI is required to identify and verify the person authorised to represent the company including business or activities either by means of a letter of authority or directors' resolution when dealing with such person.

10.26 A Labuan KRI is required to identify and take reasonable measures to verify the identity of beneficial owners according to the following sequence:

(i) 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 or shareholders with equity interest of more than twenty-five percent[2];

(ii) where there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in paragraph 10.26 (i) 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

(iii) where no natural person is identified under paragraphs 10.26 (i) and (ii), the identity of the relevant natural person who holds the position of Senior Management.

For clarity, the Labuan KRI is not required to pursue steps (ii) and (iii) in circumstances where beneficial owner(s) have been identified through step (i). Similarly, where beneficial owner(s) have been identified at step (ii), the Labuan KRI is not required to pursue step (iii).

10.27 Where there is doubt in identifying a person(s) under paragraphs 10.24, 10.25 and 10.26, the Labuan KRI shall:

(i) conduct a basic search or enquiry on the background to ensure that the person:

(a) is not in the process of being dissolved or liquidated;

(b) has not been dissolved or liquidated; or

(c) is not a bankrupt; and

(ii) verify the authenticity of the information provided by the said person with the Registrar of Companies of Labuan FSA or any other relevant authorities.

[2] In relation to partnership, this shall refers to partner with capital contribution of more than twenty-five percent.

10.28 A Labuan KRI is exempted from obtaining a copy of constituent documents[3] and from verifying the identity of directors and shareholders of the legal person which fall under the following categories:

(i) public listed companies or corporations listed in Labuan International Financial Exchange and Bursa Malaysia;

(ii) foreign public listed companies:

(a) listed in recognised exchanges; and

(b) not listed in higher risk countries;

(iii) financial institutions that are not from higher risk countries;

(iv) any person that has been licensed or approved by Labuan FSA under LFSSA and LIFFSA;

(v) licensed entities under the Financial Services Act 2013 (FSA) and Islamic Financial Services Act 2013 (IFSA);

(vi) persons licensed or registered under the Capital Markets and Services Act 2007;

(vii) prescribed institutions under the Development Financial Institutions Act 2002 (DFIA); or

(viii) licensed entities under the Money Services Business Act 2011 (MSBA).

10.29 Notwithstanding the above, a Labuan KRI is required to identify and maintain the information relating to the identity of the directors and shareholders of legal persons referred to in paragraph 10.28 either; through a public register, other reliable sources or based on information provided by the customer.

G 10.30 A Labuan KRI 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

10.31 For customers which are legal arrangements, a Labuan KRI is required to understand the nature of the customer's business, ownership and control structure.

[3] Memorandum and Articles of Association or Certificate of Incorporation.

10.32 A Labuan KRI is required to identify the customer and verify its identity through the following information:

(i) name, legal form and proof of existence, or any reliable references to verify the identity of the customer;

(ii) the powers that regulate and bind the customer, as well as the names of relevant persons having a Senior Management position;

(iii) the address of the registered office; and

(iv) the address of the principal place of business, if differ from paragraph 10.32(iii).

10.33 A Labuan KRI is required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(i) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiary or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through the chain of control/ownership); or

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

Paragraph 10.34 is only applicable to Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

10.34 For the purpose of identifying beneficiaries of trusts that are designated by characteristics or by class under paragraph 10.33, a Labuan KRI is required to obtain sufficient information concerning the beneficiary. This is to enable a Labuan KRI to be satisfied that they would be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise its vested rights.

10.35 A Labuan KRI is 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 10.36 A Labuan KRI may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.

10.37 Where reliance is placed on third parties under paragraph 10.36, a Labuan KRI is required to comply with section B.8.

Clubs, Societies and Charities

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

10.39 A Labuan KRI is also required to take reasonable measures to identify and verify the beneficial owners of the clubs, societies or charities.

10.40 Where there are doubts on the identity of persons referred to under paragraphs 10.38 and 10.39, a Labuan KRI shall verify the authenticity of the information provided by such person with the relevant authority[4].

Reinsurance/Retakaful Arrangement

10.41 Under a reinsurance/retakaful arrangement, a Labuan KRI is required to carry out verification only on the ceding company, and not on the ceding company's customers. The following verification procedure applies:

Paragraph 10.41 are only applicable to Labuan (re)insurers and Labuan (re)takaful operators

(i) verification is not required for a ceding (re)insurer licensed under LFSSA or ceding (re)takaful operator under LIFSSA, a ceding (re)insurer licensed under FSA or (re)takaful operator licensed under IFSA; and

(ii) reinsurers/retakaful operators are required to take necessary steps to verify that the ceding company is authorised to carry on insurance/takaful business in its home jurisdiction which enforces AML/CFT/CPF standards equivalent to those of the AMLA.

[4] In relation to Malaysia, relevant authorities include the Companies Commission of Malaysia, Registrar of Societies and Legal Affairs Division under the Prime Minister's Department.

Counter-party

Paragraph 10.42-10.43 are applicable to Labuan Banks, Labuan Money Broker, and Labuan Trust Companies

10.42 Where the Labuan KRI establishes a relationship with a counter-party, the Labuan KRI must be satisfied that the counter-party is properly regulated and supervised.

10.43 A Labuan KRI is required to ensure that the counterparty's CDD process is adequate and the mechanism to identify and verify its customers is reliable and consistent with the requirements under the Guidelines.

Beneficiary Account

Paragraph 10.44-10.48 are only applicable to Labuan Banks

10.44 In the case of beneficiary accounts, a Labuan KRI is required to perform CDD on the beneficiary and the authorised person acting on behalf of the beneficiary, on individual basis.

10.45 In the event that identification on individual basis cannot be performed, for example where the interests of a group of beneficiaries are pooled together without specific allocation to known individuals, the Labuan KRI is required to satisfy itself that the funds in the account are not maintained in the interest of other parties which have no relationship with the account.

G 10.46 A Labuan KRI may rely on a third party when they are unable to conduct CDD on the clients of professionals, such as legal firms or accountants acting on behalf of their clients.

10.47 Where reliance is placed on a third party under paragraph 10.46, a Labuan KRI is required to comply with section B.8.

10.48 A Labuan KRI is to comply with the requirements under section B.5.8 in the event where the person acting on behalf of the beneficiary is unable or refuses to provide the information on the identity of the beneficiaries or provide a written undertaking, where applicable.

B.5.2 Simplified CDD

G 10.49 A Labuan KRI may conduct simplified CDD where ML/TF/PF risks are assessed to be low except where there are instances of higher risks or suspicion of ML/TF/PF.

10.50 In relation to paragraph 10.49, a Labuan KRI is required to have the following processes in place:

(i) conduct adequate analysis of ML/TF/PF risk;
(ii) establish appropriate mechanisms and internal controls for effective ongoing monitoring of customers and transactions to ensure prompt detection of unusual or suspicious transactions;
(iii) obtain Board's approval for the implementation of simplified CDD and document all assessments as well as approvals; and
(iv) establish appropriate mechanisms to ensure periodic review of the ML/TF/PF risks.

10.51 A Labuan KRI is required to obtain the following information from its customer and its beneficial owner:

(i) full name;
(ii) NRIC number or passport number or reference number of any other official documents of the customer or beneficial owner;
(iii) residential and/or mailing address;
(iv) date of birth;
(v) nationality; and
(vi) contact number and/or any other contact details including email address.

10.52 A Labuan KRI shall verify the identity of the customer and its beneficial owner. A Labuan KRI may refer to the guidance provided in **Appendix IV**.

Delayed Verification

G 10.53 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 Labuan KRI may complete verification after the establishment of the

business relationship. This is to allow some flexibilities for its customer and its beneficial owner to furnish the relevant documents.

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

(i) this occurs as soon as reasonably practicable;

(ii) the delay is essential so as not to interrupt the Labuan KRI's normal conduct of business;

(iii) the ML/TF/PF risks are effectively managed; and

(iv) there is no suspicion of ML/TF/PF.

10.55 The term "reasonably practicable" under paragraph 10.54(i) shall not exceed ten working days or any other period as may be specified by Labuan FSA.

10.56 A Labuan KRI is required to adopt risk management procedures to mitigate or address the risk of delayed verification if the Labuan KRI allows the customer to utilise the business relationship prior to undertake verification.

G 10.57 The measures that a Labuan KRI may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.

G 10.58 A Labuan KRI may apply delayed verification, where:

(i) simplified CDD measures apply; or

(ii) insurance policy/takaful certificate sold with insurance premiums/takaful contribution of foreign currency equivalent to below RM5,000 per annum or foreign currency equivalent to below RM10,000 for any single premium insurance policy or single contribution takaful certificate.

Paragraph 10.58-10.60 are only applicable to Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

10.59 The delayed verification of the customers, its beneficial owners and beneficiaries must take place latest at the time of payout.

10.60 A Labuan KRI must have in place measures to prevent transactions from being intentionally split to avoid the thresholds as specified in paragraph 10.58 (ii). Therefore, the aggregated premium/takaful contribution size of multiple policies per customer must be taken into consideration.

B.5.3 Specific CDD

CDD on Wire Transfer

Section B.5.3 is only applicable to Labuan Banks

10.61 A Labuan KRI must conduct CDD and obtain the following information, for transactions involving an amount of foreign currency equivalent to below RM3,000:

(i) full name;

(ii) NRIC number or passport number or reference number of any other official documents of the customer or its beneficial owner;

(iii) residential and/or mailing address;

(iv) contact number and/or any contact details including email address;

(v) date of birth;

(vi) nationality; and

(vii) purpose of transaction.

10.62 Labuan KRI shall conduct standard CDD measures for transactions involving an amount of foreign currency equivalent to RM3,000 and above.

B.5.4 Enhanced CDD

10.63 Labuan KRI is 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:

(i) obtaining CDD information under section B.5.1;

(ii) obtaining additional information on the customer and its beneficial owner (e.g. volume of assets and other information from public databases);

(iii) enquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and

(iv) obtaining approval from Senior Management of the Labuan KRI 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 parent company.

G 10.64 In addition to paragraph 10.63, a Labuan KRI may also consider the following enhanced CDD measures in line with the ML/TF/PF risks identified:

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

(ii) where relevant, obtain additional information on the beneficial owner of the beneficiaries (e.g. occupation, volume of assets, information available through public databases);

(iii) inquiring on the reasons for intended or performed transactions; and

(iv) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD measures.

Paragraph 10.65-10.67 are only applicable to Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

10.65 A Labuan KRI is required to include the beneficiary of a life insurance policy/family takaful certificate as a relevant risk factor in determining whether enhanced CDD measures are applicable.

10.66 A Labuan KRI is required to take enhanced measures which include identifying and verifying the identity of the beneficial owner of the said beneficiary, if the beneficiary is a legal person or a legal arrangement that presents a higher risk, latest at the time of payout.

In relation to PEPs

10.67 Where the beneficiaries or the beneficial owner of the beneficiaries are PEPs and assessed as higher risk at the latest time of payout, a Labuan KRI is required to:

(i) inform the Senior Management before the payout of the policy/certificate proceeds;

(ii) conduct enhanced scrutiny on the whole business relationship with the policyholder; and

(iii) consider lodging a suspicious transaction report.

B.5.5 Ongoing Due Diligence

10.68 A Labuan KRI is required to conduct ongoing due diligence on the business relationship with its customers. Such measures shall include:

(i) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Labuan KRI's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(ii) 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 10.69 In conducting ongoing due diligence, a Labuan KRI may take into consideration the economic background and purpose of any transaction or business relationship which:

(i) appears unusual;

(ii) is inconsistent with the expected type of activity and business model when compared to the volume of transaction;

(iii) does not have any apparent economic purpose; or

(iv) casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

10.70 The frequency in implementing paragraph 10.68(i) under ongoing due diligence and enhanced ongoing due diligence shall commensurate with the level of ML/TF/PF risks posed by the customer based on the risk profiles and nature of transactions.

10.71 A Labuan KRI shall periodically review its on-going due diligence measures to ensure it remains relevant and effective for accurate customer risk profiles and nature of transactions.

10.72 In conducting enhanced ongoing due diligence, a Labuan KRI is required to:

(i) increase the number and timing of controls applied; and

(ii) identify patterns of transactions that need further examination.

B.5.6 Existing Customer – Materiality and Risk

10.73 Existing customer in this paragraph refers to those that are customers prior to the CDD obligations under section 16 of the AMLA becoming applicable to the Labuan KRI.

10.74 A Labuan KRI is required to apply CDD requirements to existing customers on the basis of materiality and risk.

10.75 A Labuan KRI is 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 10.76 In assessing materiality and risk of existing customers under paragraph 10.74, a Labuan KRI may consider the following circumstances.

(i) the nature and circumstances surrounding the transaction including the significance of the transaction;

(ii) any material change in the way the account or business relationship is operated; or

(iii) insufficient information held on the customer or change in customer's information.

B.5.7 Non-Face-to-Face Business Relationship

10.77 A Labuan KRI must be vigilant in establishing and conducting business relationships via electronic means, which includes mobile channel and online channel.

10.78 The Board shall set and ensure effective implementation of appropriate policies and procedures to address any specific ML/TF/PF risks associated with the implementation of Non-Face-to-Face (non-FTF) business relationships.

10.79 A Labuan KRI must ensure and be able to demonstrate on a continuing basis that appropriate measures for identification and verification of the non-FTF customer's identity are as effective as that of face-to-face customers. This includes effecting monitoring and reporting mechanisms to identify potential ML/TF/PF activities.

10.80 In relation to paragraph 10.79, a Labuan KRI shall take measures to identify and verify the customer's identity through any of the following:

(i) establishing independent contact with the customer;

(ii) verifying the customer's information against reliable and independent sources to confirm the customer's identity as well as to identify any known or suspected ML/TF/PF risks associated with the customer; or

(iii) requesting, sighting and maintaining records of additional documents required to perform face-to-face customer verifications.

10.81 A Labuan KRI must ensure that the developed systems and technologies used for the purpose of establishing business relationships using non-FTF channels have capabilities to support an effective AML/CFT/CPF compliance programme, including verification of identification documents.

10.82 Where there is doubt, a Labuan KRI is required to request the customer and its 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.

B.5.8 Failure to Satisfactorily Complete CDD

10.83 Where a Labuan KRI is unable to comply with CDD requirements:

(i) the Labuan KRI 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

(ii) the Labuan KRI must consider lodging a suspicious transaction report under section B.12.

B.5.9 CDD and Tipping-Off

10.84 In cases where a Labuan KRI forms a suspicion of ML/TF/PF and reasonably believes that performing the CDD process would tip-off the customer, the Labuan KRI is permitted not to pursue the CDD process. In this regard, the Labuan KRI

must document the basis for not completing the CDD and immediately file a suspicious transaction report under section B.12.

G 10.85 Notwithstanding the requirement of paragraph 10.84, the Labuan KRI may consider proceeding with the transaction itself for purposes of furthering any inquiry or investigation of the ML/TF/PF suspicion.

10.86 The Labuan KRI shall observe the prohibition of tipping-off as stipulated under section 14A of AMLA. Disclosure of any report or related information referred to in section 14 is only allowed when any of the exemptions under subsection 14A (3) of AMLA apply.

B.6 Electronic Know-Your-Customer (e-KYC)

11.1 A Labuan KRI shall obtain the Board's approval on the overall risk appetite and internal framework governing the implementation to e-KYC. The framework shall address:

(i) high risk or material risk scenarios that require the subsequent Board's approval;

(ii) variations or expectations to existing e-KYC related products or methods that require subsequent Board's approval; and

(iii) other instances that require Board's approval.

11.2 The Board shall set and ensure the effective implementation of appropriate policies and procedures to address any risks associated with the implementation of e-KYC. These include operational, customer information, human capital, information technology (IT) and money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks.

B.6.1 Identification and Verification through e-KYC

11.3 A Labuan KRI shall ensure and be able to demonstrate on a continuing basis that appropriate measures for the identification and verification of a customer's identity through e-KYC are secure and effective.

11.4 A Labuan KRI shall adopt an appropriate combination of authentication factors when establishing measures to verify the identity of a customer through e-KYC. The strength and combination of the authentication factors shall commensurate to the risks associated with inaccurate identification for a particular product or services.

11.5 In respect of paragraph 11.4, a Labuan KRI should have regard to the three basic authentication factors:

(i) personal information that the customer possesses (e.g. identity card, registered mobile number);

(ii) personal information that the customer knows (e.g PIN, personal information); and

(iii) item that is uniquely identifiable only to the customer (e.g biometric characteristics).

An e-KYC solution that depends on more than one factor is typically more secured and difficult to compromise than a single factor system.

G 11.6 In identifying and verifying a customer's identity through e-KYC, a Labuan KRI may undertake measures including but not limited to the following:

(i) verifying the customer against a government issued ID by utilising biometric technology;

(ii) ensuring that the government issued ID used to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms; and

(iii) ensuring the customer is a live subject and not an impersonator (e.g. through use of photos, videos, facial masks) by utilising liveness detection.

B.6.2 Use of Artificial Intelligence, Machine Learning or Other Forms of Predictive Algorithms

G 11.7 An e-KYC solution may utilise artificial intelligence, machine learning or other forms of predictive algorithms to ensure accurate identification and verification. This may result in automation of the decision making process for customer identification and verification, thus reducing the need for human intervention.

11.8 Where the decision to verify a customer's identity through e-KYC is automated with the use of artificial intelligence, machine learning to other forms of predictive algorithms, whether in whole or in part, a Labuan KRI shall ensure that the e-KYC solution is capable of accurately distinguishing between genuine and non-genuine cases of customer identification and verification.

11.9 For the purposes of paragraph 11.8, in ensuring accuracy of the e-KYC solution, a Labuan KRI shall take steps to minimise the overall False Acceptance Rates (FAR) which is defined as follows:

$$\left(\frac{No.\ of\ False\ Positives}{No.\ of\ False\ Positives + No.\ of\ True\ Negatives}\ X\ 100\right)$$

11.10 In measuring and assessing the FAR, a Labuan KRI shall observe the considerations and requirements listed in **Appendix V**[5].

B.6.3 Reliance on Human Representatives

G 11.11 Notwithstanding paragraph 11.7 to 11.10, a Labuan KRI may also perform e-KYC where identification and verification is conducted solely by a human representative. This includes cases where the decision to verify a customer is conducted by the Labuan KRI's representative or intermediary with the assistance of electronic means such as video calls using mobile devices.

G 11.12 In contrast with e-KYC solutions under paragraph 11.7 to 11.10 that utilise both machine and human capabilities, e–KYC performed solely by a human representative through electronic means may involve a lower level of identity assurance due to human limitations and thus may not be suitable for all circumstances.

11.13 Where the decision to verify a customer's identity through e-KYC is conducted solely by a human representative, a Labuan KRI shall give due regard to situations with potentially higher risk of misidentification and consequently establish necessary safeguards to address the risks.

B.6.4 Addressing Ongoing Vulnerabilities

11.14 A Labuan KRI shall continuously identify and address potential vulnerabilities in the e-KYC solution.

11.15 In respect of paragraph 11.14, actions to address potential vulnerabilities shall include conducting reviews on the e-KYC solution and, where applicable, submitting periodical feedback to technology providers with the aim of improving effectiveness of the underlying technology used for customer identification and verification.

[5] For avoidance of doubt, requirements for FAR within the Guidelines do not apply to e-KYC solutions where the decisions to verify a customer's identity is (i) automated without the use of artificial intelligence, machine learning or other similar forms of predictive algorithms; or (ii) conducted solely by a human representative, as described in paragraph 11.11.

B.6.5 Additional Safeguards to Facilitate Deployment

11.16 The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification.

11.17 Where there are limited data points to determine accuracy of the e-KYC solution in the initial deployment stage, a Labuan KRI shall establish additional safeguards, particularly for products that pose higher risks arising from inaccurate identification.

B.6.6 Reporting Requirements

11.18 In monitoring the effectiveness and accuracy of e-KYC solutions utilising artificial intelligence, machine learning or other forms of predictive algorithms, a Labuan KRI shall maintain a record of the performance of the e-KYC solution segregated on a monthly basis in accordance with the reporting template in **Appendix VI.**

11.19 A Labuan KRI must ensure that the e-KYC system remains relevant and review periodically based on risks associated to the products and services from time to time.

11.20 In addition to record keeping requirement under section B.14, a Labuan KRI to maintain a monthly performance record as to assess the accuracy and effectiveness of the e-KYC validation system, using the specified reporting template as attached in **Appendix VI**. A Labuan KRI shall submit the annual report to Labuan FSA by 15 January of the following year as prescribed under paragraph 23.1.

B.7 Politically Exposed Persons (PEPs)

FATF Recommendation 12:

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(i) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;

(ii) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

(iii) take reasonable measures to establish the source of wealth and source of funds; and

(iv) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation.

B.7.1 General

12.1 The requirements specified in this paragraph are applicable to all types of PEPs and family members or close associates of those PEPs.

12.2 In identifying individuals who fall within the definition of a close associate of a PEP, a Labuan KRI must take reasonable measures to determine the extent to which these individuals are directly engaged or involved in the activity of the PEP.

B.7.2 Foreign PEPs

12.3 A Labuan KRI is required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

12.4 Insurance and takaful operators are required to take reasonable measures to determine whether the beneficiary and/or, where required, the beneficial owner of the beneficiary, is a foreign PEP.

12.5 Upon determination that a customer or a beneficial owner under paragraph 12.3 and beneficiary or beneficial owner of a beneficiary under paragraph 12.4 is a foreign PEP, the requirements of enhanced CDD as specified in section B.5.4 and enhanced ongoing due diligence as specified in paragraph 10.72 must be conducted.

B.7.3 Domestic PEPs or Person Entrusted with a Prominent Function by an International Organisation

12.6 A Labuan KRI is 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.

12.7 A Labuan KRI is required to assess the level of ML/TF/PF risks related to business relationship with the customer or beneficial owner whom is a domestic PEP or a person entrusted with a prominent function by an international organisation. For insurance and takaful operators, this includes beneficiaries and beneficial owner of a beneficiary.

12.8 The assessment of the ML/TF/PF risks as specified in paragraph 12.7, shall take into account the profile of the customer or beneficial owner under paragraph 6.19.

12.9 The requirements on enhanced CDD as specified in section B.5.4 and enhanced ongoing due diligence as specified in paragraphs 10.72 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 12.10 A Labuan KRI may apply CDD measures similar to other customers for domestic PEPs or persons entrusted with a prominent function by an international organisation if the Labuan KRI is satisfied that such persons are not assessed as higher risk.

B.7.4 Cessation of PEP Status

12.11 A Labuan KRI shall consider the following factors in determining whether a person is no longer holds a prominent public function can cease from being regarded as a PEP:

(i) Whether the PEP could still exert informal influence, despite vacating from such position; and

(ii) Whether the PEP's current position either official capacity or otherwise is no longer linked to the same substantive matter as that of the previous function.

B.8 Reliance on Third Parties

FATF Recommendation 17:

Financial institutions may be permitted to rely on third parties to perform CDD measures. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

B.8.1 Customer Due Diligence

G 13.1 A Labuan KRI may rely on third parties to conduct CDD or to introduce business.

13.2 The ultimate responsibility and accountability for CDD measures shall remain with the Labuan KRI.

13.3 A Labuan KRI 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 risk to the international financial system.

13.4 A Labuan KRI is prohibited from relying on third parties located in higher risk countries that have been identified in accordance with section B.9.

13.5 The relationship between a Labuan KRI and the third parties accountability 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 Labuan KRI, at a minimum:

(i) must be able to obtain immediately the necessary information concerning CDD as required under section B.5; and

(ii) must be reasonably satisfied that the third party:

(a) has an adequate CDD process;

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

(c) can provide the CDD information and provide copies of the relevant documentation immediately upon request; and

(d) regulated and subjected to supervisory oversight relating to AML/CFT/CPF matters by relevant competent authorities.

13.6 A Labuan KRI shall obtain an attestation from the third party to satisfy itself that the requirements in paragraph 13.5 have been met.

G 13.7 A Labuan KRI 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 B.5.

G 13.8 The requirements under paragraphs 13.1, 13.3 and 13.5 may be fulfilled if the Labuan KRI relies on a third party that is part of the same financial group, subject to the following conditions:

(i) the group applies CDD, record keeping and AML/CFT/CPF programmes in line with requirements under the Guidelines;

(ii) the implementation of CDD, record keeping and AML/CFT/CPF programmes is supervised at a group level by the relevant authority; and

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

B.8.2 Ongoing Due Diligence

13.9 A Labuan KRI shall not rely on third parties to conduct ongoing due diligence of its customers.

B.9 Higher Risk Countries

FATF Recommendation 19:

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

14.1 A Labuan KRI is 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 identified by the FATF or Government of Malaysia.

14.2 Notwithstanding the generality of paragraph 14.1 above, the enhanced CDD shall include any specific CDD measure as may be imposed by the FATF or Government of Malaysia.

14.3 A Labuan KRI is required to apply appropriate countermeasures, proportionate to the risks, when called upon to do so by the FATF or Government of Malaysia.

G 14.4 For the purpose of paragraph 14.3 above, the countermeasures may include the following:

(i) limiting business relationships or financial transactions with the identified country or persons located in the country concerned;

Paragraph 14.4 (iv) is only applicable to Labuan Banks, and Labuan (re)insurers, Labuan (re)takaful operators, insurance and takaful brokers

(ii) reviewing and amending, or if necessary terminating, correspondent banking relationships with financial institutions in the country concerned;

(iii) conducting enhanced external audits, by increasing the intensity and frequency, for branches and subsidiaries of the Labuan KRI or financial group, located in the country concerned;

(iv) submitting an annual report with a summary of exposure to customers and beneficial owners from the country concerned as specified in **Appendix VII**. A Labuan KRI shall submit the report to Labuan FSA by 31 March of the following year as prescribed under paragraph 23.1; and

(v) conduct any other countermeasures as may be specified Labuan FSA.

14.5 In addition to the above, where ML/TF/PF risks are assessed as higher risk, a Labuan KRI is 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.

G 14.6 For the purpose of requirements under paragraphs 14.1, 14.2, 14.3 and 14.5, a Labuan KRI may refer to the FATF website: http://www.fatf-gafi.org.

B.10 Wire Transfers

FATF Recommendation 16:

Financial institutions must require and ensure accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Section B.10 is only applicable to Labuan Banks

B.10.1 General

15.1 The requirements under this paragraph are applicable to a Labuan KRI providing cross-border wire transfers and domestic wire transfers including serial payments and cover payments.

15.2 A Labuan KRI must comply with the requirements on targeted financial sanctions in relation to terrorism financing, proliferation financing and other under UN-Sanctions under section B.17.

15.3 A Labuan KRI shall not execute the wire transfer if it does not comply with the requirements specified in this paragraph.

15.4 A Labuan KRI is required to maintain all originator and beneficiary information collected in accordance with record keeping requirements under section B.14.

B.10.2 Ordering Institutions

Cross-border wire transfers

15.5 A Labuan KRI which is an ordering institution is required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount of foreign currency equivalent to RM3,000 and above are accompanied by at least the following information:

(i) Required and accurate originator information:

(a) name;

(b) account number (or a unique reference number if there is no account number) which permits traceability of the transaction; and

(c) address or date and place of birth.

(ii) Required beneficiary information:

(a) name; and

(b) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

15.6 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and ordering institutions are required to include the originator's account number or unique transaction reference number.

15.7 A Labuan KRI is required to ensure that the message or payment instruction for all cross-border wire transfers for foreign currency equivalent to below RM3,000 are accompanied by at least the following information:

(i) Required originator information:

(a) name; and

(b) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

(ii) Required beneficiary information

(a) name; and

(b) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

15.8 The information required under paragraph 15.7 need not be verified for accuracy except when there is a suspicion of ML/TF/PF.

Domestic wire transfers

15.9 A Labuan KRI is required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire

transfers, unless this information can be made available to the beneficiary institution and relevant authorities by other means.

15.10 Where the information accompanying the domestic wire transfer can be made available to the beneficiary institution and relevant authorities by other means, the ordering institution shall include only the originator's account number or if there is no account number, a unique identifier, within the message or payment form, provided that this account number or unique identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering institution is required to provide the information within three working days of receiving the request either from the beneficiary institution or from the relevant authorities and must provide the information to LEAs immediately upon request.

B.10.3 Intermediary Institutions

15.11 For cross-border wire transfers, intermediary institution is required to retain all originator and beneficiary information that accompanies a wire transfer as required under paragraphs 15.5 and 15.7.

15.12 Where the required originator or beneficiary information accompanying a cross-border wire transfer cannot be transmitted due to technical limitations, intermediary institution is required to keep a record in accordance with record keeping requirements under section B.14.

15.13 Intermediary institution is required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

15.14 Intermediary institution is required to have effective risk-based policies and procedures for determining:

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

(ii) the appropriate follow-up action.

B.10.4 Beneficiary Institutions

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

15.16 For cross-border wire transfers of an amount of foreign currency equivalent to RM3,000 and above, beneficiary institution is required to verify the identity of the beneficiary, if the identity has not been previously verified. In addition, beneficiary institution is required to maintain this information in accordance with record keeping requirements under section B.14.

15.17 Beneficiary institution is required to have effective risk-based policies and procedures for determining:

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

(ii) the appropriate follow-up action.

B.11 Correspondent Banking

FATF Recommendation 13:

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Section B.11 is only applicable to Labuan Banks

16.1 A Labuan KRI providing correspondent banking services to respondent institution is required to take the necessary measures to ensure that they are not exposed to ML/TF/PF threat through the accounts of the respondent institutions such as being used by shell banks.

16.2 In relation to cross-border correspondent banking and other similar relationships, a Labuan KRI is required to:

(i) gather sufficient information on a respondent institution to fully understand the nature of the respondent institution's business, and to determine its reputation from publicly available information as well as the quality of supervision exercised, including whether it has been subject to ML/TF/PF investigation or regulatory action;

(ii) assess the respondent institution's AML/CFT/CPF controls having regard to AML/CFT/CPF measures of the country or jurisdiction in which the respondent institution operates;

(iii) obtain approval from the Senior Management before establishing new correspondent banking relationships; and

(iv) clearly understand the respective AML/CFT/CPF responsibilities of each institution.

16.3 In relation to "payable-through accounts", a Labuan KRI is required to satisfy themselves that the respondent institution:

(i) has performed CDD obligations on its customers that have direct access to the accounts of the Labuan KRI; and

(ii) is able to provide relevant CDD information to the Labuan KRI upon request.

16.4 A Labuan KRI shall not enter into, or continue, correspondent banking relationships with shell banks. A Labuan KRI is required to satisfy themselves that respondent institution do not permit their accounts to be used by shell banks.

B.12 Suspicious Transaction Report

FATF Recommendation 20:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit.

B.12.1 General

17.1 A Labuan KRI is required to promptly submit a suspicious transaction report to the FInD, Bank Negara Malaysia and Labuan FSA whenever the Labuan KRI suspects or has reasonable grounds to suspect that the transaction (including attempted or proposed), regardless of the amount:

(i) appears unusual;

(ii) has no clear economic purpose;

(iii) appears illegal;

(iv) involves proceeds from an unlawful activity or instrumentalities of an offence; or

(v) indicates that the customer is involved in ML/TF/PF.

17.2 A Labuan KRI must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but 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.

17.3 A Labuan KRI must establish a reporting system for the submission of suspicious transaction reports.

B.12.2 Reporting Mechanisms

17.4 A Labuan KRI is 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 parent company. In the case of employees at the parent company, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

17.5 A Labuan KRI is 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.

17.6 Upon receiving any internal suspicious transaction report whether from the parent company, 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.

17.7 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.

17.8 A Labuan KRI 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.

17.9 A Labuan KRI must provide additional information and documentation as may be requested by the FinD, Bank Negara Malaysia and must respond promptly to any further enquiries with regard to any report received under section 14 of the AMLA.

17.10 A Labuan KRI 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 17.11 Where a suspicious transaction report has been lodged, a Labuan KRI may update or make a fresh suspicious transaction report as and when a new suspicion arises.

17.12 The Compliance Officer of a Labuan KRI that has been granted access to Financial Intelligence System (FINS), administered by the FInD, Bank Negara Malaysia must submit the suspicious transaction report through the following website: https://fins.bnm.gov.my.

17.13 The Compliance Officer of a Labuan KRI may apply for an access to FINS by using the template attached in **Appendix VIII**.

17.14 For a Labuan KRI that has not been granted access to FINS, the Compliance Officer must submit the suspicious transaction report to Bank Negara Malaysia and concurrently, send email notification of the reporting to Labuan FSA. The specified reporting form for suspicious transaction as provided in Bank Negara Malaysia's AML/CFT website: https://amlcft.bnm.gov.my/aml/cft-policies

Director
Financial Intelligence Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)
Fax : +603-2691 6108
E-mail : str@bnm.gov.my

Head
AML Policy, Risk Monitoring & Market Surveillance
E-mail : aml@labuanfsa.gov.my

B.12.3 Triggers for Submission of Suspicious Transaction Report

17.15 A Labuan KRI is required to establish internal criteria ("red flags") to detect suspicious transactions.

17.16 A Labuan KRI must consider submitting a suspicious transaction report when any of its customer's transactions or attempted transactions fits the Labuan KRI's list of "red flags".

G 17.17 A Labuan KRI may refer to **Appendix IX** for examples of transactions that may constitute triggers for the purpose of reporting suspicious transactions.

G 17.18 A Labuan KRI may be guided by examples of suspicious transactions provided by Labuan FSA or other corresponding competent authorities, supervisory authorities and international organisations.

B.12.4 Internal Suspicious Transaction Reports

17.19 A Labuan KRI 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.

17.20 Pursuant to paragraph 17.19, if no suspicious transaction reports are submitted to the Authorities, the internal suspicious transaction reports and the relevant supporting documentary evidence must be made available to either of the Authorities upon request.

B.13 Disclosure of Suspicious Transaction Report and Related Information

18.1 A Labuan KRI is prohibited from disclosing any suspicious transaction report and where applicable, 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.

18.2 The prohibition under paragraph 18.1 does not apply where the exceptions under section 14A (3) of the AMLA apply.

18.3 Where the exceptions under section 14A(3) of the AMLA apply, a Labuan KRI must has the following measures in place:

(i) a set of parameters on:

(a) the circumstances where disclosure is required;

(b) types of information that can be disclosed; and

(c) to whom it can be disclosed;

(ii) internal governance procedures to ensure that any disclosure is properly justified, duly authorised and managed in a controlled and secured environment;

(iii) apprise all employees and intended recipients who are privy to the reports and related information to maintain confidentiality; and

(iv) an audit trail is maintained in respect of the disclosure of such information.

G 18.4 For any disclosure of reports and related information pursuant to section 14A (3)(d) of the AMLA, a Labuan KRI may make a written application to the FInD, Bank Negara Malaysia for a written authorisation.

18.5 In making an application under paragraph 18.4, the Labuan KRI shall provide the following:

(i) details and justification for the disclosure;

(ii) details on the safeguards and measures in place to ensure confidentiality of information transmitted at all times;

(iii) information on persons authorised by the Labuan KRI to have access to the reports and related information;

(iv) any other documents or information considered relevant by Labuan KRI; and

(v) any other documents or information requested or specified by Bank Negara Malaysia.

B.14 Record Keeping

FATF Recommendation 11:

Financial institutions are expected to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

19.1 A Labuan KRI is 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[6] must be up-to-date, relevant and retrievable.

19.2 A Labuan KRI must ensure that all relevant records relating to transactions are sufficiently kept to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

19.3 A Labuan KRI is 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.

19.4 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 a Labuan KRI is informed by the relevant LEA that such records are no longer required.

19.5 A Labuan KRI is 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 supervisory authorities and LEA in a timely manner.

[6] Physical records or stored on electronic media.

B.15 Management Information System

20.1 A Labuan KRI must have in place an adequate manual or electronic management information system (MIS) to complement its CDD process. The MIS shall be able to provide timely information on a regular basis to detect irregularities and/or any suspicious activity.

20.2 The MIS shall be commensurate with the nature, scale and complexity of the Labuan KRI's activities and ML/TF/PF risk profile.

20.3 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.

20.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems.

G 20.5 The MIS may be integrated with the Labuan KRI's system that contains its customer's normal transactions or business profile, which is accurate, up-to-date and reliable.

B.16 Enforcement Orders

21.1 A Labuan KRI is required to produce any information or document requested by the relevant LEA, pursuant to any investigation order under Part VI of the AMLA served on the Labuan KRI. The information or document is required to be provided within a reasonable time frame that has been agreed upon between the investigating officer and the Labuan KRI.

21.2 A Labuan KRI is required to have in place the necessary policies, procedures and systems to ensure no undue delay in responding to such orders.

B.17 Targeted Financial Sanctions on Terrorism Financing, Proliferation Financing and under Other UN-Sanctions Regimes

FATF Recommendation 6 & 7:

Targeted financial sanctions regime should comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing as well as prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

B.17.1 General

22.1 A Labuan KRI is required to keep abreast of the relevant UNSCR list relating to combating the financing of terrorism, which includes:

Relates to Targeted Financial Sanctions on Terrorism Financing

(i) 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

(ii) new UNSCR list which is published by the UNSC or its relevant Sanctions Committee as published in the United Nations (UN) website.

22.2 A Labuan KRI is required to keep updated with the list of countries and persons designated as restricted end-users and prohibited end-users under the Strategic Trade Act 2010 (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 as listed in **Appendix X.**

Relates to Targeted Financial Sanctions on Proliferation Financing

22.3 A Labuan KRI is required to keep updated with the list of designated countries and persons under the CBA Regulations, in accordance with the relevant UNSCR relating to upholding of peace and security, through prevention of armed conflicts and human rights violations, as published in the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee as listed in **Appendix XI.**

Relates to Targeted Financial Sanctions under Other UN-Sanctions Regime

B.17.2 Maintenance of Sanctions List

22.4 A Labuan KRI is required to maintain a sanctions database which comprised, at the minimum, the following:

(i) UNSCR List; and

(ii) Domestic List.

UNSCR List

22.5 A Labuan KRI must ensure that the information contained in the sanctions database is updated and effected without delay upon the publication by the UNSC or its relevant Sanctions Committee's designation in the UN website.

G 22.6 A Labuan KRI may refer to the Consolidated UNSCR List published in the following UN website: *https://www.un.org.*

22.7 The UNSCR List shall remain in the sanctions database until delisting of the specified entities[7] and designated country or person[8] by the UNSC or its relevant Sanctions Committee is published in the UN website.

Domestic List [9]

22.8 A Labuan KRI is required to keep updated with the Domestic List as and when this is gazetted.

22.9 A Labuan KRI must ensure that the information contained in the sanctions database is updated and effected without delay upon gazetted.

22.10 The Domestic List shall remain in the sanctions database until such specified entities are delisted from the Gazette.

G 22.11 A Labuan KRI may refer to the Domestic List published in the following website: *http://lom.agc.gov.my*.

---

7 List for Targeted Financial Sanctions on Terrorism Financing.
8 List for Targeted Financial Sanctions on Proliferation Financing and Under Other UN-Sanctions Regimes.
9 List for Targeted of Financial Sanctions on Terrorism Financing.

Other Requirements

22.12 A Labuan KRI must ensure that the information contained in the sanctions database is comprehensive and easily accessible by their employees at the parent company, branch, subsidiary and where relevant, to their external service providers or their agents.

G 22.13 A Labuan KRI may monitor and consolidate other countries' unilateral sanctions lists in their sanctions database.

G 22.14 A Labuan KRI may also consider electronic subscription services to ensure prompt updating of the sanctions database.

B.17.3 Sanctions Screening – Customers

22.15 A Labuan KRI is 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 ongoing due diligence.

22.16 For clarity, sanctions screening obligations apply to all customers and transactions regardless of any thresholds for CDD or features of a product or service.

22.17 A Labuan KRI 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, a Labuan KRI shall obtain the following information:

(i) Full name;

(ii) NRIC number or passport number or reference number of any other official documents; and

(iii) Date of birth.

22.18 A Labuan KRI is required to screen its entire customer database without delay including dormant accounts for any positive name match against the:

(i) Domestic List upon gazetted; and

(ii) UNSCR List upon published by the UNSC or the relevant Sanctions Committee's designation in the UN website.

22.19 A Labuan KRI in the insurance and takaful sector shall conduct sanctions screening upon establishing business relationships, during in-force period of the policy and before any payout.

G 22.20 When conducting the sanctions screening process, a Labuan KRI may perform name searches based on a set of possible permutations for each specified entity to prevent unintended omissions.

Paragraph 22.20 relates to Targeted Financial Sanctions on Proliferation Financing

22.21 A Labuan KRI shall maintain the records on the sanctions screening conducted and make such records available to supervisory authorities, upon request.

Dealing with False Positives

22.22 A Labuan KRI is required to ensure that any matches to Domestic List or UNSCR List are true matches in order to eliminate false positives.

22.23 A Labuan KRI is 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 22.24 In the case of similar or common names, a Labuan KRI may direct any query to the relevant Authorities to ascertain whether or not the customer is a specified entity.

B.17.4 Related Parties

22.25 A Labuan KRI shall undertake due diligence on related parties.

22.26 In undertaking due diligence on the related parties, a Labuan KRI is required to examine and analyse past transactions of the specified entities, designated person and related parties, and maintain records on the analysis of these transactions.

G 22.27 In ascertaining whether an entity is owned or controlled by a specified entity, designated person and related parties, a Labuan KRI may refer to the definition

of a "beneficial owner" in paragraph 5.2, and requirements under section B.5 in relation to CDD on beneficial owners.

B.17.5 Freezing, Blocking and Rejecting - Customers and Related Parties

22.28 Upon determination and confirmation of a customer's identity as a specified entity, designated person and/or related parties, a Labuan KRI is required to immediately conduct the following:

(i) freeze the customer's funds, properties, other financial assets and economic resources; or

(ii) where applicable, to block transactions in order to prevent dissipation of the funds, other financial assets and economic resources.

22.29 A Labuan KRI is required to reject a potential customer, when there is a positive name match.

22.30 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 22.7 and 22.10[10].

22.31 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 22.7[11].

Allowable Transactions

22.32 Any dealings with frozen funds or properties, whether by the specified entity, related party, or any interested party, requires prior written authorisation from Malaysia's Minister of Home Affairs[12].

22.33 Any dealings with frozen funds, other financial assets or economic resources, whether by the designated country, person, identified related party or any

---

The requirements are applicable for:
[10] Targeted Financial Sanctions on Terrorism Financing - Paragraph 22.28.
[11] Targeted Financial Sanctions on Proliferation Financing and under other UN-Sanctions Regimes – Paragraph 22.29.
[12] Targeted Financial Sanctions on Terrorism Financing - Paragraph 22.30 and 22.33.

interested party, would require prior written authorisation from the Strategic Trade Controller under the STA[13].

22.34 Any dealings with frozen funds, other financial assets or economic resources, whether by the designated person, related party or any interested party, would require prior written authorisation from the UNSC or its relevant Sanctions Committee[14].

22.35 The frozen funds and properties may continue to receive deposits, dividends, interests, bonuses, premiums/contributions or other benefits. However, such funds and benefits shall remain frozen as long as the specified entity continues to be listed under the Domestic List and UNSCR List[12].

22.36 The frozen funds, other financial assets or economic resources may continue receiving deposits, dividends, interests, bonuses, premiums/contributions or other benefits. However, such funds and benefits shall remain frozen as long as the countries and persons continue to be listed under the UNSCR list[13,14].

Exemption for Basic and Extraordinary Expenditures

G 22.37 A Labuan KRI may advise the specified entity, a related party or any interested party to make an application to Malaysia's Minister of Home Affairs for exemptions on basic and extraordinary expenditures for the following[15]:

(i) frozen funds or properties; or

(ii) blocked or rejected transactions.

22.38 A Labuan KRI shall only proceed with payments for basic and extraordinary expenditures upon receiving written authorisation from Malaysia's Minister of Home Affairs[15].

G 22.39 A Labuan KRI may advise the designated person, related party or any interested party to make an application to the Strategic Trade Controller under the STA to

[13] Targeted Financial Sanctions on Proliferation Financing – Paragraph 22.31 and 22.34.
The requirements are applicable for:
[14] Targeted Financial Sanctions Under other UN-Sanctions Regimes - Paragraph 22.32 and 22.34.
[15] Targeted Financial Sanctions on Terrorism Financing - Paragraph 22.35 and 22.36.

allow payments due under contracts entered into prior to the designation for the following[16]:

(i) frozen funds,

(ii) other financial assets or economic resources; or

(iii) blocked or rejected transaction.

22.40 A Labuan KRI shall only proceed with the payments due under existing contracts upon receiving written authorisation from the Strategic Trade Controller under the STA[16].

G 22.41 A Labuan KRI may advise the customer, related party or any interested party to make an application to the UNSC or its relevant Sanctions Committee to allow payments due under contracts entered into prior to the designation for the following[17]:

(i) frozen funds;

(ii) other financial assets or economic resources; or

(iii) blocked or rejected transaction.

22.42 A Labuan KRI shall only proceed with the payments due under existing contracts upon receiving written authorisation from the UNSC or its relevant Sanctions Committee[17].

Exemption for Payments Due under Existing Contracts

G 22.43 A Labuan KRI 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[18].

The requirements are applicable for:
[16] Targeted Financial Sanctions on Proliferation Financing - Paragraph 22.37 to 22.38.
[17] Targeted Financial Sanctions Under Other UN-Sanctions Regimes - Paragraph 22.39 to 22.40.
The requirements are applicable for:
[18] Targeted Financial Sanctions on Proliferation Financing - Paragraph 22.41 to 22.42.

22.44 A Labuan KRI shall only proceed with the payments due under existing contracts upon receiving prior written authorisation from the Strategic Trade Controller under the STA[18].

G 22.45 A Labuan KRI may advise the customer, 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 UNSC or its relevant Sanctions Committee to allow payments due under contracts entered into prior to the designation[19].

22.46 A Labuan KRI shall only proceed with the payments due under existing contracts upon receiving prior written authorisation from the UNSC or its relevant Sanctions Committee[19].

B.17.6 Reporting on Positive Name Match

Reporting upon Determination of a Positive Name Match

22.47 A Labuan KRI is required to immediately report by submitting the information under **Appendix XII**[20] via Statistical Management System (SMS), upon it determining that it is in possession or in control of funds or properties, of any specified entity and/or related party to:

(i) Labuan FSA; and

(ii) Inspector-General of Police, Malaysia

22.48 A Labuan KRI is required to immediately report to the Labuan FSA on any detection, freezing, blocking or rejection actions undertaken with regard to any identified funds, other financial assets and economic resources or transactions, by submitting the information under **Appendix XII**[21] via SMS.

[19] Targeted Financial Sanctions Under Other UN-Sanctions Regimes - Paragraph 22.43 to 22.44.
The requirements are applicable for:
[20] Targeted Financial Sanctions on Terrorism Financing.
[21] Targeted Financial Sanctions on Proliferation Financing and Under Other UN-Sanctions Regimes.

B.17.7 Periodic Reporting on Positive Name Match

22.49 A Labuan KRI that has reported positive name matches and are in possession or in control of frozen or blocked funds or properties of any specified entity, designated person and/or related party are required to report any changes to those funds, other financial assets and economic resources, are to use the form and at intervals as specified in **Appendix XIII**.

22.50 Notwithstanding paragraph 22.49, a Labuan KRI is not required to submit periodic reporting on positive name matches involving customers who conduct one-off transactions and where they do not maintain an account with them.

B.17.8 Reporting of Suspicious Transaction

On Related Transactions

22.51 A Labuan KRI is 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 the following:

(i) specified entity or related party[22]; and

(ii) designated countries, persons or related party[23].

22.52 A Labuan KRI is also required to submit a suspicious transaction report on any attempted transactions undertaken by the following:

(i) specified entity or related party[22]; and

(ii) designated countries, persons or related party[23].

On Name Match with Other Unilateral Sanctions Lists

22.53 A Labuan KRI shall submit a suspicious transaction report if there is any positive name match with individuals or entities listed in other unilateral sanctions lists.

The requirements are applicable for:

[22] Targeted Financial Sanctions on Terrorism Financing.

[23] Targeted Financial Sanctions on Proliferation Financing and Under Other UN-Sanctions Regimes.

Imposition of New Measures

22.54 In the event the UNSC or its relevant Sanctions Committee imposes new measures relating to the prevention of PF or proliferation of weapon of mass destruction (WMD), upholding of peace and security, and prevention of conflicts and human rights violations, a Labuan KRI is required to adhere to such measures as specified by Labuan FSA.

B.18 Submission of Regulatory Reports

23.1 For the purpose of submission of regulatory report to Labuan FSA as required under paragraph 7.17, 11.20 and 14.4, the submission shall be made to Labuan FSA at the following address:

Director
Supervision Department
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Federal Territory of Labuan, Malaysia

Telephone no: 03 8873 2000
Facsimile no: 03 8873 2209
Email: *sed@labuanfsa.gov.my*

Labuan Financial Services Authority
28 October 2026 (Updated)
3 February 2025 (Updated)
21 May 2024 (Updated)
31 March 2022

Appendix I List of Policy Documents to be Read Together with the Guidelines and List of Superseded Guidelines

1. The Guidelines shall complement and to be read together with the following Guidelines and Circulars:

   (i) Guidelines on Implementation of Targeted Financial Sanctions on Terrorism Financing;

   (ii) Guidelines on Politically Exposed Person (PEP) – Family Members and Close Associates of PEP;

   (iii) Guidelines on Beneficial Ownership for Labuan Entities;

   (iv) Guidelines on Travel Rule for Labuan Digital Financial Services;

   (v) Guidelines on Fit and Proper Person Requirements;

   (vi) Guidelines on Compliance Function for Labuan Financial Institutions;

   (vii) Guidelines on External Service Arrangements for Labuan Financial Institutions;

   (viii) Guidelines on Digital Governance Framework;

   (ix) Directive on Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF);

   (x) Circular on Innovative Financial Services in the Labuan International Business and Financial Centre;

   (xi) Circular on Electronic Know-Your-Customer (e-KYC) for Digital Financial Services;

   (xii) Clarification Note on Electronic Know-Your-Customer (e-KYC);

   (xiii) Circular on Submission of Compliance Report and Anti-Money Laundering Counter Financing of Terrorism (AML/CFT) Independent Audit Report to Labuan FSA; and

   (xiv) Governance and Market Conduct Framework for Labuan Trust Companies.

2. With the implementation of the Guidelines, the following Guidelines will be superseded:

(i) Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions issued on 31 March 2022;

(ii) Guidelines on AML/CFT – Banking Sector issued on 30 December 2013;

(iii) Guidelines on AML/CFT – Insurance and Takaful Sectors issued on 20 December 2013;

(iv) Guidelines on AML/CFT - Trust Company Sector issued on 30 December 2013;

(v) Guidelines on AML/CFT – Capital Market and Other Business Sectors issued on 30 December 2013; and

(vi) Guidelines on Risk-Based Approach (RBA) for the Purpose of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) issued on 17 July 2017.

Appendix II 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 FATF Recommendations. The focus on risk is intended to ensure a Labuan KRI is able to identify, assess and understand the ML/TF/PF risks to which it is exposed to and take the necessary AML/CFT/CPF control measures to mitigate them.

1.2 The Guidance on Application of Risk-Based Approach (the Guidance) seeks to:

(i) assist the Labuan KRI to design and implement AML/CFT/CPF control measures by providing a common understanding of what the RBA encompasses; and

(ii) 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 Labuan KRI has developed its own RBA, the Labuan KRI is expected to ensure its RBA achieves the outcomes as specified in the Guidelines and as further clarified in this Guidance.

1.3 The Guidance is not intended to supersede or replace any of the existing mandatory requirements on RBA that are provided in section B.1 of the Guidelines.

1.4 For a Labuan KRI under a group structure, the requirements on the RBA as provided in the Guidelines and this Guidance are applicable to a Labuan KRI at the entity level, not group level, whether as a holding or subsidiary entity. For example, for financial groups which comprise a licensed conventional bank, a licensed Islamic bank and a licensed insurance company, these are considered as three separate Labuan KRIs/entities for the purpose of complying with the Guidelines.

1.5 The RBA:

(i) recognises that the ML/TF/PF threats to a Labuan KRI vary across customers, countries, products and services, transactions and distribution channels;

(ii) allows the Labuan KRI 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 Labuan KRI's business and ML/TF/PF risk profile; and

(iii) facilitates more effective allocation of the Labuan KRI's resources and internal structures to manage and mitigate the ML/TF/PF risk identified.

1.6 The RBA provides an assessment of the threats and vulnerabilities of the Labuan KRI from being used as a conduit for ML/TF/PF. By regularly assessing the Labuan KRI's ML/TF/PF risks, it allows the Labuan KRI to protect and maintain the integrity of its business and the financial system as a whole.

2.0 Business-Based and Relationship-Based Risk Assessment

2.1 The RBA entails two (2) assessments:

A. Business-based Risk Assessment (BbRA)

In a BbRA, a Labuan KRI is expected to identify ML/TF/PF risk factors that affect its business and address the impact on the Labuan KRI's overall ML/TF/PF risks.

- ***Refer to requirements in Sections B.1.2 and B.1.3 in the Guidelines***

(i) Perform Risk Assessment

A Labuan KRI is expected to perform an assessment on the degree of ML/TF/PF risks that the Labuan KRI's business is exposed to and determine its risk appetite level. To this end, a Labuan KRI 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 Labuan KRI is expected to establish and implement policies, procedures and controls 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.

B. Relationship-based Risk Assessment (RbRA)

In an RbRA or Customer Risk Profiling, a Labuan KRI 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 Section B.1.4 in the Guidelines***

(i) Determine the Risk Parameters for Customer Risk Profiling

A Labuan KRI is expected to identify specific ML/TF/PF risk factors and parameters for customers' profiling. Where relevant, the Labuan KRI may adopt similar parameters that have been used for the assessment of the ML/TF/PF risk factors considered under the BbRA.

(ii) Conduct Risk Profiling on Customers

Based on the CDD information obtained at point of on-boarding new customers, or ongoing CDD information obtained from existing customers, as the case may be, a Labuan KRI 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 ongoing CDD that is

applicable throughout the duration of the business relationship with the customer.

(iii) Apply Customer Risk Management and Mitigation Control Measures

A Labuan KRI 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 provide financial services and the customer should be subject to more frequent and intense ongoing 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 Labuan KRI's business, size, structure and activities.

2.3 A Labuan KRI is expected to incorporate the RBA into its existing policies and procedures as part of its overall risk management function. All steps and processes in relation to the RBA for purpose of BbRA and RbRA are expected to be documented and supported by appropriate rationale and be subject to approval by Senior Management and/or the Board, as appropriate (Refer to paragraph 6.23 in the Guidelines).

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 Labuan KRI is expected to understand that assessing and mitigating ML/TF/PF risks is not a static exercise. Therefore, a Labuan KRI is expected to periodically review, evaluate and update the RBA accordingly.

2.5 The outcome of the BbRA and RbRA is to complement each other. Therefore, to effectively implement the RBA:

(i) a Labuan KRI is expected to determine reasonable risk factors and parameters for the BbRA and RbRA; and

(ii) over a period of time, data from the RbRA may also be useful in updating the parameters of the BbRA.

3.0 Business-based Risk Assessment (BbRA)

A. Perform Risk Assessment

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

3.2 The Labuan KRI 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 Labuan KRI is expected to consider all relevant risk factors that affect their business and operations, which may include the following:

(i) Specific risk factors or high risk crimes that the Labuan KRI may consider for the purpose of identifying its ML/TF risks;
(ii) Type of customers;
(iii) Geographic location of the Labuan KRI;
(iv) Transactions and distribution channels offered by the Labuan KRI;
(v) Products and services offered by the Labuan KRI;
(vi) Structure of the Labuan KRI; and
(vii) 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 Labuan KRI to another, depending on their respective circumstances. Consequently, a Labuan KRI 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 Labuan KRI.

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

(i) Customers

In conducting business transactions, the Labuan KRI is exposed to various types of customers that may pose varying degrees of ML/TF/PF risks. In analysing its customers' risk, a Labuan KRI may consider the non-exhaustive examples below:

- *Exposure to high-net-worth customers within the Labuan KRI;*
- *Nature and type of business or occupation of the customers;*
- *Nature and type of business of merchants;*
- *Exposure to foreign PEP customers;*
- *Exposure to domestic PEP customers assessed as higher risk;*
- *Exposure to customers and/or merchants related to PEPs assessed as higher risk;*
- *Exposure to customers that are legal arrangements (e.g. trusts and charities) and legal persons and the level of complexity of such legal structures;*
- *Likelihood of the customers and/or transactions originating from FATF black or grey list countries or tax haven jurisdictions;*
- *Exposure to customers from jurisdictions exposed to high levels of corruption, organised crime and/or drug production/distribution;*
- *Exposure to customers that are mostly domiciled in, or conducting business in or through, countries that are listed by FATF in its Public Statement or the Government of Malaysia, or sanctioned by the United Nations Security Council;*
- *High growth in customer account base;*
- *Exposure to customers that authorise a proxy/agent to operate the account on their behalf;*
- *Exposure to non-resident customers;*
- *Exposure to companies that have nominee shareholders or shares in bearer form;*
- *Exposure to legal persons or arrangements that are personal asset holding vehicles.*

(ii) Countries or Geographic Location

A Labuan KRI should take into account such factors including the location of the Labuan KRI's holding company, head office, branches and subsidiaries and agents (where applicable), and whether its holding company is located within a jurisdiction with full AML/CFT/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 e.g. countries identified by FATF in its Public Statement, countries designated by the Government of Malaysia, countries subjected to sanctions by the United Nations Security Council;*
- *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*
- *Jurisdictions that have been identified by credible sources as providing funding or support for money laundering, terrorism or proliferation of weapons of mass destruction.*

(iii) Transactions and Distribution Channels

A Labuan KRI 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, transactions conducted with third party agents of the Labuan KRI may be more vulnerable to ML/TF/PF in comparison to those conducted at the Labuan KRI's own branches. In this regard, a Labuan KRI 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 Labuan KRI, including the following non-exhaustive examples:

- *Mode of distribution e.g. direct channel, brokers, bancassurance, introducers, online or technology based transaction;*
- *Mode of payment e.g. wire transfers, e-payments;*
- *Anonymous transactions or other form of incentives*
- *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.*

(iv) Products and Services

Given the variety of financial products in the market, a Labuan KRI 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 Labuan KRI may take into account are as follows:

- *Nature of the products i.e. transferability/liquidity of the products;*
- *Level of complexity of the products and services;*
- *Bearer instruments;*
- *Electronic money and services e.g. e-money, e-wallet etc.;*
- *Domestic and international private banking facilities and/or trust and asset management products/services;*
- *E-banking or mobile banking products and services;*
- *Volume of stored value cards offered with no restrictions;*
- *Products that return a significant portion of premiums paid as surrender value in the event of surrender or early termination;*
- *Products with a short maturity period;*
- *Payment instruments with funds transfer /cross border facility; and*
- *Payment instruments with cash withdrawal facility.*

(v) Labuan KRI's Structure

The ML/TF/PF risk of the Labuan KRI may differ according to its size, structure and nature of business. Appropriate assessment of its business model and structure may assist a Labuan KRI to identify the level of ML/TF/PF risks that it is exposed to. In this regard, a Labuan KRI may take into account the following non-exhaustive examples:

- *Number of branches, subsidiaries and/or agents;*
- *Size of the Labuan KRI relative to industry/sector;*
- *Number and profile of employees;*
- *Degree of dependency on technology;*
- *Number of foreign correspondent financial institution accounts with inadequate AML/CFT/CPF controls, policies and procedures;*
- *Number of foreign correspondent financial institutions accounts located in higher risk jurisdictions;*
- *Level of staff turnover, especially in key personnel positions*

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

Under the NRA, a Labuan KRI is expected to take into account the following:

- *Sectors identified as highly vulnerable to ML/TF/PF risks and the Labuan KRI's 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 Labuan KRI's mitigating measures to detect and deter such illegal proceeds or in preventing dealings with customers involved in such illicit activities;*
- *Terrorism Financing and/or Proliferation Financing risks faced by the industry.*

(vii) Other Factors

A Labuan KRI 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 Labuan KRI'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 the FInD, BNM and Labuan FSA; and*
- *Whether the Labuan KRI has been subjected to service any freeze or seize order by any law enforcement agencies pursuant to the AMLA, Dangerous Drugs (Forfeiture of Property) Act 1988, Malaysian Anti-Corruption Commission Act 2009, etc*

3.5 In considering each risk factor mentioned above, a Labuan KRI 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 Labuan KRI 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 Labuan KRI:

Example 1: For all sectors

Risk Factor	Examples	Formulated Parameters
Customer	Significant growth of customer account base	• Customer base increased more than 30% within a year • Number of high risk customers and businesses totalling more than 30% of total loans and deposits
	Significant growth in percentage of high net worth customers	• Customers with net worth of RM5 million or more

Risk Factor	Examples	Formulated Parameters
	Percentage of local and foreign customers	• Customers originating from high-risk jurisdictions domestically, regionally and globally
Transactions and Distribution Channels	Cash intensive or other forms of anonymous transactions	• High volume of cash transactions above RM50,000 within a year • High volume of conversion of ringgit to foreign currency by a single customer exceeding RM50,000 per transaction within a year • High volume of anonymous / proxy transactions exceeding RM50,000 per transaction within a year
	Percentage of non-face-to-face transactions	• Non-face-to-face transactions exceeding 50% of total transactions
	Frequency and amount of cash payments	• Cash transactions above RM10,000
	Wide array of e- banking products and services	• More than 30% of new accounts are opened via internet, mail or telephone without prior relationship
Findings of the NRA	Sectors identified as highly vulnerable to ML/TF/PF risks	• Number of customers with occupation or nature of business from highly vulnerable sectors identified under the NRA

Note: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which a Labuan KRI should apply in assessing the ML/TF/PF risks of the business. A Labuan KRI is 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 Labuan KRI 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 Labuan KRI is willing to accept (i.e. the Labuan KRI'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, procedures and controls adopted by the Labuan KRI.

3.8 Apart from ensuring that the risk assessment is reflected in its policies and procedures, a Labuan KRI is also expected to justify the outcome of the risk assessment conducted. A Labuan KRI is reminded of the requirement under the AMLA to maintain proper records on any assessments and approvals by Senior Management and/or the Board on the ML/TF/PF risk assessments conducted to enable reviews to be conducted as and when it is requested by the relevant supervisory authorities.

B. Formulate and Implement Business Risk Management and Mitigation Control Measures

3.9 Once a Labuan KRI has identified and assessed the ML/TF/PF risks it faces after performing its risk assessment under section 3 above, a Labuan KRI 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

(i) nature, scale and complexity of the Labuan KRI's operating structure;
(ii) diversity of the Labuan KRI's operations, including geographical locations;
(iii) types of customers;
(iv) products or services offered;

(v) distribution channels used either directly, through third parties or agents or on non-face-to-face basis;

(vi) volume and size of transactions; and

(vii) degree to which the Labuan KRI has outsourced its operations to other entities (Group).

3.12 The following are non-exhaustive examples of the risk controls that Labuan KRI may adopt:

(i) restrict or limit financial transactions;

(ii) require additional internal approvals for certain transactions and products or services;

(iii) conduct regular training programmes for directors and employees or increase resources where applicable;

(iv) employ technology-based screening or system-based monitoring of transactions; and

(v) employ biometric system for better customer verification.

4.0 Relationship-based Risk Assessment (RbRA)

A. Determine the Risk Parameters for Customer Profiling

A Labuan KRI 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 Labuan KRI in identifying the ML/TF/PF risk factors for customers for the purpose of risk profiling. Refer to Example 2 below for illustration purposes.

Example 2 for all sectors:

Risk Factor	Parameters determined for risk profiling		Risk Rating
Customer	Type	Individual / Group insured members	Low
		Legal Person	Medium
		Legal Arrangement	High
	Net Worth*[24]	Less than RM500,000	Low

[24] Foreign currency equivalent.

Risk Factor	Parameters determined for risk profiling		Risk Rating
		RM500,000 – RM3 million	Medium
		Above RM3 million	High
	Nationality	Low risk countries	Low
		Countries neighbouring high-risk or sanctioned countries	Medium
		High-risk or sanctioned countries	High
	Country of Origin	Malaysia	Low
		Singapore	Medium
		North Korea	High
	Country of Residence	Malaysia	Low
		Singapore	Medium
		North Korea	High
Transaction or Distribution Channel	Over the Counter / Direct / Bancassurance		Low
	On behalf / Through intermediaries and/or agents		Medium
	Non-Face-to-face		High
Products and Services	Savings Account		Low
	Unit Trust		Medium
	Private Banking		High
Product Features	Pure insurance/takaful products with zero or minimal savings/investment element (e.g. group/individual policies with life/medical/PA coverage)		Low
	Products with the following features but not limited to: • Products that return a portion of premiums paid as surrender value in the event of surrender or early termination		Medium
	Products with the following features but not limited to: • Products that return a significant portion of premiums paid as surrender value in the event of surrender or early termination • Products that allow top-up and/or partial/full withdrawal • Products with a short maturity period		High

***Note 1**: The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which a Labuan KRI should apply for purpose of client risk profiling. A Labuan KRI is 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 a Labuan KRI, which could be based on more granular approach e.g. four-scale or five-scale or more rating model.*

4.1 Where relevant, a Labuan KRI may adopt similar risk factors and parameters that have been used for the assessment of the ML/TF/PF risks considered under BbRA.

4.2 The different RbRA 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.

4.3 Identifying one high risk indicator for a customer does not necessarily mean that the customer is high risk[25]. The RbRA ultimately requires a Labuan KRI 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 ongoing basis.

4.4 Therefore, a Labuan KRI is expected to ensure that the CDD information obtained at the point of on-boarding and ongoing due diligence is accurate and up to date.

B. Conduct Risk Profiling on Customers

4.5 Based on the processes under section 5 below, a Labuan KRI 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 Labuan KRI to determine whether to apply standard or enhanced CDD measures in respect of each customer.

4.6 A Labuan KRI is expected to document the reason and basis for each risk profiling and risk scoring assigned to its customers.

4.7 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.

[25] Except for high risk customer relationships that have already been prescribed, e.g. foreign PEPs or customers from high risk jurisdiction identified by FATF.

4.8 While CDD measures and risk profiling of customers are performed at the inception of the business relationship, the risk profile of a customer may change once the customer has commenced transactions. Ongoing monitoring 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

4.9 Based on the risk profiling conducted on customers, a Labuan KRI 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.

4.10 Non-exhaustive examples of risk management and mitigation control measures for RbRA include:

(i)	Develop and implement clear customer acceptance policies and procedures;
(ii)	Obtain, and where appropriate, verify additional information on the customer;
(iii)	Update regularly the identification of the customer and beneficial owners, if any;
(iv)	Obtain additional information on the intended nature of the business relationship;
(v)	Obtain information on the source of funds and/or source of wealth of the customer;
(vi)	Obtain information on the reasons for the intended or performed transactions;
(vii)	Obtain the approval of Senior Management to commence or continue business relationship;
(viii)	Conduct appropriate level and frequency of ongoing monitoring commensurate with risks identified;
(ix)	Scrutinise transactions based on a reasonable monetary threshold and/or pre-determined transaction patterns; and
(x)	Impose transaction limit or set a certain threshold.

4.11 In assessing a Labuan financial institution as a customer and the related business relationship under paragraph 10.4 of the Guidelines, a Labuan KRI is expected to determine the customer's risk rating using its own risk assessment

methodology. The assessment should take into account the relevant risk assessment findings referred to in paragraph 3.4(vi) together with all relevant customer-specific risk factors. CDD measures shall be commensurate with the identified risks and consideration should also be given to whether those risks can be effectively mitigated, in accordance with paragraph 10.5 of the Guidelines. Example 3 below is strictly for illustration purposes and is intended to facilitate better understanding of the application of paragraphs 10.4 and 10.5. It is not intended to serve as a prescription or recommendation on the parameters, specific thresholds, risk ratings or methodology to be adopted by the Labuan KRI:

Example 3: Risk-Based Assessment and Application of CDD Measures to a Labuan Financial Institution

Key Principle: A Labuan KRI should understand the customer and business relationship, assess individual risks using relevant risk assessment findings and customer-specific factors, and consider effective mitigation. It shall not apply blanket de-risking by excluding customers solely on the basis of sector or entity type without assessing individual risks and considering effective mitigation. This approach supports financial inclusion by facilitating access to financial services where the identified ML/TF/PF risks can be effectively managed.

A Labuan bank is executing an onboarding process for a Labuan fund manager for its business transactions. For illustration purposes, the relevant sectoral risk assessment rates capital market intermediaries as “Medium” risk.

Assessment stage	Illustrative application
Stage 1: Consider relevant risk assessment findings	The bank takes into consideration relevant NRA, sectoral and thematic risk assessment findings, including vulnerabilities associated with the fund manager’s activities. The Medium sector risk rating is taken into account in the assessment.
Stage 2: Understand and assess the	The bank establishes that ownership is transparent and beneficial owners are identifiable. Expected transactions comprise management-fee receipts and

customer and business relationship	business payments, with identifiable counterparties and clear commercial purposes. The bank also assesses geographical exposure, transaction volumes and patterns, whether client funds are involved, and other relevant risk factors.
Stage 3: Determine the customer's risk rating	Based on the assessments conducted under Stage 1 and Stage 2, the bank identifies limited exposure to the relevant sector vulnerabilities. Applying its own risk assessment methodology, the bank assigns the customer a "Low" risk rating and documents its rationale. The Medium sector risk rating is considered but does not automatically determine the customer's risk classification.
Stage 4: Apply commensurate CDD measures	The bank completes the applicable standard CDD requirements, including identifying and verifying the fund manager and its beneficial owners. Having assessed the customer-specific risks and determined that the applicable controls can effectively mitigate those risks, the bank decides to proceed with onboarding and documents its assessment and reasons.

The following additional scenarios illustrate how different sectoral risk ratings are considered together with customer-specific risk factors to determine customer risk classifications and corresponding CDD measures:

Illustrative sectoral risk rating	**Illustrative customer circumstances**	**Possible customer rating and CDD approach**
Low	Transparent ownership, straightforward activities and predictable transactions, with no additional material risk factors identified.	**Low:** Standard CDD and proportionate monitoring. Simplified CDD where the requirements under section B.5.2 of the Guidelines are met.
Medium	Transparent ownership, identifiable counterparties and clear business transaction purposes, with low exposure to	**Low, where supported:** Standard CDD and proportionate monitoring.

	vulnerabilities identified in the relevant NRA.	
Medium-High	Transparent ownership, but regular cross-border receipts and payments involving several counterparties create exposure to identified sector vulnerabilities. Transaction purposes are clear and verifiable.	**Medium, where supported:** Standard CDD with more frequent or detailed monitoring and reviews.
High	Higher risk geographical exposure, complex ownership structure and expected transactions involving multiple third parties without a clear commercial rationale. These factors increase its exposure to vulnerabilities identified in the relevant NRA.	**High, where supported:** Enhanced CDD and enhanced ongoing monitoring.

Note 1: *The ratings, circumstances and CDD approaches above are illustrative and do not prescribe the same outcome for similar customers. A Labuan KRI is expected to determine and justify the customer's risk rating and corresponding CDD measures using its own risk assessment methodology, considering relevant NRA findings, applicable sectoral or thematic risk assessments and all relevant customer-specific risk factors.*

Note 2*: In relation to 'Customer 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 customer rating models adopted by a Labuan KRI, which could be based on more granular approach e.g. four-scale or five-scale or more rating model.*

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 Labuan KRI 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 Labuan KRI'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 Labuan KRI may be required to update or review either its BbRA or RbRA.

5.4 A Labuan KRI 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 Labuan KRI is expected to ensure the RBA process is properly documented.

6.2 Documentation by the Labuan KRI is expected to include:

(i)	Process and procedures of the RBA;
(ii)	Information that demonstrates higher risk indicators have been considered, and where they have been considered and discarded, reasonable rationale for such decision;
(iii)	Analysis of the ML/TF/PF risks and conclusions of the ML/TF/PF threats and vulnerabilities to which the Labuan KRI is exposed to;
(iv)	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 Labuan KRI is expected to document the rationale for any additional due diligence measures it has undertaken (or any which it has waived) 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 Principal Officer) and the Board of the Labuan KRI.

Appendix III Appointment of Designated Compliance Officer

APPOINTMENT OF DESIGNATED COMPLIANCE OFFICER

The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA 2001)

Name of Institution :
Type of License :

PROFILE OF DESIGNATED COMPLIANCE OFFICER (DCO) *Important: All fields are mandatory and should not be left blank*		
Section A : Personal Details		
Name *(as per NRIC/passport)*		
NRIC Details *(for Malaysian)*	Old IC No.:	
	NRIC No.:	
Passport Details *(for Non-Malaysian)*	Passport No.:	
	Country of Issuance:	
Contact	Email Address:	
	Telephone No.:	
	Address:	
Designation	Title:	
	The DCO Post is at Management Level: Yes ☐ No ☐	
Appointment Date		
Section B : Education and Professional Qualification		
Qualification	Awarding Institution / Professional Body	Year Obtained

Appendix IV Methods to Identify and Verify Beneficial Owner

Methods to Identify Beneficial Owner

1. The following recommended source documents will assist the Labuan KRI with the identification of ultimate beneficial owners and controllers.

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

Type of legal person/ legal arrangement	Information relating to beneficial ownership	Source documents
Trust arrangement	(i) Parties to the trust (ii) Persons involved in the trust establishment (iii) Administrator of the trust (iv) Type of trust	• Trust deed • Trust registration document
Cooperatives	(i) Management of the cooperatives (ii) Rules governing the cooperatives	• Registration form of the Cooperatives • By-laws of the cooperative • Minutes of General Meeting
Clubs/Societies/ Foundations/ Charities/ NGOs	(i) Rules governing the clubs/societies/ foundations/ charities/NGOs	• Constitution/ charter/ rules • Registration form • Minutes of meeting • List of members of committee

Note: The listing is serves as a guidance and non-exhaustive.

2. The identity of beneficial owners of a legal person or legal arrangement depends on type and may be determined based on the following relationships:

Type of legal person/ legal arrangement	Relationships to be determined, if any
Companies (Private & Public)	• Shareholders • Senior management • Joint venture agreement • Persons with voting rights • Nominee directors/ shadow directors • Persons with power to appoint or remove directors • Other persons with interest within the company
Partnership	• Partners within the partnership • Other natural persons with effective control over the partnership

Type of legal person/ legal arrangement	Relationships to be determined, if any
Government linked companies - Government investment linked companies, state based company etc.	• Person authorised in the government to exerciseor influence decision making on the GLC • Other persons who exercise or influence decisionsover the GLC
Clubs/ Societies/ Foundations/ Charities/ NGOs/ Cooperatives	• Office bearer (e.g. president, secretary, treasureror other committee) • Senior management/ management team • Other member with effective control over the club/societies/ charities/ foundations/ cooperatives
Trust arrangement	• Settlor • Trustee • Protector • Beneficiaries or class of beneficiaries • Other natural persons with effective control overthe trust

3. A Labuan KRI shall take all reasonable measures to identify their customers' beneficial owner and shall be satisfied, based on the measures taken,that they know the ultimate beneficial owner. The longer the chain of entities between a legal vehicle and the more jurisdictions the entities span, the harder it is to identity the beneficial owner given the need to determine who controls each of the layers.

4. A Labuan KRI may examine as many levels of information from the entity structure as they deem necessary. "Reasonable measures[26]", in this situation refer to practical, necessary and appropriate steps taken in accordance with its risk assessment, at best efforts basis.

[26] Reasonable measures through best efforts basis by thoroughly enquiring the customer on information of beneficial owner, obtaining all relevant documents relating and reviewing all relevant entity's documents and obtaining information through online and offline publicly available sources including information maintained by public registrars.

5. A Labuan KRI to incorporate a list of reasonable measures into its internal policies and procedures to ensure standard measures for implementation.

6. In the event of a Labuan KRI is unable to identify or further verify the information of beneficial owners including of a foreign natural persons, record must show it has exhausted all reasonable measures in identifying the beneficial owners. This may include obtaining a statutory declaration from the customer on the identification of the foreign beneficial owner.

7. A Labuan KRI may choose to implement and adopt stricter internal policies and procedures with regard to identification and verification of beneficial ownership information. For example, a Labuan KRI may choose to collect information of shareholders with less than 25% ownership if they so wish.

8. In the case of a protected cell company (PCC), its cell does not have a legal personality separate from the cell company. Where a cell wishes to contract with another party, it does through the cell company on its behalf. In dealing with a PCC, the Labuan KRI must therefore establish whether the transaction is for the PCC itself or acting on behalf of its cell.

Methods to Verify Beneficial Owner

1. A Labuan KRI shall use reliable and independent source documents to verify the identity of beneficial owners.

2. A Labuan KRI is expected to perform identification and verification of beneficial owners at the on-boarding stage, as well as when there are any changes to the beneficial ownership information.

3. A Labuan KRI may conduct delayed verification of beneficial owner based on risk assessment of the customer and beneficial owner and also to comply with the delayed verification requirements of the Guidelines. A Labuan KRI is obligated to identify and verify beneficial ownership information regardless of the level of risk associated with the customer and beneficial owner.

4. Similar to the identification process, a Labuan KRI shall ensure that all reasonable measures have been taken to verify the identity of the beneficial owner of its customer. This may include but not limited to the following:

(i) conducting verification through independent documents provided by the customer;

(ii) relying on public registries or government bodies;

(iii) researching publicly available information; or

(iv) arranging a face-to-face meeting with the beneficial owner to corroborate the undertaking or declaration provided by the customer.

5. In the event that the Labuan KRI is unable to verify the beneficial owner's identity, a Labuan KRI may manage the risks of customer's activities, by either:

(i) limiting the activities of the customer;

(ii) treating the customer's activities as high risk; or

(iii) applying enhanced ongoing due diligence on the customer.

6. Where the customer falls under the list of exempted legal persons listed under paragraph 10.28 of the Guidelines, a Labuan KRI is not required to verify their directors or shareholders. Notwithstanding this, a Labuan KRI is still required to identify and maintain the information relating to the identity of the directors and shareholders, based on public register, reliable sources or other information provided by the customer.

7. In the event that there is no existing independent and reliable document submitted on a foreign beneficial owner, record must show that the Labuan KRI has exhausted all reasonable measures in verifying the foreign beneficial owner's identity.

8. A Labuan KRI may conduct a self-assessment exercise to determine whether:

(i) has taken adequate steps to verify the beneficial owner's identity; and

(ii) understand the rationale of the beneficial owner using complex corporate structures.

Appendix V False Acceptance Rate and Sampling

1. In measuring the accuracy and effectiveness of e-KYC solutions, the FAR may be considered a useful measurement as it captures the capability of the solution to identify non-genuine identification and verification cases. Generally, a lower FAR indicates that the e-KYC solution has correctly identified non-genuine or fraudulent identification and verification attempts on a regular basis.

2. FAR shall be measured based on the number of complete[27] identification and verification cased processed under e-KYC.

3. In determining FAR, a Labuan KRI shall conduct audits to classify identification and verification cases into genuine and non-genuine cases. Where it is not feasible for a Labuan KRI to audit every identification and verification case facilitated through e-KYC, a Labuan KRI may adopt a sampling approach. In doing so, a Labuan KRI shall adopt a risk-based sampling approach in determining the appropriate sample size for each module[28] of the e-KYC solution and ensure that the sample size data used to determine FAR is random, unbiased and representative of the entire population of customers.

4. In respect of paragraph 3 of this Appendix, a Labuan KRI shall conduct the audits on the first six months of e-KYC implementation. After the first six months of e-KYC implementation, the Board would need to determine and ensure that the frequency of audits conducted by the Labuan KRI commensurate with its risks and vulnerabilities.

5. In determining the appropriate sample size and group, a Labuan KRI shall ensure that FAR calculations are based on total sample case tested (i.e. if 1,000 cases were tested as the sample size, then the FAR data submitted must be based on the 1,000 cases sampled).

6. In determining the appropriate sampling approach, a Labuan KRI shall at minimum take into consideration the following sampling dimensions to ensure that FAR results from the sample size tested appropriately reflects the severity

[27] A complete identification and verification case processed under e-KYC is defined as a case where the customer has completed only the e-KYC checks as described in paragraph 2 of Appendix VI. This includes cases where e-KYC for individuals related to legal persons are implemented. This does not include other steps in the e-KYC processes (e.g credit transfer).

[28] i.e., facial recognition, liveness detection & ID document.

of any FAR threshold breaches[29]:

(i) Minimum sample size: The sample size shall minimally meet a 95% confidence level and 3% margin of error or 400 cases per month, whichever is higher.

(ii) Time-based considerations: For the first 6 months of implementation where the level of assurance of the e-KYC solution effectiveness is not yet optimal, a higher sample size is recommended to gain a higher level of assurance. Subsequent to this, a Labuan KRI may lower the sampling size tested if the FAR performance is satisfactory.

(iii) Risk-based considerations: For higher risk financial products or segments (e.g. current and savings account for customers that do not have an existing bank account), a Labuan KRI may wish to conduct a larger or full sampling approach.

(iv) Progressive sampling: Where one or more false positives are detected in the initial sample, a Labuan KRI may wish to consider a higher sample size, with a focus on e-KYC cases that may share the same profile and result in a similar outcome as the identified false positive case.

7. A Labuan KRI shall make readily available upon request by Labuan FSA, information on false positive cases that are genuine fraud attempts and cases that were falsely accepted by the solution due to other reasons[30].

8. In principle, a Labuan KRI is highly encouraged to strive to ensure that the overall FAR of the e-KYC solution is as low and close to zero as possible. Nevertheless, a Labuan KRI should also take into consideration other data points beyond FAR to form an informed view of the risk level and effectiveness of the solution. This may include factors such as the number of identification and verification cases, number of false positives, availability of other safeguards, fraud patterns observed, and the risks associated with inaccurate identification

[29] For avoidance of doubt, the higher or stricter of considerations in (i) – (iv) shall apply in determining the minimum sample size. For example, if the minimum sample size required from 5(ii) is lower than that needed to meet requirements in 5(i), the minimum sample size required shall not be lower than that of 5(i).

[30] Reasons may include but are not limited to blurry images (ID images that are blurry but may be genuine, which were falsely accepted by the solution but should have been rejected), poor image quality, poor lighting or overexposure during facial recognition/ID document verification step, poor framing of the face/ID document, etc.

for a particular product or service offered through e-KYC.

9. Generally, for e-KYC solutions leveraging the use of artificial intelligence, FAR should reduce with the increase in identification and verification cases processed.

10. To strengthen solution performance and enable quicker cadence for remedial action, a Labuan KRI shall adopt a tiered approach for FAR threshold monitoring, review and notification, as follows:

Table 1: FAR thresholds and actions to be taken

FAR thresholds	**Action to be taken when breached**
Level 1 (0% – 3%)	A Labuan KRI shall continuously monitor and improve the capability of e-KYC solutions.
Level 2 (> 3%)	A Labuan KRI shall conduct a risk assessment for notification to the Board and internal review to strengthen the e-KYC solution, including taking the appropriate rectification measures. In conducting the risk assessment, Labuan KRI may consider the FAR performance together with other relevant factors, observation points and considerations to provide an informed view of the risk level of the solution performance. For example, this may include the total number of identification and verification cases performed, number of false positives, existing mitigating controls, fraud patterns observed, etc.
Level 3 (> 5%)	Where FAR is measured to be more than 5% for any two months within a four-month period, a Labuan KRI shall notify Labuan FSA and submit an assessment of the e-KYC solution performance and mitigation measures. The notification shall be submitted to Supervision Department, as the case may be, in writing within fourteen working days

	upon the completion of the latest audit and detection of this FAR scenario. The notification to Labuan FSA shall include the following: (i) an assessment on the current performance of the e-KYC solution, including reasons for the observed level of FAR, risk level of the e-KYC solution, as well as existing mitigating controls in place; (ii) an assessment on whether the false positive case was successfully onboarded, or if the false positive case was detected and rejected through other mitigating controls[31] already in place as part of the e-KYC process. This assessment shall also include an analysis on the nature of the false positive cases (e.g. whether the cases are related to any mule activity, an emerging fraud trend/modus operandi, suspicious transactions, etc); (iii) proposed rectification actions to reduce the FAR going forward and address any identified vulnerabilities; (iv) proposed new mitigating actions or additional controls to safeguard the effectiveness of the e-KYC process; and (v) evidence that the Board is satisfied with items (i) to (iv) above, and with the decision to either continue or suspend using the same e-KYC solution, when such assessment by the Board has been made.

12. In respect of paragraph 10(iv) of this Appendix, the mitigating actions and/or additional controls may include but are not limited to the following:

(i) enhanced monitoring of customers identified and verified through e-KYC; and/or

[31] e.g., Via verification against existing credible bureau files, fraud databases or any other form of fraud detection measures.

(ii) conducting audits on e-KYC cases prior to opening an account.

13. Where FAR exceeds 5% and Labuan FSA assesses a Labuan KRI and its Board did not effectively undertake the expected rectification measures on vulnerabilities that were identified, relevant enforcement action may be taken against the Labuan KRI. Labuan FSA may also specify controls or intervention measures as deemed necessary.

Appendix VI Reporting Template on e-KYC

IDENTIFICATION AND VERIFICATION FOR e-KYC

Name of Institution :

Type of License :

Reporting Period :

---

1. The performance data below shall be recorded when reporting e-KYC identification and verification cases performed by a reporting institution[32].

DATA	(YEAR)			
	January	**…**	**June**	**Total**
Total identification and verification cases performed				
Total identification and verification cased that were accepted by solution				
Total sample size of identification and verification cases audited				
True Positive				
True Negative				
False Positive				
False Negative				
False Acceptance Ratio (%)				
False Rejection Ratio (%), defined as : $\frac{No.of\ False\ Negatives}{No.of\ False\ Negatives + No.of\ True\ Positives}\ x\ 100$				

[32] For the avoidance of doubt, the term "cases" in the table under paragraph 1 of this Appendix refer to complete identification and verification cases as defined in footnote 31 of Appendix V.

2. A robust e-KYC solution may consist of a series of e-KYC checks (e.g. document authenticity and biometric checks as outlined in paragraph 11.6) in identifying and verifying a customer. Where a financial institution utilises a series of e-KYC checks in the solution, the performance data below shall be recorded for each e-KYC check.

DATA	**(YEAR)**			
Type of e-KYC checks	**January**	**…**	**June**	**Total**
Document authenticity, segregated by-				
a) *MyKad*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
b) *Passport*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
c) *Other official identity documents*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
Liveness detection				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
Biometric matching				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				

3. Other relevant metrics to be reported:

Average time taken for completion of e-KYC process[33]. Average time taken from start of application to: (i) completion of application (minutes); (ii) account opening (hours); and (iii) account activation (hours).	

Reported by:

……

Name:

Designation and Department:

[33] Item (ii) and (iii) under paragraph 3 of this Appendix are not applicable to life insurers and family takaful operators.

Appendix VII Annual Summary Report of Exposure to Customers and Beneficial Owners from High Risk Countries

Appendix VII.1 Annual Summary Report of Exposure to Customers and Beneficial Owners from High Risk Countries for Bank

SULIT

Reporting Institution : _____
Officer's Name : _____
Designation : _____
E-mail : _____
Telephone : _____

Guides to complete the survey

- Please answer all questions below with mandatory fields marked in yellow
- Please provide amount as at 31 December YYYY (except for Question 2 & 3 which require full year data)
- Please input "n/a" for unused text field and "0" for unused number field

Category:

1. **Customers and beneficial owners from jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks emanating from the jurisdiction.**
2. **Customers and beneficial owners from jurisdictions subject to a FATF call on its members and other jurisdictions to apply enhanceddue diligence measures proportionate to the risks arising from the jurisdiction.**

QUESTION 1: No. of customer and account balance by: - product/services used, & - customer profile		Country A		Country B	
		No. of customers	Account balance @ 31Dec YYYY (USD)	No. of customers	Account balance @ 31 Dec YYYY (USD)
1. Loan / Financing					
Individual	Expatriate				
	Government Representative				
	PEP				
	Student				
	Businessman / Businesswoman				
	Housewife				
	Retiree				
	Others (please specify)				
Legal Person	Resident Company/Business				
	Foreign Company/Business				
	NGOs				
Legal Arrangement	Trust				
	Other Legal Arrangements				
Others (please specify)					
2. Deposit					
Individual	Expatriate				
	Government Representative				
	PEP				
	Student				
	Businessman / Businesswoman				
	Housewife				
	Retiree				

QUESTION 1: No. of customer and account balance by: - product/services used, & - customer profile		Country A		Country B	
		No. of customers	Account balance @ 31Dec YYYY (USD)	No. of customers	Account balance @ 31 Dec YYYY (USD)
	Others (please specify)				
Legal Person	Resident Company/Business				
	Foreign Company/Business				
	NGOs				
Legal Arrangement	Trust				
	Other Legal Arrangements				
Others (please specify)					
3. Others					
Individual	Expatriate				
	Foreign Labour				
	Government Representative				
	PEP				
	Student				
	Businessman / Businesswoman				
	Housewife				
	Retiree				
	Others (please specify)				
Legal Person	Resident Company/Business				
	Foreign Company/Business				
	NGOs				
Legal Arrangement	Trust				
	Other Legal Arrangement				
Others (please specify)					

QUESTION 2: Funds transferred to/received from in YYYY	Country A	Country B
Total funds transferred to (in USD)		
Total funds received from (in USD)		

QUESTION 3: Transactions with correspondent bank (operating in these countries) in YYYY (in USD)		Country A	Country B
Bank 1:			
Bank 2:			
Bank 3:			
Bank 4:			
Bank 5:			

Appendix VII.2 Annual Summary Report of Exposure to Customers and Beneficial Owners from High Risk Countries for Insurance and Takaful

SULIT

Reporting Institution : _____
Officer's Name : _____
Designation : _____
E-mail : _____
Telephone : _____

Guides to complete the survey

- Please answer all questions below with mandatory fields marked in yellow
- Please provide amount as at 31 December YYYY
- Please input "n/a" for unused text field and "0" for unused number field
- The institution is required to provide the overall number of customer of each jurisdiction regardless of how many policies held by the samecustomers (refer column "Total number of customers from the jurisdiction")

Category:

1. **Customers and beneficial owners from jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks emanating from the jurisdiction.**
2. **Customers and beneficial owners from jurisdictions subject to a FATF call on its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdiction.**

No. of customer and account balance by: - product/services used, & - customer profile		Country A			Country B		
		No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)	No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)
1. Whole life							
Individual	Expatriate						
	Government Representative						
	PEP						
	Student						
	Businessman / Businesswoman						
	Housewife						
	Retiree						
	Others (please specify)						
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
2. Annuity							
Individual	Expatriate						
	Government Representative						
	PEP						
	Student						
	Businessman / Businesswoman						

No. of customer and account balance by: - product/services used, & - customer profile		Country A			Country B		
		No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)	No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)
	Housewife						
	Retiree						
	Others (please specify)						
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
3. Investment-Linked							
Individual	Expatriate						
	Government Representative						
	PEP						
	Student						
	Businessman / Businesswoman						
	Housewife						
	Retiree						
	Others (please specify)						
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
4. Fire							
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
5. Marine/Aviation/Transit							
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
6. Engineering							
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						

No. of customer and account balance by: - product/services used, & - customer profile		Country A			Country B		
		No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)	No. of customers	Premium/ Contribution received @ 31 Dec YYYY (USD)	Sum Insured/ Participated (USD)
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
7. Motors							
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
8. Miscellaneous							
Legal Person	Resident Company/Business						
	Foreign Company/Business						
	NGOs						
	Government						
Legal Arrangement	Trust						
	Other Legal Arrangement						
Others (please specify)							
Total number of customers from the jurisdiction							

Appendix VIII Template for Application of Financial Intelligence ~~Network~~ System (FINS)

FINANCIAL INTELLIGENCE SYSTEM (FINS)
REGISTRATION FORM

FIRST NAME	
LAST NAME	
IDENTIFICATION NUMBER	
NAME OF INSTITUTION	
DESIGNATION	
E-MAIL ADDRESS	
USER GROUP FUNCTION	*Requestor is only allowed to be one (1) user function.* Maker ☐ Checker ☐ Main Compliance Officer ☐
CONTACT NUMBER	i) Office : ii) Fax :

Requirement for FINS accessibility:

1. PC Hardware: 1Gb RAM
2. Bandwidth: 256Kbps or higher
3. Screen Resolution: Best viewed in 1024 x 768 pixel
4. OS : Windows 2000 above
5. Web Brower: Microsoft IE 6.0 above
6. Configure pop-up blockers to by pass FINS

AUTHORISED SIGNATORIES

Requested by:

……..
Requestor
Date:

Recommended for approval

……
Principal Officer/Department Head
Date:

Appendix IX List of Transactions That May Trigger Suspicion

Labuan Banks

Examples of Transactions[34] That May Trigger Suspicion

1. Unusual amount of remittances which does not commensurate with an individual or company business activities.
2. Substantial increases in transactions of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

Accounts

3. Accounts that appear to act as pass through accounts with high volumes of credits and debits and low average monthly balances.
4. Customers who wish to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions which involve nominee names.
5. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total amount of credits would be large.
6. Any individual or company whose account shows no normal personnel banking or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. substantial increase in turnover on an account).
7. Reluctance to provide normal information when opening an account or providing information that is difficult for the reporting institution to verify.
8. Customers who appear to have accounts with several reporting institutions within the same locality but choose to consolidate funds from such accounts on regular basis for onward transmission to a third-party account.

[34] Modified from 'A Model of Best Practices to Combat Money Laundering in the Financial Sector' (September 2000) by the Commonwealth Secretariat.

9. Large withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpectedly large credit from abroad.
10. Company's representatives avoiding contact with branch officers.
11. Substantial increases in deposits or negotiable instrument by a professional firm or company, using client accounts or in-house company, or trust accounts, especially if the deposits are promptly transferred between other client's company and trust accounts.
12. Customers who show an apparent disregard for accounts offering morefavourable terms, e.g. avoidance of high interest rate facilities for large credit balances.
13. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
14. Insufficient use of normal banking facilities.
15. Large number of individuals making payments into the same account withoutany adequate explanation.
16. Large deposit made into a newly opened company/business account and withdrawn in a short period within same or next few days.
17. Sudden change of transaction pattern(s) observed in customers' account.
18. Customer deposits, withdraws or operates an account accompanied or watched or under instruction by a third party.
19. Common mobile number, address and employment reference being used by numerous individuals to open multiple bank accounts in different names.
20. Transactions with apparent front, shell or shelf companies.
21. Lifestyle that does not commensurate with employment or business line.
22. Media or other reliable sources suggest that a customer may be linked to criminal activity which could generate proceeds of crime.
23. Company receiving high value projects or contracts which are not compatible with its background or profile and is usually linked to persons related to the projects or contracts awarding authority.

24. Transferring of funds from bank accounts to high risk vehicles abroad, such as corporate trusts.
25. Customer involved in regulated activities without proper license or approval by the relevant authorities.

International Banking/Trade Finance

26. Customers introduced by an overseas branch, affiliate or any other bank based in countries where production of drugs or drug trafficking may be prevalent.
27. Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
28. Customers who make regular and large payments, including wire transfers, that cannot be clearly identified as bona fide transactions, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs, prescribed terrorist organizations or which are tax havens.
29. Building up of large balances, which are not consistent with the knownturnover of the customer's business, and subsequent transfer to accounts held overseas.
30. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing, through an account.
31. Customers who show apparent disregard for arrangements offering more favourable terms.
32. Items shipped that are inconsistent with the nature of the customer's business.
33. Customers conducting business in higher risk countries.
34. Customers shipping items through higher risk countries, including transit through non-cooperative countries.
35. Customers involved in potentially higher risk activities, including activities that may be subject to export/import restrictions (e.g. equipment for military of foreign governments, weapons, ammunition, chemical mixtures, classified defence articles and sensitive technical data).

36. Obvious over or under pricing of goods and services.
37. Obvious misrepresentation of quantity or type of goods imported or exported.
38. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
39. Customers request payment of proceeds to an unrelated third party.
40. Shipment locations or description of goods not consistent with letter of credit.
41. Significantly amended letters of credits without reasonable justification or changes to the beneficiary or location of payment.
42. Use of misleading or non-specific description of goods on trade or financial documents.
43. Inconsistent information contained in trade and financial documents, i.e. names, companies, addresses, final destination, etc.

Employees and Agents

44. Changes in employee's characteristics, e.g. lavish life styles or avoiding taking holidays.
45. Changes in employees or agent's performance, e.g. the salesman, selling products for cash, have a remarkable or unexpected increase in performance.
46. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

Examples of Transactions that May Trigger Suspicion

Brokerage and Sales

1. New Business

(a) A personal lines customer for whom verification of identity proves unusually difficult, who is evasive or reluctant to provide full details or a customer who source of funds is not clear.

(b) A corporate/trust customer where there are difficulties and delays in obtaining a copy of the statements of accounts or other documents of incorporation.

(c) A customer with no discernible reason for using the insurer's/takaful operator'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.

(d) 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.

(e) Any transaction in which the insured is unknown.

(f) Customer purchases products with termination features without concern for the product's investment performance.

(g) Customer purchases insurance/takaful products using a single, large premium/contribution payment, particularly when payment is made through unusual methods such as currency or currency equivalents.

(h) Customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.

(i) Customer borrows against the cash surrender value of permanent life insurance policies or permanent family takaful certificate, particularly when payments are made to apparently unrelated third parties.

(j) Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer/takaful operator. This would include second hand endowment and bearer insurance/takaful policies.

(k) A customer is known to purchase several insurance/takaful products and uses the proceeds from an early policy/certificate surrender to purchase other financial assets.

(l) Payment to unrelated third party.

2. Transactions which are abnormal or do not make economic sense

(a) Proposals from an intermediary not in accordance with the normal business introduced.

(b) 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.

(c) Early cancellation of policies with return of insurance premium/takaful contribution, for no discernible purpose or in circumstances which appear unusual.

(d) A number of policies/certificates entered into by the same insurer/takaful intermediary for small amounts and then cancelled at the same time.

(e) 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 anexisting customer whose current contracts are small and withregular payments only.

(f) Assignment of policies/certificates to apparently unrelated third parties.

(g) 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.

(h) 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.

(i) Customer purchasing high number of insurance policies/takaful certificates for self and family members which is not consistent with earning capacity or profile.

Settlement

1. Payment

(a) A number of policies taken out by the same insured for low insurance premiums/takaful contribution, each purchased for cash and then cancelledwith return of insurance premium/takaful contribution to a third party.

(b) Large or unusual payment of insurance premiums/takaful contribution or transaction settlement by cash.

(c) Overpayment of insurance premiums/takaful contribution with a request to refund the excess to a third party or different country.

(d) 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.

(e) 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/takaful certificate or annuity payments.

2. Disposition

(a) Payment of claims to a third party without any apparent connection to the insurance policy/takaful certificate owner.

(b) Abnormal settlement instructions, including payment to apparently unconnected parties or to countries in which the insured is not known to operate.

3. Claims and Reinsurances/Retakaful

(a) Strong likelihood of risks occurring, resulting in substantial claims, with consequently high insurance premiums/takaful contribution.

(b) Claims which, while appearing legitimate, occur with abnormal regularity.

(c) Regular small claims within insurance premium/takaful contribution limit.

(d) Treaty reinsurances/retakaful with high incidence of small claims.

(e) Regular reinsurance/retakaful claims paid overseas to third parties.

(f) Recent change of ownership/assignment of policies/certificate just prior to a loss.

(g) Abnormal loss ratios for the nature and class of risk bound under a binding authority.

Examples of Transactions that May Trigger Suspicion

1. Transactions that appear inconsistent with a customer's known profile or unusual deviations from normal transaction or relationship.
2. Transactions that require the use of complex and opaque legal entities and arrangements.
3. Transaction with entity established in jurisdictions with weak or absent AML/CFT/CPF laws and/or secrecy laws.
4. A customer who is reluctant to provide evidence of his identity or where the customer is a corporate entity, evidence of its place of incorporation and the identity of its major shareholders and its director(s) or relevant officer(s).
5. A customer is a known or suspected triad member, drug trafficker or terrorist, or where the customer has been introduced by any such persons.
6. Any situation where the identity of the customer is difficult to be determined.
7. The entry of matching buys and sells in particular securities, creating illusion of trading. Such trading does not result in a bona fide market position, and might provide 'cover' for a money launderer.
8. Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual.
9. Larger or unusual settlements of securities transactions in cash form.

Examples of Transactions that May Trigger Suspicion

1. Transactions that appear inconsistent with a customer's known profile or unusual deviations from normal transaction or relationship.
2. Transactions that require the use of complex and opaque legal entities and arrangements.
3. Transaction with entity established in jurisdictions with weak or absent AML/CFT/CPF laws and/or secrecy laws.
4. A customer who is reluctant to provide evidence of his identity or where the customer is a corporate entity, evidence of its place of incorporation and the identity of its major shareholders and its director(s) or relevant officer(s).
5. A customer is a known or suspected triad member, drug trafficker or terrorist, or where the customer has been introduced by any such persons.
6. Any situation where the identity of the customer is difficult to be determined.

Appendix X Relevant UNSCR and UNSC Sanctions Committee for Targeted Financial Sanctions on Proliferation Financing

In relation to paragraph 22.2, the relevant UNSCR or UNSC Sanctions Committee relating to prevention of proliferation of weapons of mass destruction (WMD) are as follows:

(i) Democratic People's Republic of Korea

UNSC Sanctions Committee established pursuant to Resolution 1718 (2006) concerning the Democratic People's Republic of Korea.

(ii) Islamic Republic of Iran

United Nations Security Council Resolution 2231 (2015) on Iran Nuclear Issue.

(iii) Any other UNSCR or UNSC Sanctions Committee as specified by Labuan FSA in the Guidelines.

Appendix XI Relevant UNSCR and UNSC Sanctions Committee for Targeted Financial Sanctions on Other UN-Sanctions Regimes

In relation to paragraph 22.3, the relevant UNSCR, UNSC Sanctions Committee and its corresponding Central Bank of Malaysia Act 2009 Regulation for other UN-sanctioned regimes relating to upholding of peace and security, and prevention of conflicts and human right violations are as follows:

(i) The Democratic Republic of Congo Sanctions Committee

- United Nations Security Council Committee established pursuant to Resolution 1533 (2004) concerning the Democratic Republic of the Congo
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the Democratic Republic of Congo) Regulations 2014 *(P.U.(A) 80/2014)*

(ii) 2140 Sanctions Committee (Yemen)

- United Nations Security Council Committee established pursuant to Resolution 2140 (2014)
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the Republic of Yemen) Regulations 2016 *(P.U.(A) 39/2016)*

(iii) South Sudan Sanctions Committee

- United Nations Security Council Committee established pursuant to Resolution 2206 (2015) concerning South Sudan
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the Republic of South Sudan) Regulations 2016 *(P.U.(A) 271/2016)*

(iv) Somalia Sanctions Committee

- United Nations Security Council Committee pursuant to Resolution 751 (1992) concerning Somalia
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the Federal Republic of Somalia) Regulations 2017 *(P.U.(A) 167/2017)*

(v) Libya Sanctions Committee

- United Nations Security Council Committee established pursuant to Resolution 1970 (2011) concerning Libya
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to Libya) Regulations 2017 *(P.U.(A) 318/2017)*

(vi) 1518 Sanctions Committee (Iraq)

- United Nations Security Council Committee established pursuant to Resolution 1518 (2003)
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to The Republic of Iraq) Regulations 2017 *(P.U.(A) 349/2017)*

(vii) The Central African Republic Sanctions Committee

- United Nations Security Council Committee established pursuant to Resolution 2127 (2013) concerning the Central African Republic
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the Central African Republic) Regulations 2018 *(P.U.(A) 282/2018)*

(viii) The Sudan Sanctions Committee

- United Nations Security Council Committee established pursuant to Resolution 1591 (2005) concerning the Sudan
- Central Bank of Malaysia (Implementation of the United Nations Security Council Resolutions Relating to the State of Sudan) Regulations 2019 *(P.U.(A) 38/2019)*

(ix) Any other UNSCR or UNSC Sanctions Committee as specified by Labuan FSA.

Appendix XII Template for Reporting Upon Determination of a Positive Name Match

1) **E-mail to:**

RAHSIA

AML/CFT Unit, Labuan FSA at aml@labuanfsa.gov.my

2) **Adressed to:**

Ketua Polis Negara

(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

(b) u/p : Bahagian E8,Cawangan Khas
Tingkat 24, Menara 2, Ibu Pejabat Polis
Bukit Aman, 50560, Kuala Lumpur

RE: **REPORTING OF DETERMINATION AND THE FREEZING OF FUNDS PURSUANT TO THE ANTI-MONEY LAUNDERING, ANTI-TERRORISM FINANCING AND PROCEEDS OF UNLAWFUL ACTIVITIES ACT 2001 AND ITS SUBSIDIARY LEGISLATION**

Circular / Gazette Reference No.: _____

Circular / Gazette Reference Date: _____

Match with Specified Individual / Entity (YES / NO) :_____

If YES, please fill-up the details in the form below.

No	Name	Address	NRIC / Passport No.	Institution Name (*E.g. Islamic, Investment, Insurance*) - if reporting done on group basis	Branch maintaining the account/ facility	Account No.	Account Facility/ Financial Services Type	Date financial services given (DD/MM/YYYY)	Account / Facility Status before it being frozen	Date account frozen (DD/MM/YYYY)	Balance as at...		Related Parties	Remarks
											• Banking (CR) / • Insurance (Sum Insured)	• Banking (DR) / • Insurance (Premium Received)		
1														
2														
3														
4														
5														
6														

Reporting Institution Details:

Reporting Institution Name : _____

Contact Person : _____

Designation : _____

Tel & Fax No. : _____

E-mail : _____

Reporting Date : _____

RAHSIA

Appendix XIII Template for Periodic Reporting on Positive Name Match

E-mail to:

RAHSIA

AML/CFT Unit, Labuan FSA at aml@labuanfsa.gov.my

RE: **REPORTING OF DETERMINATION AND THE FREEZING OF FUNDS PURSUANT TO THE ANTI-MONEY LAUNDERING, ANTI-TERRORISM FINANCING AND PROCEEDS OF UNLAWFUL ACTIVITIES ORDERS**

Circular / Gazette Reference No.: _____

Circular / Gazette Reference Date: _____

Match with Specified Individual / Entity (YES / NO) :_____

If YES, please fill-up the details in the form below.

No	Name	Address	NRIC / Passport No.	Institution Name (*E.g. Islamic, Investment, Insurance*) - if reporting done on group basis	Branch maintaining the account/ facility	Account No.	Account Facility/ Financial Services Type	Date financial services given (DD/MM/YYYY)	Account / Facility Status before it being frozen	Date account frozen (DD/MM/YYYY)	Balance as at...		Related Parties	Remarks
											• Banking (CR) / • Insurance (Sum Insured)	• Banking (DR) / • Insurance (Premium Received)		
1														
2														
3														
4														
5														
6														

Reporting Institution Details:

Reporting Institution Name : _____

Contact Person : _____

Designation : _____

Tel & Fax No. : _____

E-mail : _____

Reporting Date : _____

RAHSIA