BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Concept Paper

Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Designated Non-Financial Businesses and Professions (DNFBPs) & Other Non-Financial Sectors

(FOR DISCUSSION PURPOSES ONLY)

Preface

This concept paper is issued by the Financial Working Group established under the National Co-ordinating Committee for Countering Money Laundering (NCC). Members of the Financial Working Group are Bank Negara Malaysia (the Bank), Securities Commission and Labuan Financial Services Authority.

The key mandate of the Financial Working Group is to undertake the review of the existing AML/CFT policies across the reporting institutions. The aims of the review are to:

(a) address implementation issues and challenges faced by reporting institutions, regulatory and supervisory authorities;
(b) ensure consistent application of the AML/CFT policies throughout the relevant sectors; and
(c) meet the international standards on AML/CFT.

The Bank invites written comments on this concept paper, including suggestions for specific policy proposals to be further clarified or any alternative proposals that the Bank should consider. To facilitate the Bank's assessment, please support each comment with a clear rationale and supporting evidence or illustration, where relevant.

In addition to providing general feedback, reporting institutions are required to respond to the specific questions posed throughout this concept paper.

Feedback shall be submitted to the Bank **by 28 June 2013**:

Pengarah
Jabatan Perisikan Kewangan dan Penguatkuasaan
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: fiu@bnm.gov.my

Table of Contents

PART A OVERVIEW 2

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 Policies Superseded 7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

PART B POLICY REQUIREMENTS 17

11. Applicability to Foreign Branches and Subsidiaries 17
12. Risk-Based Approach Application 18
13. Customer Due Diligence (CDD) 20
14. Politically Exposed Persons (PEPs) 34
15. New Products and Business Practices 36
16. Reliance on Third Parties 36
17. Non Face-to-Face Business Relationship 37
18. Higher Risk Countries 38
19. Failure to Satisfactorily Complete CDD 39
20. Management Information System 39
21. Record Keeping 40
22. AML/CFT Compliance Programme 41
23. Suspicious Transaction Report 51
24. Cash Threshold Report 55
25. Combating the Financing of Terrorism 57
26. Non-Compliance 59

DRAFT

PART A OVERVIEW

1. Introduction

1.1 Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate which may lead to economic and social consequences. The globalisation of the financial services industry and advancement in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in utilising reporting institutions to launder illicit funds and use them as conduits for ML/TF activities.

1.2 Since the formation of the National Co-ordinating Committee for Countering Money Laundering (NCC), efforts have been undertaken to effectively enhance the AML/CFT compliance framework of reporting institutions resulting in the introduction of the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (UPW/GP1) and the relevant Sectoral Guidelines. While these efforts have addressed the ML/TF risks and vulnerabilities, there is a need to continuously assess the effectiveness of our AML/CFT framework to ensure that it continues to evolve in line with international standards.

1.3 Prior to 2012, the Financial Action Task Force (FATF) undertook a comprehensive review of the 40+9 Recommendations, which is aimed at bringing the Recommendations more up-to-date with the evolving financial, law enforcement and regulatory environment besides addressing new and emerging threats. The 2012 revision, the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt

DRAFT

a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

1.4 This Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – DNFBPs and Other Non-Financial Sectors is based on the principle that reporting institutions must conduct their business in conformity with high ethical standards and guard against undertaking any business transaction that is or may be connected with or may facilitate ML/TF, so as to safeguard the integrity and soundness of the Malaysian financial system.

2. Policy Objective

2.1 This AML/CFT- DNFBPs and Other Non-Financial Sectors is formulated in accordance with the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and the FATF 40 Recommendations and is intended to ensure that reporting institutions understand and comply with the requirements and obligations imposed on them.

3. Scope of Policy

3.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors sets out the:

(a) obligations of reporting institutions with respect to the requirements imposed under the AMLATFA;

(b) requirements of reporting institutions in implementing a comprehensive risk assessment framework; and

(c) role of the reporting institutions' Board of Directors and Senior Management (or its equivalent) in putting in place the relevant AML/CFT measures.

DRAFT

4. Legal Provisions

4.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors is issued pursuant to Section 83 of the AMLATFA.

5. Applicability

5.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors is applicable to the following reporting institutions including branches and subsidiaries outside Malaysia carrying on any activity listed in the First Schedule to the AMLATFA:

(a) Designated Non-Financial Business & Professions which consist of:

(i) licensed casino carrying on gaming business under the Common Gaming Houses Act 1953;

(ii) registered estate agents as defined in the Valuers, Appraisers and Estate Agents Act 1981;

(iii) persons carrying on activities of dealing in precious metals or precious stones carried out by companies incorporated pursuant to the Companies Act 1965 and businesses as defined and registered under the Registration of Businesses Act 1956, hereinafter referred to as dealers in precious metals/stones;

(iv) Lawyers and Accountants which consist of:

- advocates and solicitors as defined in the Legal Profession Act 1976;
- persons admitted as advocates pursuant to the Advocate Ordinance Sabah 1953;
- persons admitted as advocates pursuant to the Advocate Ordinance Sarawak 1953; and
- accountants holding valid practising certificates issued pursuant to Rule 9 of the Malaysian Institute of Accountants (Membership and Council) Rules 2001;

when they prepare or carry out the following activities for their

clients:

i. buy and sell of immovable property;
ii. manage client's money, securities or other property;
iii. manage accounts including savings and securities accounts;
iv. organise contributions for the creation, operation or management of companies; or
v. create, operate or manage legal entities or arrangements and buy and sell of business entities;

(v) Notaries public as defined in the Notaries Public Act 1959 when they exercise their powers and functions under that Act in relation to the following activities for their clients:

i. buy and sell of immovable property;
ii. manage client's money, securities or other property;
iii. manage accounts including savings and securities accounts;
iv. organise contributions for the creation, operation or management of companies; or
v. create, operate or manage of legal entities or arrangements and buy and sell of business entities;

(vi) Trust Companies as defined in the Trust Companies Act 1949; and the Corporation as defined in the Public Trust Corporation Act 1995, when they carry out the following activities for their clients:

i. act as (or arrange for another person to act as) a director or secretary of a company, a partner of a partnership or any similar position in relation to other legal entities;
ii. act as (or arrange for another person to act as) a trustee of an express trust; or
iii. act as (or arrange for another person to act as) a

nominee shareholder for another person;

(vii) Persons prescribed by the Minister or licensed by the Registrar of Companies to act as a company secretary of a company pursuant to section 139A of the Companies Act 1965, when they, whether in person or through a firm or company, prepare or carry out the following activities for their clients

i. act as a formation agent of legal entities;

ii. act as (or arrange for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal entities;

iii. provide a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal entities or arrangement;

iv. act as (or arrange for another person to act as) a trustee of an expressed trust; or

v. act as (or arrange for another person to act as) a nominee shareholder for another person.

(b) Other Non- financial Sectors which consist of:

(i) reporting institutions hereafter referred to as licensed gaming outlets which carry out activities as a:

i. licensee as defined in the Pool Betting Act 1967;

ii. totalizator agency as defined in the Racing (Totalizator Board) Act 1961; and

iii. racing club as defined in the Racing Club (Public Sweepstakes) Act 1965.

(ii) Moneylender as defined under the Moneylenders Act 1951, Money Lenders Ordinance [*Sabah Chapter 81*] and

Moneylenders Ordinance [*Sarawak Chapter 114*]; Pawnbroking business as defined in the Pawnbrokers Act 1972.

(c) any other persons as specified by the Bank.

5.2 Where the reporting institutions are subject to more than one AML/CFT policies, the more stringent requirements shall apply.

5.3 AML/CFT policies under Paragraph 5.3 refer to documents issued pursuant to section 83 of the AMLATFA.

6. Effective Date

6.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors shall take effect on 15 July 2013.

7. Compliance Date

7.1 Compliance to the requirements outlined in this AML/CFT - DNFBPs and Other Non-Financial Sectors shall take effect immediately, unless otherwise specified.

8. Policies Superseded

8.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors supersedes:

(a) the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) (UPW/GP1) issued in November 2006;

(b) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 5 for Licensed Casino (UPW/GP1[5]) issued in February 2007;

(c) the Anti-Money Laundering and Counter Financing of Terrorism

(AML/CFT) Sectoral Guidelines 6 for Designated Non-Financial Businesses and Professions (DNFBPs) (UPW/GP1[6]) issued in February 2007;

(d) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 7 for Licensed Gaming Outlets (UPW/GP1[7]) issued in April 2007;

(e) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 8 for Licensed Moneylenders and Pawnbrokers (UPW/GP1[8]) issued in November 2007; and

(f) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 10 for Dealers in Precious Metals or Precious Stones (UPW/GP1[10]) issued in May 2008.

9. Relationship with Existing Policies

9.1 This AML/CFT – DNFBPs and Other Non-Financial Sectors shall be read together with other policy documents issued by the Bank relating to compliance with AML/CFT requirements.

10. Definition and Interpretation

10.1 For the purpose of this AML/CFT – DNFBPs and Other Non-Financial Sectors , the following definitions and interpretations apply -

"Bank"	Refers to Bank Negara Malaysia.
"beneficial owner"	Refers to any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. For legal persons, beneficial owner refers to person(s)

	who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes the natural person with a controlling interest and the natural persons who comprise the mind and management of company. Reference to "ultimately owns or control" or "ultimate effective control" refers to situation in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.
"beneficiary"	In relation to trust law, a beneficiary refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. In relation to wire transfer, refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

DRAFT

"beneficiary account"	Includes trust accounts, nominees 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.
"Board of Directors"	Refers to a governing body or a group of directors. A director includes any person who occupies the position of a director, however styled, of a body corporate or unincorporated, and includes in the case of: (a) a corporation, the same meaning assigned to it in subsection 4(1) of the Companies Act 1965; (b) a sole-proprietorships, means the sole-proprietor; and (c) a partnerships, means the senior or equity partners.
"customer"	Refers to both account holder and non-account holder includes client.
"customer due diligence"	Refers to any measures undertaken pursuant to section 16 of the AMLATFA.
"Government-linked company"	Refers to a corporate entity that may be private or public (listed on a stock exchange) where the government owns an effective controlling interest, or is owned by any corporate entity where the government is a shareholder.

DRAFT

"guidance"	Refers to practice guides which are intended to promote common understanding among the players in the industry and improve industry practices. Guidance includes interpretative guidance and examples of possible approaches and practices that can be adopted to meet the requirements. Guidance will be labelled as "Practice Guides" (PG) in this AML/CFT – DNFBPs and Other Non-Financial Sectors.
"higher risk"	Refers to circumstances where the reporting institutions assess the ML/TF risks as higher, taking into consideration, and not limited to the following factors: (a) Customer risk factors: • the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting institution and the customer); • non-resident customer; • legal persons or arrangements that are personal asset-holding vehicles; • companies that have nominee shareholders or shares in bearer form; • business that are cash-intensive; • the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; • high net worth individuals; • persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling);

DRAFT

	• businesses or activities identified by the FATF as having higher risk for ML/TF; • legal arrangements that are complex (e.g. trust, nominee); and • persons who match the red flags criteria of the reporting institutions. (b) Country or geographic risk factors : • countries having inadequate AML/CFT systems; • countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations; • countries having significant levels of corruption or other criminal activity; and • countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country. In identifying countries and geographic risk factors, reporting institutions may refer, to credible sources such as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports published by international organisations such as the United Nations. (c) Product, service, transaction or delivery channel risk factors: • anonymous transactions (which may include cash); • non face-to-face business relationships or

DRAFT

	transactions; • payment received from multiple persons and/or countries that do not fit into the person's nature of business and risk profile; and • payment received from unknown or un-associated third parties.
"higher risk countries"	Refers to countries that are listed by FATF or the Government of Malaysia with either on-going or substantial ML/TF risks or strategic AML/CFT deficiencies that pose a risk to the international financial system.
"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 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; (c) military international organisations such as the North Atlantic Treaty Organization; and (d) economic organisations such as the World Trade Organization.

DRAFT

"legal arrangement"	Refers to express trusts or other similar legal arrangements.
"legal person"	Refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, foundations, partnerships, or associations and other similar entities.
"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 of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, 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 of government, senior politicians, senior government, judiciary 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

DRAFT

	directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals of foreign, domestic PEPs, or persons entrusted with a prominent function by an international organisation.
"requirements"	Refers to requirements that are issued pursuant to substantive provisions in the relevant laws administered by the Bank and are binding. In the event of non-compliance, the Bank may take enforcement actions. "Requirements" will be labelled as "Standards" (S) in this AML/CFT – DNFBPs and Other Non-Financial Sectors.
"satisfied"	Where reference is made to a reporting institution being "satisfied" as to a matter, that reporting institution must be able to justify its assessment to the supervisory authority.
"Self-Regulatory Body (SRB)"	Refers to a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession.
"Senior Management"	Refers to any person(s) having authority and responsibility for planning, directing or controlling the

DRAFT

	activities including the management and administration of a reporting institution.
"third parties"	Refers to reporting institutions that are supervised and monitored and that meet the requirements under Paragraph 16 of this AML/CFT - DNFBPs and Other Non-Financial Sectors, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process. This definition does not include outsourcing or agency relationships because the outsourced person or agent is regarded as synonymous with the reporting institution.

DRAFT

PART B POLICY REQUIREMENTS

11. Applicability to Foreign Branches and Subsidiaries

S 11.1 Reporting institutions are required to closely monitor the reporting institution's foreign branches or subsidiaries operating in jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF or the Government of Malaysia. Such being the case, reporting institutions must apply risk mitigating steps and countermeasures, where necessary.

S 11.2 Reporting institutions are required to ensure that their foreign branches and subsidiaries apply AML/CFT measures consistent with the home country requirements. Where the minimum AML/CFT requirements of the host country are less stringent than those of the home country, the reporting institution must apply the home country requirements, to the extent that host country laws and regulations permit.

S 11.3 In the event a reporting institution's foreign branch or subsidiary is unable to observe the more stringent requirements, including the reporting of suspicious transaction due to the prohibition of the host country's laws and regulations, the reporting institution should place additional AML/CFT controls on the respective foreign branches or subsidiaries.

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

DRAFT

12. Risk-Based Approach Application

12.1 Risk Management Functions

S 12.1.1 In the context of "Risk-Based Approach", the intensity and extensiveness of risk management functions shall be guided by the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

12.2 Risk Assessment

S 12.2.1 In assessing ML/TF risks of their customers, reporting institutions are required to develop internal policies which include having the following processes in place:

(a) documenting their risk assessments and findings;

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

(c) keeping the assessment up-to-date;

(d) having a periodic assessment which commensurate with the level of ML/TF risks; and

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

S 12.2.2 Reporting institutions are required to conduct additional assessment as and when specified by the supervisory authorities.

S 12.2.3 Reporting institutions are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels.

PG 12.2.4 Reporting institutions may be guided by the national risk assessment in conducting their own risk assessments.

DRAFT

12.3 Risk Control and Mitigation

S 12.3.1 Reporting institutions are required to:

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

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

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

12.4 Risk Profiling

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

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

(a) the origin of the customer and location of business;

(b) background or profile of the customer;

(c) nature of the customer's business;

(d) customer's relationship objective;

(e) customer's financial background;

(f) structure of ownership for a legal person;

(g) risks associated with non face-to-face business relationship; and

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

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

DRAFT

S 12.4.4 Upon the initial acceptance of the customer, reporting institutions are required to regularly review the customer's risk profile.

Question 1:

The Bank seeks views on the practicality and implementation challenges of the risk-based approach as the new paragraph is introduced to ensure that reporting institutions understand and are aware of the extent of ML/TF risks.

13. Customer Due Diligence (CDD)

13.1 When CDD is required

S 13.1.1 Reporting institutions are required to conduct CDD on the customer and the person conducting the transaction:

(a) for licensed casino, when engaging any transaction involving an amount totalling RM10,000 and above;

(b) for licensed gaming outlets, when a customer winnings is equivalent to or exceeding the internal threshold set by the licensed gaming outlet;

(c) for dealers in precious metals or stones, when engaging any cash transactions involving an amount equivalent to RM50,000 and above including situations where the transactions is carried out in a single transaction or several transactions in a day that appear to be linked;

(d) for all other reporting institutions, when establishing business relations; or

(e) when carrying out any other transaction that the Bank may specify.

S 13.1.2 Notwithstanding the requirement under paragraph 13.1.1, reporting institutions are required to conduct CDD on the customer and the person conducting the transaction:

DRAFT

(a) when the reporting institution has any suspicion of ML/TF, regardless of the amount transacted;

(b) when the reporting institution has any doubt about the veracity or adequacy of previously obtained information; and

(c) any other conditions as specified by the Bank.

13.2 **What is required**

S 13.2.1 The CDD measures undertaken by reporting institutions shall comprise, at least the following:

(a) identifying and verifying the identity of the customer;

(b) identifying and verifying the identity of the beneficial ownership and person who controls the transaction;

(c) identifying and verifying the identity of any persons purporting to act on behalf of the customer and whether such person is so authorised; and

(d) obtaining information on the purpose of the transaction and intended nature of the business relationship.

13.3 **Timing of Verification**

S 13.3.1 Reporting institutions are required to verify the identity of the customer and beneficial owner before or during the course of establishing business relationship or conducting transaction for occasional customer.

PG 13.3.2 In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing business relationship, the reporting institution may complete verification after the establishment of the business relationship to allow some flexibilities for its customer to furnish the relevant documents, provided that:

DRAFT

(a) this occurs as soon as reasonably practicable;
(b) this is essential not to interrupt the normal conduct of business; and
(c) the ML/TF risks are effectively managed.

S 13.3.3 The term "reasonably practicable" under Paragraph 13.3.2(a) shall not be later than ten working days or any other period specified by the Bank.

S 13.3.4 Reporting institutions are required to document the rationale and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification.

S 13.3.5 Reporting institutions are required to have risk management procedures to mitigate or address the risk of delayed verification.

PG 13.3.6 The measures that reporting institutions may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.

13.4 ***On-Going Monitoring***

S 13.4.1 Reporting institutions are required to conduct on-going monitoring on the business relationship. Such measures shall include:

(a) monitoring and detecting patterns of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of

DRAFT

the customer's risk profile; and

(b) ensuring that the documents, data or information collected under the CDD process is kept up-to-date and relevant.

S 13.4.2 Reporting institutions are required to examine and clarify the economic background and purpose of any transaction or business relationship that:

(a) appears unusual;

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

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

(d) gives about doubt about the legality of such transaction especially with regard to complex and large transactions or higher risk customers.

S 13.4.3 The frequency of the on-going monitoring shall commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

13.5 *Existing Customer – Materiality and Risk*

S 13.5.1 Reporting institutions are required to take the necessary measures to apply CDD requirements to existing customer on the basis of materiality and risk.

S 13.5.2 In assessing materiality and risk on the existing customer under Paragraph 13.5.1, reporting institutions shall consider the following circumstances:

(a) the nature and circumstances surrounding the

DRAFT

transaction including the significance of the transaction;

(b) there is a material change in the way the account or business relationship is operated; or

(c) it discovers that the information held on the customer is insufficient or has changed.

13.6 ***Specific CDD Measures***

Individual Customer and Beneficial Owner

S 13.6.1 In conducting CDD on an individual customer and beneficial owner, the reporting institution is required to at least the following information:

(a) full name;

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

(c) permanent and mailing address;

(d) date of birth; and

(e) nationality.

S 13.6.2 In the case of lawyers, accountants, company secretaries, notaries public, trust companies and public trust corporation, reporting institutions are required to obtain from the customer and beneficial owner the following information:

(a) occupation type;

(b) name of employer or nature of self-employment/nature of business; and

(c) contact number (home, office or mobile).

DRAFT

S 13.6.3 Reporting institutions can accept any other official documents bearing the photograph of the customer and beneficial owner under Paragraph 13.6.1(b) provided that the reporting institution can be satisfied that the documents can be validated for authenticity and has the necessary required information.

Question 2:

The Bank seeks the view of practical challenges in allowing any other official documents which can be validated for authenticity for the purposes of conducting CDD.

S 13.6.4 Reporting institutions shall verify requirements under Paragraph 13.6.1(b) by requiring the customer and beneficial owner to furnish the original and make a copy of the said document.

S 13.6.5 Where there is any doubt, the reporting institution is required to request the customer and beneficial owner to produce other supporting identification documents bearing their photographs, issued by an official authority or an international organisation, to enable their identity to be ascertained and verified.

Legal Persons

S 13.6.6 For customers that are legal persons, the reporting institution is required to understand the nature of the customer's business and its ownership, including the beneficial owners and control structure.

DRAFT

S 13.6.7 Reporting institutions are required to identify the customer and verify its identity through the following information:

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

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

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

S 13.6.8 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person including the following:

(i) identification document of Directors/ Shareholders with equity interest of more than twenty five percent/Partners (certified true copy/duly notarised copies or the latest Form 24 and 49 as prescribed by the Companies Commission of Malaysia or equivalent documents for Labuan companies or foreign incorporation, may be accepted);

(ii) authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and

(iii) relevant documents such as NRIC for

DRAFT

Malaysian/permanent resident or passport for foreigner, to identify the identity of the person authorised to represent the company or business in its dealing with the reporting institution.

(b) to the extent that there is doubt under Paragraph 13.6.8(a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) 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 or arrangement through other means; or

(c) where no natural person is identified under Paragraphs 13.6.8(a) or (b) above, the identity of the relevant natural person who holds the position of senior management.

S 13.6.9 Where there is any doubt under Paragraphs 13.6.7 and 13.6.8, the reporting institution shall:

(a) conduct a basic search or enquiry on the background of such person to ensure that it has not been, or is not in the process of being, dissolved, liquidated or is a bankrupt; and

(b) verify the authenticity of the information provided by such person with the Companies Commission of Malaysia, Labuan Financial Services Authority or any other relevant agencies.

S 13.6.10 Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or certificate of incorporation and from identifying and verifying

DRAFT

the directors and shareholders of the legal person which fall under the following categories:

(a) public listed companies or corporations listed in Bursa Malaysia;
(b) foreign public listed companies:
- listed in exchanges recognised by Bursa Malaysia; and
- not listed in higher risk countries;

(c) government-linked companies in Malaysia;
(d) state-owned corporations and companies in Malaysia;
(e) authorised person licensed under the Financial Services Act 2012 and the Islamic Financial Services Act 2012,
(f) financial institutions licensed under the Capital Markets and Services Act 2007;
(g) institutions licensed under the Labuan Financial Services and Securities Act 2010 and Labuan Islamic Financial Services and Securities Act 2010; or
(h) prescribed institutions under the Development Financial Institutions Act 2002.

Legal Arrangements

S 13.6.11 For customers that are legal arrangements, reporting institutions are required to understand the nature of the customer's business and its ownership, including the beneficial owners and control structure.

S 13.6.12 Reporting institutions are required to identify the customer and verify its identity through the following information:

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

DRAFT

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

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

S 13.6.13 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

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

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

S 13.6.14 For the purposes of identifying beneficiaries of trusts that are designated by characteristic or by class, under Paragraph 13.6.13, reporting institutions are required to obtain sufficient information concerning the beneficiary in order to be satisfied that it would be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intents to exercise vested rights.

PG 13.6.15 Reporting institutions may rely on the licensed trustee or nominee to verify or confirm the identity of the beneficial owners when it is not practical to identify every beneficiary. For this purpose, reporting institutions are required to establish internal policies and procedures to mitigate associated risks. Such measures may include requiring a

DRAFT

written undertaking from the licensed trustee or nominee that identification documents of the beneficiaries have been obtained, recorded, retained and be made available promptly from the trustee upon request.

Clubs, Societies and Charities

S 13.6.16 In conducting CDD on a club, society or charity, reporting institutions shall require the club, society or charity to furnish the relevant identification and constituent documents (or other similar documents) including certificate of registration and the identification and verification of the office bearer or any person authorised to represent the club, society or charity, as the case may be.

13.7 Sector Specific CDD

13.7.1 Licensed Casino

S (a) The CDD requirement in Paragraph 13.1 shall be conducted at the following entry or exit points:

(i) when customers exchange cash for cash chips and/or playing chips at the gaming tables;

(ii) when customers exchange cash and/or vouchers for chip warrants at the cashier counters;

(iii) when customers request for cheques or wire transfers for payments of winnings and/or capital; or

(iv) when customers use their membership cards or temporary or casual cards in respect of the e-cash out facility at the cashier counters or cash dispenser machines or gaming tables.

(b) In relation to bank intermediated transactions, CDD

DRAFT

shall be conducted prior to customers being allowed to use the funds.

(c) The licensed casino is also required to carry out CDD on junket operator and its customers.

(d) The licensed casino is required to conduct CDD on the third party when the customers requesting for payment to a third party account for the amount equivalent to RM10,000 and above

(e) In addition to the requirement under Paragraph 13.7.1(d), the licensed casino must obtain the following information:
   (i) the relationship between the third party and the customer; and
   (ii) the purpose of payment to the third party.

13.7.2 Licensed Gaming Outlets

S

(a) Licensed gaming outlets are required to establish an appropriate internal threshold based on its own risk assessment for conducting CDD on the winners and such threshold shall not be revealed to the members of the public.

(b) In addition to the requirements under Paragraph 13.6.1, licensed gaming outlets are required to obtain and verify the accuracy of the following information:
   (i) ticket number;
   (ii) registration number and address of the outlet where the winning ticket was purchased; and

DRAFT

(iii) winning amount.

(c) Licensed gaming outlets are required to conduct CDD on the third party when the winner requesting for payment to a third party account for an amount equivalent to the internal threshold and above.

(d) In addition to the requirement in Paragraph 13.7.2(c), licensed gaming outlets must obtain the following information:

(i) the relationship between the third party and the customer; and

(ii) the purpose for payment to the third party.

13.7.3 Moneylender and Pawnbroking Business

(a) When an agreement between a reporting institution and a customer (borrower) involves a guarantor, the reporting institution is also required to conduct CDD on the guarantor.

13.8 **Enhanced CDD**

S 13.8.1 In addition to the CDD requirements, reporting institutions are required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include, at least, the following:

DRAFT

(a) obtaining additional information on the customer and beneficial owner (e.g. volume of assets and other information from public database);
(b) inquiring on the source of wealth and source of funds;
(c) obtaining approval from the Senior Management of the reporting institution before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office; and
(d) conducting enhanced on-going monitoring by increasing the intensity and frequency of controls applied, and selecting patterns of transactions that need further examination.

PG 13.8.2 In addition to Paragraph 13.8.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

(a) obtaining additional information on the intended level and nature of the business relationship;
(b) updating more regularly the identification data of customer and beneficial owner;
(c) inquiring on the reasons for intended or performed transactions; and
(d) requiring the first payment to be carried out through an account in the customer's name with a banking institution subject to similar CDD standards.

DRAFT

Question 3:

The Bank seeks the view on the expansion of scope of EDD measures particularly on the aspect of practicality and implementation challenges.

14. Politically Exposed Persons (PEPs)

14.1 General

S 14.1.1 The requirements set out under Paragraph 14 are applicable to family members or close associates of all types of foreign, domestic PEPs and persons entrusted with a prominent function by an international organisation.

14.2 Foreign PEPs

S 14.2.1 Reporting institutions are required to put in place a risk management framework to determine whether a customer or a beneficial owner is a foreign PEP.

S 14.2.2 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD as set out under Paragraph 13 are applicable.

14.3 Domestic PEPs or Person entrusted with a prominent function by an international organisation

S 14.3.1 Reporting institutions are required to put in place policies and procedures in identifying and assessing whether or not a customer or beneficial owner is a domestic PEP or person entrusted with a prominent function by an international organisation.

DRAFT

S 14.3.2 If the customer or beneficial owner is assessed as domestic PEP or person entrusted with a prominent function by international organisation, reporting institutions are required to assess the level of ML/TF risks posed by business relationship with the domestic PEP or person entrusted with a prominent function by international organisation.

S 14.3.3 The assessment of the ML/TF risks, as specified under Paragraph 14.3.2, shall take into accounts the following factors:

(a) customer risks;

(b) country risks;

(c) product, services, transactions or delivery channel risks; and

(d) other information gathered through publicly available information or other reasonable means.

S 14.3.4 The requirements of enhanced CDD as set out under Paragraph 13 are applicable for domestic PEPs or persons entrusted with a prominent function by an international organisation, which are assessed as higher risk.

PG 14.3.5 Reporting institutions may apply CDD measures similar to other customer for domestic PEPs or person entrusted with a prominent function by an international organisation which are not assessed as higher risk.

***Question 6**:*

The Bank seeks the view on the implementation challenges of this new requirement for domestic PEPs and persons entrusted with a prominent function by an international organisation.

DRAFT

15. New Products and Business Practices

S 15.1 Reporting institutions are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

S 15.2 Reporting institutions are required to:

(a) undertake the risk assessment prior to the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate the risks.

16. Reliance on Third Parties

Customer Due Diligence

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

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

S 16.3 Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties, including those from foreign jurisdictions.

S 16.4 The relationship between reporting institutions and their third parties shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, reporting institutions must be satisfied that the third party:

(a) can obtain immediately the necessary information concerning the identification of the customer and beneficial owner;

DRAFT

(b) has an adequate CDD process;

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

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

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

On-going Monitoring

S 16.5 Reporting institutions shall not rely on third parties to conduct on-going monitoring of its customer.

17. Non Face-to-Face Business Relationship

PG 17.1 Reporting institutions may establish non face-to-face business relationships after having in place policies and procedures to address any specific risks associated with non face-to-face business relationships. Any business relationship or transaction that avoids face-to-face contact without proper customer identification and verification may be subject to abuse by money launderers and financiers of terrorism in gaining access to the financial system.

S 17.2 Reporting institutions are required to pay special attention in establishing and conducting business relationships via information communication technology.

S 17.3 Reporting institutions are required to establish appropriate measures for customer verification that shall be as effective as that for face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.

PG 17.4 Reporting institutions may use the following measures to verify non face-to-face customer such as:

DRAFT

(a) requesting additional documents to complement those which are required for face-to-face customer;
(b) developing independent contact with the customer; or
(c) verifying customer information against database maintained by the authorities.

18. Higher Risk Countries

S 18.1 Reporting institutions are required to give special attention to business relationships and transactions with individuals, businesses, companies and reporting institutions from higher risk countries highlighted by the FATF or the Government of Malaysia as insufficiently implementing the AML/CFT international standards.

S 18.2 Where Paragraph 18.1 applies, reporting institutions are required to conduct enhanced CDD under Paragraph 13.

S 18.3 Where countermeasures are applicable, reporting institutions are required to carry out the following measures, proportionate to the level of ML/TF risk:
(a) limiting business relationship or financial transactions with identified countries or persons located in the country concerned;
(b) review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned;
(c) report on summary exposure to customer and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia on an annual basis;
(d) conduct enhanced external audit on branches and subsidiaries located in the country concerned; and
(e) conduct any other measures as specified by the Bank.

DRAFT

18.4 In addition to Paragraph 18.3, reporting institutions are prohibited from relying on a third party located in the country concerned for conducting CDD.

***Question 5*:**
The Bank seeks the views on the additional measures imposed under Paragraphs 18.3 and 18.4 when dealing with higher risk countries.

19. Failure to Satisfactorily Complete CDD

S 19.1 Reporting institutions shall not open the account, commence business relation or perform any transaction in relation to potential customer or shall terminate business relations in the case of existing customer, if the reporting institution is unable to comply with the CDD requirements.

S 19.2 In the event of failure with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report.

S 19.3 Where the reporting institution is satisfied that by performing CDD would tip off the customer, the reporting institution shall be guided by the requirement under Paragraph 23.3.1.

20. Management Information System

S 20.1 Reporting institutions must have in place an adequate management information system (MIS), either electronically or manually, to complement its CDD process. The MIS is required to provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect irregularity and/or any suspicious activity.

S 20.2 The MIS shall commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

S 20.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomaly in transactions pattern, customer's risk profile and transactions exceeding any internally specified threshold.

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

PG 20.5 The MIS may be integrated with the reporting institution's information system that contains its customer's normal transaction or business profile, which is accurate, up-to-date and reliable.

21. Record Keeping

S 21.1 Reporting institutions are required to keep the relevant records including any account, files and business correspondence and documents relating to transactions, in particular, those obtained during CDD process (including documents used to verify the identity of customers and beneficial owners) and results of any analysis undertaken, 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. The records maintained must remain up-to-date and relevant.

S 21.2 In situations where the records are subject to ongoing investigations or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the law enforcement agency that such records are no longer required.

DRAFT

S 21.3 Reporting institutions are required to retain the relevant records in the form that is admissible in court and make available to the supervisory authorities and law enforcement agencies in a timely manner.

22. AML/CFT Compliance Programme

Policies, Procedures and Controls

22.1 **Board of Directors**

S 22.1.1 *General*

(a) Board members shall understand their roles and responsibilities in managing ML/TF risks faced by the reporting institution.

(b) Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.

(c) Board members must understand the AML/CFT measures required by law, regulations, guidelines and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent it from being abused by money launderers and financiers of terrorism.

S 22.1.2 *Roles and Responsibilities*

The roles and responsibilities of the Board include to:

(a) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

(b) approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going monitoring, reporting of suspicious

DRAFT

transactions and combating the financing of terrorism;

(c) establish mechanism to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF;

(d) establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by reporting institutions;

(e) define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

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

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

(h) establish MIS that is reflective of the nature of the reporting institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

22.2 ***Senior Management***

S 22.2.1 Senior management is accountable for the implementation and management of AML/CFT compliance program in accordance with policies and procedures established by the

DRAFT

Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

S 22.2.2 *Roles and Responsibilities*

The roles and responsibilities of the Senior Management include to:

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

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

(c) establish mechanism and formulate procedures to effectively implement AML/CFT policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

(d) undertake review and propose to the Board the necessary enhancement to the AML/CFT policies to reflect changes in the reporting institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

(e) provide timely periodic reporting to the Board on the level of ML/TF risks facing the reporting institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact

DRAFT

on the reporting institution;

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

(g) appoint compliance officer at management level at Head Office and at each branch or subsidiary;

(h) provide appropriate level of AML/CFT training for its employees at all level throughout the organisation;

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

(j) ensure that AML/CFT issues raised are timely addressed; and

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

Question 6:

The Bank seeks the view on the practicality and implementation challenges related to the expansion of the roles and responsibilities of both Board and Senior Management.

22.3 **Compliance Management Arrangements at the Head Office**

S 22.3.1 The Compliance Officer acts as the reference point for AML/CFT matters within the reporting institution.

S 22.3.2 The Compliance Officer must have sufficient stature, authority and seniority within the reporting institution to participate and able to influence decisions relating to AML/CFT.

DRAFT

S 22.3.3 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.

PG 22.3.4 For the purposes of Paragraph 22.3.3, "fit and proper" may include minimum criteria relating to-

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

S 22.3.5 Reporting institutions are required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia within ten working days on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required by the Bank.

S 22.3.6 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

S 22.3.7 The Compliance Officer has a duty to ensure the following:

(a) the reporting institution's compliance with the AML/CFT requirements;
(b) implementation of the AML/CFT policies;
(c) the appropriate AML/CFT procedures, including, CDD, record-keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
(d) the AML/CFT mechanism is regularly assessed to

DRAFT

ensure that it is effective and sufficient to address any change in ML/TF trends;

(e) the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;

(f) all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;

(g) internal generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and

(h) the identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

S 22.3.8 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.

Compliance Officer for certain DNFBPs

S 22.3.9 For the purpose of administrative efficiency, in certain DNFBP sectors where AMLATFA obligations are imposed on licensed/certified individual practitioners e.g. lawyers, accountants, company secretaries and estate agents, who conduct their practice as a group e.g. in a partnership or

DRAFT

corporation, the responsibility of implementing the AML/CFT internal procedures and control may be assigned to a designated individual with management responsibilities within such group. The designated individual would assume the roles and responsibilities of the compliance officer as specified in Paragraph 22. However, each individual under the relevant profession is still deemed as a reporting institution and remains ultimately responsible for his reporting obligation under the AMLATFA.

***Question 7*:**
The Bank seeks the view on the expansion of Compliance Officers functions and expectations on carrying out their roles and responsibilities.

22.4 **Employee Screening Procedures**

S 22.4.1 The screening procedures shall apply upon hiring the employee and throughout the course of employment.

S 22.4.2 Reporting institutions are required to establish an employee assessment system that commensurate with the size of operations and risk exposure of reporting institutions to ML/TF.

S 22.4.3 The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.

22.5 **Employee Training and Awareness Programmes**

S 22.5.1 Reporting institutions are required to conduct awareness and training programmes on AML/CFT practices and measures for their employees. Such training must be

conducted regularly and supplemented with refresher course.

S 22.5.2 The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

S 22.5.3 The reporting institution must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must at least contain the following:

(a) the relevant Policy documents on AML/CFT issued by the Bank, relevant supervisory authorities or SRBs; and

(b) the reporting institution's internal AML/CFT policies and procedures.

S 22.5.4 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting institutions.

S 22.5.5 Employees who deal directly with the customer shall be trained on AML/CFT prior to dealing with customers.

PG 22.5.6 Training for all employees may provide a general background on ML/TF, the requirement and obligation to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

PG 22.5.7 In addition, training may be provided to specific categories of employees:

DRAFT

a) Front-Line Employees

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

b) Employees – Establishing Business Relationship

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

c) Supervisors and Managers

The training on Supervisors and Managers may include overall aspects of AML/CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customer, penalties for non-compliance and procedures in addressing the financing of terrorism issues.

22.6 **Independent Audit Functions**

S

22.6.1 The Board is responsible to ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFA, its Regulations and subsidiary legislations, including the relevant

DRAFT

policy documents on AML/CFT issued by the Bank as well as the requirements of the relevant laws and regulations of other supervisory authorities, if any.

S 22.6.2 The Board is required to ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor include, at a minimum:

(a) checking and testing the compliance with, and effectiveness of the AML/CFT policies, procedures and controls; and

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

S 22.6.3 The scope of independent audit shall include, at a minimum:

(a) compliance with AMLATFA, its Regulations and relevant policies;

(b) compliance with internal AML/CFT policies and procedures;

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

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

S 22.6.4 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT measures and any inadequacy in internal controls and procedures.

DRAFT

***Question 8*:**
The Bank seeks the view on the implementation challenges of the independent audit function requirements.

23. Suspicious Transaction Report

23.1 General

S 23.1.1 Reporting institutions are required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia whenever the reporting institution suspect or have reason to suspect that the transaction or attempted transaction appears unusual, the economic purpose or the legality of the transaction is not immediately clear or unusual patterns of transactions involves proceeds from an unlawful activity or the customer is involved in ML/TF, regardless of the amount of the transaction.

S 23.1.2 Reporting institutions are required to provide the required and relevant information giving rise to the suspicion in the suspicious transaction report form not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

S 23.1.3 Reporting institutions must establish a reporting system for the submission of suspicious transaction reports.

PG 23.1.4 Reporting institutions may refer to **Appendix I** to this AML/CFT – DNFBPs and Other Non-Financial Sectors which provides examples of transactions that may constitute triggers for the purposes of reporting suspicious

DRAFT

transactions.

23.2 Reporting Mechanisms

S 23.2.1 In addition to the appointment of the Compliance Officer as required under Paragraph 22, reporting institutions must appoint at each branch and subsidiary carrying out any of the businesses or activities listed in the First Schedule to the AMLATFA, a branch or subsidiary compliance officer. The branch or subsidiary compliance officer is responsible, to channel all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer. For employees at the head office, such internal suspicious transaction report would be channelled directly to the Compliance Officer.

S 23.2.2 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document the decision, supported by the relevant documents and internally file the report.

S 23.2.3 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report form through any of the following modes:

DRAFT

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

Fax : +603-2693 3625

E-mail : str@bnm.gov.my

S 23.2.4 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the compliance officer of a reporting institution must submit its suspicious transaction reports on-line:

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

S 23.2.5 The Compliance Officer must ensure that the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.

S 23.2.6 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 transaction.

S 23.2.7 Reporting institutions must provide additional information and documentation as may be requested by the Bank and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.

DRAFT

S 23.2.8 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

S 23.2.9 Where a suspicious transaction report has been lodged, reporting institutions are not precluded from making a fresh suspicious transaction report when a new suspicion arises.

23.3 **Tipping Off**

S 23.3.1 In cases where the reporting institution form a suspicion of ML/TF and reasonably believe that performing the CDD process would tip off the customer, the reporting institution are permitted not to pursue the CDD process and instead is required to file a suspicious transaction report.

23.4 **Triggers for Submission of Suspicious Transaction Report**

S 23.4.1 Reporting institutions are required to establish internal criteria ("red flags") to detect suspicious transactions.

PG 23.4.2 Reporting institutions may be guided by examples of suspicious transactions provided by the Bank or other corresponding competent authorities, supervisory authorities, SRBs and international organisations.

S 23.4.3 Reporting institutions must consider submitting a suspicious transaction report when any of its customer's transaction or attempted transaction fits the reporting institution's list of "red flags".

DRAFT

23.5 **Other Issues**

S 23.5.1 Reporting institutions must ensure that the Compliance Officer maintains a complete file on all internally generated reports and any supporting documentary evidence regardless that such reports have been submitted. If there is no suspicious transaction reports submitted, the internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities when requested.

24. Cash Threshold Report

24.1 **General**

S 24.1.1 Where the requirement of cash threshold report applies, reporting institutions are required to promptly submit cash threshold report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

24.2 **Definition**

24.2.1 For the purpose of this Paragraph, the following definition are applicable:

(a) "Cash" refers to Malaysian Ringgit or foreign currency accepted as currency of exchange; and

(b) "Cash transaction" refers to transactions involving physical currencies and bearer negotiable instruments such as travellers' cheques and cash cheques but excludes bank drafts, cheques, electronic transfers or fixed deposit rollover or renewal.

24.3 **Applicability**

S 24.3.1 The requirement for cash threshold report are applicable to single or multiple cash transaction within the same account for

the amount specified by the Bank in a day.

S 24.3.2 Reporting institutions shall not offset the cash transactions against one another. Where there are deposit and withdrawal transactions, the amount should be aggregated. For example a deposit of RM40,000 and a withdrawal of RM20,000 must be aggregated to the amount of RM60,000 and hence, must be reported if it exceeds the amount specified by the Bank.

S 24.3.3 Transactions referred under Paragraph 24.3.1 include cash contra transacted from an account to different account(s) over the counter by any customer.

24.4 Reporting of Cash Threshold Report

S 24.4.1 Reporting institutions are required to establish a reporting system for the submission of cash threshold report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

S 24.4.2 The Compliance Officer must submit the cash threshold report through any of the following modes:

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

Fax : +603-2693 3625

E-mail : str@bnm.gov.my

DRAFT

S 24.4.3 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the Compliance Officer of a reporting institution must submit its cash transaction reports on-line: https://bnmapp.bnm.gov.my/fins2

S 24.4.4 The Compliance Officer must ensure that the cash threshold report is submitted within five working days, from the date of the transaction.

S 24.4.5 A submission of cash threshold report does not preclude the reporting institution's obligation to submit a suspicious transaction report.

25. Combating the Financing of Terrorism

25.1 Reporting institutions are required to keep updated with the various
S resolutions passed by the United Nations Security Council (UNSC) in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011) which require sanctions against individuals and entities belonging or related to the Taliban, Usama bin Laden and the Al-Qaida organisation.

S 25.2 Reporting institutions are required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at:

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

S 25.3 Reporting institutions are required to maintain a database of names and particulars of listed persons in the Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLATFA by the Minister of Home Affairs.

S 25.4 Reporting institutions shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.

S 25.5 Reporting institutions are required to conduct regular checks on the names of new and existing customer against the names in the database. If there is any name match, reporting institutions are required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, reporting institutions must immediately:

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

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

(c) submit a suspicious transaction report; and

(d) inform the relevant supervisory authorities as the case may be.

S 25.6 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the listed person.

S 25.7 Reporting institutions are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positive". The reporting institutions are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

PG 25.8 Reporting institutions may also consolidate their database with the other recognised lists of designated persons or entities issued by other jurisdictions.

DRAFT

26. Non-Compliance

S 26.1 Non-compliance with provisions under this AML/CFT – DNFBPs and Other Non-Financial Sectors will subject the reporting institutions to actions under:

(a) Sections 22, 66E, 86 and 92 of the AMLATFA; and/or

(b) any other relevant provisions under the laws which this AML/CFT - DNFBPs and Other Non-Financial Sectors is subject to.

DRAFT

Appendix I

Examples of Transactions That May Trigger Suspicion

Licensed Casino

1. Customer conducting small changing of chips or deposit or withdrawal of funds without gambling.

2. Customer requesting for multiple payments of winnings and capital to the same account of a third party.

3. Multiple players requesting for payments to the same beneficiary (except for customers of junket operators)

4. Fund transfer to a customer or from a customer that is through multiple financial institutions or jurisdictions in an attempt to disguise their origin.

5. Acquaintances betting against each other in even-money games and appearing that they are intentionally losing to one of the parties.

6. Customer requesting for fund transfer to charity that is unfamiliar to the casino or appears to have links to countries that have lack AML/CFT controls.

7. Buying casino chips and cashing them in without gambling.

8. Structuring the purchase of chips below the mandatory cash transaction reporting threshold.

9. Putting money into slot machines and claiming the accumulated credits as a jackpot win.

DRAFT

Designated Non-Financial Businesses and Professions

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 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 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 determine

Licensed Gaming Outlets

1. Transaction conducted indicates that the same punter frequently wins and the amount is not less than the internally set threshold.

2. The punter requests the winning amount to be paid using separate cheques for different individuals.

3. The punter presents a stack of winning tickets claiming the winnings.

4. Different punters requesting for cheques to the same individual.

DRAFT

Moneylender & Pawnbroking Business

1. Repayment of loan is accelerated by way of one lump sum payment which does not commensurate with the customer's financial standing.

2. Repayment made by a third party who has no apparent relationship with the customer.

Persons Carrying on Activities of Dealing in Precious Metals or Precious Stones

1. Unusual payment methods, for example the use of large amount of cash, multiple and/or sequentially numbered money orders, traveller's checks, cashier's checks, or payment from unknown third parties

2. Purchases or sales that are unusual or out of the norm for the particular customer or supplier or type of customer or supplier.

3. Attempt by a customer or supplier to maintain a high and unusual degree of secrecy with respect to the transaction, such as a request that the records be destroyed or not kept.

4. Unwillingness by a customer or supplier to provide the required customer identity information.

DRAFT