BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Concept Paper

Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Money Services Business Sector

(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:

(i) address implementation issues and challenges faced by reporting institutions, regulatory and supervisory authorities;

(ii) ensure consistent application of the AML/CFT policies throughout the relevant sectors; and

(iii) 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.

Responses 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 1

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 Policies Superseded 4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

PART B POLICY REQUIREMENTS 15

11. Applicability to Foreign Branches and Subsidiaries 15
12. Risk-Based Approach Application 16
13. Customer Due Diligence (CDD) 18
14. Politically Exposed Persons (PEPs) 28
15. New Products and Business Practices 30
16. Wire Transfers (Remittance) 31
17. Money and value transfer services (MVTS) 35
18. Non Face-to-Face Business Relationship 36
19. Higher Risk Countries 36
20. Failure to Satisfactorily Complete CDD 37
21. Management Information System 37
22. Record Keeping 38
23. AML/CFT Compliance Programme 40
24. Suspicious Transaction Report (STR) 50
25. Combating the Financing of Terrorism 54
26. Non-Compliance 56

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

DRAFT

Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

1.4. This Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Money Services Business Sector 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 – Money Services Business Sector 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.

DRAFT

3. Scope of Policy

3.1 This AML/CFT – Money Services Business Sector sets out the:

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

(b) requirements of the 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.

4. Legal Provisions

4.1 This AML/CFT – Money Services Business Sector is issued pursuant to:

(a) Section 83 of the AMLATFA; and

(b) Section 74 of the Money Services Business Act 2011

5. Applicability

5.1 This AML/CFT – Money Services Business Sector 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) money services business licensed under the Money Services Business Act 2011; and

(b) 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 requirement shall apply.

DRAFT

6. Effective Date

6.1 This AML/CFT – Money Services Business Sector shall take effect on 15 July 2013.

7. Compliance Date

7.1 Compliance to the requirements outlined in this AML/CFT – Money Services Business Sector shall take effect immediately, unless otherwise specified by the Bank

8. Policies Superseded

8.1 This AML/CFT – Money Services Business Sector supersedes:

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

(b) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 3 for Licensed Money Changer and/or Non-Bank Remittance Operators (UPW/GP1[3]) issued in November 2006

9. Relationship with Existing Policies

9.1 This AML/CFT – Money Services Business Sector shall be read together with other policy documents issued by the Bank relating to compliance with AML/CFT requirement.

DRAFT

10. Definition and Interpretation

10.1 For the purpose of this AML/CFT – Money Services Business Sector, the following definitions and interpretations apply -

"accurate"	Refers to information that has been verified for accuracy.
"Bank"	Refers to Bank Negara Malaysia.
"batch transfer"	Refers to a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may or may not be ultimately intended for different persons.
"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.

DRAFT

"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.
"beneficiary reporting institutions (reporting institutions conducting inward remittance)"	Refers to the reporting institution which receives the wire transfer from the ordering reporting institution directly or through an intermediary reporting institution and makes the fund available to the beneficiary.
"Board of Directors"	Refers to a governing body or a group of directors. A director includes any person who occupies a position of a director, however styled, of a body corporate or unincorporated, and includes in the case of: (a) a corporation, the same meaning assigned to it in sub-section 4(1) of the Companies Act 1965;

DRAFT

	(b) a sole proprietorship, means the sole proprietor; and (c) a partnership, means the senior or equity partners.
"cover payment"	Refers to a wire transfer that combines a payment message sent directly by the ordering reporting institution to the beneficiary reporting institution with the routing of the funding instruction (the cover) are carried out or performed through one or more intermediary reporting institutions.
"cross-border wire transfer"	Refers to any wire transfer where the ordering reporting institution and beneficiary reporting institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the reporting institutions involved is located in a different country.
"customer"	Refers to a person for whom the licensee undertakes or intends to undertake business transactions. It includes account holder and non-account holder.
"customer due diligence"	Refers to any measures undertaken pursuant to section 16 of the AMLATFA.
"domestic wire transfers"	Refers to any wire transfer where the ordering reporting institution and beneficiary reporting 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 though the system used to transfer the payment message may be located outside Malaysia.

DRAFT

"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.
"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 AML/CFT – Money Services Business Sector.
"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

DRAFT

	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); • legal arrangements that are complex (e.g. trust, nominee); and • any 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

DRAFT

	risk factors: • anonymous transactions (which may include cash); • 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 for which countermeasures are being applied to protect the international financial system from the on-going and substantial ML/TF risks emanating from the named countries. (website should be provided)
"intermediary reporting institution"	Refers to the reporting institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering reporting institution and the beneficiary reporting institution, or another intermediary reporting 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

DRAFT

	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.
"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 include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities.
"money services business"	Refer to the definition under the Money Services Business Act 2011.
"Money or value transfer service (MVTS)"	Refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other forms to a beneficiary by means of communication, message, transfer, or to a clearing network to which a MVTS provider belongs. Transactions performed by such services can involve one or more intermediary and a final payment to a third party, and may include any new payment methods. Sometimes this services have ties to particular geographic region and are describe using a variety of a specific terms, including *hawala*, *hundi*, and *fei-chen*.

DRAFT

"ordering reporting institution (reporting institution conducting outward remittance"	Refers to the reporting 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 reporting institution to perform the wire transfer.
"person"	Includes a body of persons, corporate or unincorporate.
"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, 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 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

DRAFT

	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 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 – Money Services Business Sector.
"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.
"Senior Management"	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a reporting institution.
"serial payment"	Refers to a direct sequential chain of payment where the wire transfer and accompanying payment messages travel together from the ordering reporting institution to the beneficiary reporting institution directly or through one or more intermediary reporting institutions (e.g. correspondent banks).

DRAFT

"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.
"wire transfer (remittance)"	Refers to any transaction carried out on behalf of an originator through a reporting institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary reporting institution, irrespective of whether the originator and the beneficiary are the same person.

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 counter-measures, 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	If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirement, the reporting institution is required to apply appropriate additional measures to manage the ML/TF risks, and report to their home supervisors on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.
PG	11.4	In addition, the reporting institution may consider ceasing the operations of the said branch or subsidiary that is unable to put in place the necessary mitigating control as required under Paragraph 11.3.

DRAFT

	Question 1: The Bank seeks views on the proposal to include the requirement to report on the reporting institution's assessment on the level of ML/TF risks.	
	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.
	12.2.2	Reporting institutions are required to conduct additional assessment, as and when required by the supervisory authority.
S	12.2.3	Reporting institutions are required to take appropriate steps

DRAFT

		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	12.2.3	Reporting institutions may be guided by the national risk assessment in conducting their own risk assessment.
PG	12.2.4	Reporting institutions may refer to **Appendix I** to this AML/CFT – Money Services Business Sector for guidance on how to conduct risk assessment.
	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;

DRAFT

		(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.
S	12.4.4	Upon the initial acceptance of the customer, reporting institutions are required to regularly review the customer's risk profile.
	Question 2: 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 institution understand and are aware of the extent of the 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 person conducting the transaction, when:

DRAFT

		(a) establishing business relations, where applicable; (b) providing money services business for transaction involving an amount equivalent to RM3,000 and above; (c) it has any suspicion of ML/TF regardless of the amount transacted; or (d) it has any doubt about the veracity or adequacy of previously obtained information.
	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.
	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

DRAFT

		undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer's risk profile; and (b) ensuring that 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 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.

DRAFT

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 transaction including the significance of the transaction; (b) there is a material change in the way the 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 obtain 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 the beneficial owner; (c) permanent and mailing address; (d) date of birth; and (e) nationality.
S	13.6.2.	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 documents can be validated for authenticity and has the necessary required information.

DRAFT

	Question 3: The Bank seeks the view of practical challenges in allowing any other official documents which can be validated for authenticity for the purpose of conducting CDD.	
S	13.6.3.	Reporting institutions shall verify the 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	13.6.4.	Where there is any doubt, the reporting institution is required to request the customer and beneficial owner to produce other supporting identification documents bearing a their photographs, issued by an official authority or an international organisation, to enable the customer's identity to be ascertained and verified.
	Legal Persons	
S	13.6.5.	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, where applicable.
S	13.6.6.	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

DRAFT

		(c) the address of the registered office and, if different, from the principal place of business.
S	13.6.7.	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 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 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 13.6.7(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

DRAFT

		arrangement through other means; or (c) where no natural person is identified under Paragraphs 13.6.7 (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.
S	13.6.8.	Where there is any doubt under Paragraph 13.6.6 and 13.6.7, 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 or liquidated or is 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	13.6.9.	Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or certificate of incorporation and from identifying and verifying the directors and shareholders of the legal person which fall under the following categories:
		(a) public listed companies/corporations listed in Bursa Malaysia; (b) foreign public listed companies listed in: • 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

DRAFT

	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	13.6.10. 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, where applicable.
S	13.6.11. Reporting institutions are required to identify the customer and verify its identity through the following information: (a) name, legal form and proof of existence, or any reliable references to verify the identity of the customer; (b) the powers that regulate and bind the customer, as well as the names of relevant persons having a senior management position in the customer; and (c) the address of the registered office, and if different, a principal place of business.
S	13.6.12. Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information: (a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiary or class of

DRAFT

	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	13.6.13. For the purposes of identifying beneficiaries of trusts that are designated by characteristics or by class under Paragraph 13.6.12, reporting institutions are required to obtain sufficient information concerning the beneficiary in order to be satisfied that it would be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.
PG	13.6.14. 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 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	13.6.15. 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

DRAFT

		any person authorised to represent the club, society or charity, as the case may be.
	13.7	**Enhanced CDD**
S	13.7.1.	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:
		(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	13.7.2.	In addition to Paragraph 13.7.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified (where relevant):

DRAFT

		(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 the banking institution subject to similar CDD standards.
	13.7.3.	In relation to MSB, the following situations are deemed to be of higher risk and hence, the application on enhanced CDD applies:
		(a) when the customer sends a representative to execute the transactions; (b) activities identified by FATF as having higher risk of ML/TF; and (c) non face-to-face business relationship or transaction through bank account or in a form of instruction received from internet, fax, or telephone, with the customer of whom the business relationship has been established.
	Question 4: The Bank seeks the view on the practicality of expanding enhanced CDD requirements in line with FATF Recommendations.	
	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.
S	14.3.2	If the customer or beneficial owner is assessed as domestic PEP or person entrusted with a prominent function by an 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 an 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;

DRAFT

		(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 when the reporting institution is satisfied that such person is not assessed as higher risk.
	Question 5: The Bank seeks the view on the implementation challenges of this new requirement for domestic PEPs and persons entrusted with a prominent function by international organisation.	
	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.	**Wire Transfers (Remittance)**
	General	
S	16.1	The requirements under this Paragraph are applicable to cross-border wire transfers and domestic wire transfers including serial payments and cover payments.
S	16.2	Reporting institutions are required to observe the requirements under Paragraph 25 in carrying out wire transfer.
	Ordering Reporting Institutions (Reporting Institutions Conducting Outward Remittance)	
	Cross-border wire transfers	
S	16.3	Ordering reporting institutions are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount equivalent to RM3,000 and above are accompanied by the following:
		16.3.1 Required and accurate originator information:
		(i) name; (ii) NRIC or passport number; (iii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction; (iv) address (or in lieu of the address, date and place of birth); and

DRAFT

		(v) purpose of transaction.
	16.3.2	Required beneficiary information:
		(i) name; and (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.
S	16.4	Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and reporting institutions are required to include the originator's account number or unique transaction reference number.
S	16.5	Reporting institutions are required to ensure that the message or payment instruction for all cross-border wire transfers below RM3,000 are accompanied by the following:
		(a) Required originator information:
		(i) the name of the originator; and (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.
		(b) Required beneficiary information:
		(i) the name of the beneficiary; and (ii) account number (or a unique reference number if there is no account number), which permits traceability of the

DRAFT

		transaction.
S	16.6	The information required under Paragraph 16.4 need not be verified for accuracy except when there is a suspicion of ML/TF.
		Domestic wire transfers
S	16.7	Ordering reporting institutions are 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 reporting institution and relevant authorities by other means.
S	16.8	Where the information accompanying the domestic wire transfer can be made available to the beneficiary reporting institution and relevant authorities by other means, the ordering reporting 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 reporting institution are required to provide the information within three working days of receiving the request either form the beneficiary reporting institutions or from the relevant authorities. In the case of law enforcement agencies, information should be provided immediately upon request.
S	16.9	Ordering reporting institutions are required to maintain all originator and beneficiary information collected.
S	16.10	Ordering reporting institutions shall not execute the wire transfer if it does not comply with the requirements specified above.

DRAFT

	Intermediary Reporting institutions	
S	16.11	For cross-border wire transfers, intermediary reporting institutions are required to retain all originator and beneficiary information that accompanies a wire transfer.
S	16.12	Where the required originator or beneficiary information accompanying a cross-border wire transfer cannot be transmitted, intermediary reporting institutions are required to keep a record, of all the information received for at least six years.
S	16.13	Intermediary reporting institutions are required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.
S	16.14	Intermediary reporting institutions are required to have risk-based policies and procedures for determining:
		(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.
	Beneficiary Reporting Institutions (Reporting Institutions Conducting Inward Remittance)	
S	16.15	Beneficiary reporting institutions are required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.
S	16.16	For cross-border wire transfers of an amount equivalent to RM3,000 and above, beneficiary reporting institutions are required to verify the

DRAFT

	identity of the beneficiary, if the identity has not been previously verified, and maintain this information for a period of at least six years.
S	16.17 Beneficiary reporting institutions are required to have effective risk-based policies and procedures for determining:
	(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.
	Question 6: The Bank seeks the view on the expansion of requirements relating to wire transfer.
	17. Money and value transfer services (MVTS)
S	17.1. Reporting institutions offering MVTS either directly or as an agent to MVTS operators or providers are required to comply with all of the relevant requirements under Paragraph 16 of this AML/CFT - Money Services Business Sector in the countries in which they operate, directly or through their agents.
S	17.2. Where the reporting institutions offering MVTS control both the ordering and the beneficiary side of a wire transfer, the reporting institutions are required to:
	(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and (b) file a suspicious transaction report in any country affected by the suspicious wire transfer, and to the Financial Intelligence

DRAFT

		and Enforcement Department to the extent that host country laws and regulations permit.
	Question 7: The Bank seeks the view on the practicality of the requirement under Paragraph 17 and the implementation challenges.	
	18. Non Face-to-Face Business Relationship	
S	18.1	Reporting institutions shall not undertake any transactions without face-to-face contact with the customer and prior to the completion of the CDD measures.
	19. Higher Risk Countries	
S	19.1	Reporting institutions are required to give special attention to business relationships and transactions with individuals, businesses, companies and financial institutions from higher risk countries highlighted by the FATF or the Government of Malaysia as insufficiently implementing the AML/CFT international standards.
S	19.2	Where Paragraph 19.1 applies, reporting institutions are required to conduct enhanced CDD under Paragraph 13.
S	19.3	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

DRAFT

	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.
	19.4 In addition to Paragraph 19.3, reporting institutions are prohibited from relying on a third party located in the country concerned for conducting CDD.
	Question 8: The Bank seeks the views on the additional measures imposed under Paragraphs 19.3 and 19.4 when dealing with higher risk countries.
	20. Failure to Satisfactorily Complete CDD
S	20.1 Reporting institutions shall not 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	20.2 In the event of failure with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report.
S	20.3 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 24.3.1
	21. Management Information System
S	21.1 Reporting institutions must have in place an adequate management information system (MIS), either electronically or manually, to

DRAFT

		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	21.2	The MIS shall commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.
S	21.3	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	21.4	The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems.
PG	21.5	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.
	22. Record Keeping	
S	22.1	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.

DRAFT

S	22.2	In situations where the records are subject to on-going investigations or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the law enforcement agency that such records are no longer required.
S	22.3	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.
		Issuance of receipt
	22.4	The following information are required to be recorded in the receipt of transaction with the customer:
		(a) For money changing/ wholesale currency business: (i) the reporting institution's name, business address and telephone number; (ii) date of transaction; (iii) receipt serial number; (iv) amount and type of currency exchanged by the customer (v) amount and type of currency the customer exchanged for; (vi) exchange rate offered; (vii) fees and chargers for services provided to the customer (viii) name of customer (where applicable); and (ix) customer's NRIC or passport number (where applicable). (b) For wire transfer (remittance) business: (i) the reporting institution's name, business address and telephone number; (ii) date of transaction; (iii) receipt serial number; (iv) exchange rate offered; (v) the amount of funds to be remitted in ringgit and its

DRAFT

	equivalent amount in foreign currency to be received by the beneficiary; (vi) fees and chargers for services provided to the customer (vii) name of originator (where applicable); (viii) name of beneficiary (where applicable); and (ix) customer's NRIC or passport number (where applicable).
	23. AML/CFT Compliance Programme
	Policies, Procedures and Controls
	23.1 Board of Directors
S	23.1.1 *General*
	(a) Board members shall understand their roles and responsibilities in 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	23.1.2 *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;

DRAFT

	(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 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.

DRAFT

	23.2 Senior Management	
S	23.2.1	Senior management is accountable for the implementation and management of AML/CFT compliance program in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.
S	23.2.2	*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;

DRAFT

	(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 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 (depending on the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile);
	(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.

DRAFT

	***Question 9*:** 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 in the context of MSB.	
	23.3 Compliance Management Arrangements at the Head Office (where applicable)	
S	23.3.1	The Compliance Officer acts as the reference point for the AML/CFT matters within the reporting institution.
S	23.3.2	The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.
PG	23.3.3	For the purposes of Paragraph 23.3.2, "fit and proper" may include minimum criteria relating to: (a) probity, personal integrity and reputation; (b) competency and capability; and (c) financial integrity.
S	23.3.4	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	23.3.5	Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

DRAFT

S	23.3.6 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 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	23.3.7. The Compliance Officer must have the necessary knowledge, expertise and authority to effectively discharge his roles and responsibilities, including being informed of the

DRAFT

			latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.
	Question 10: The Bank seeks the view on the expansion of Compliance Officers functions and expectations on carrying out their roles and responsibilities.		
	23.4	**Employee Screening Procedures**	
S		23.4.1	The screening procedures shall apply upon hiring the employee and throughout the course of employment.
S		23.4.2	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		23.4.3	The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.
	23.5	**Employee Training and Awareness Programmes**	
S		23.5.1	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		23.5.2	The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

DRAFT

S	23.5.3	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; and (b) the reporting institution's internal AML/CFT policies and procedures.
S	23.5.4	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	23.5.5	Employees who deal directly with the customer shall be trained on AML/CFT prior to dealing with customers.
PG	23.5.6	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	23.5.7	In addition, training may be provided to specific categories of employees:
		(a) Front-Line Employees
		Front-line employees may be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customer transacting in large cash, PEPs, higher risk customers

DRAFT

		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.
	23.6	**Independent Audit Functions**
S	23.6.1	The requirements for the independent audit functions shall be read together with the Guidelines on Risk Management and Internal Controls for Conduct of Money Services Business (BNM/RH/GL 022-3).
S	23.6.2	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 policy documents on AML/CFT issued by the Bank.

DRAFT

S	23.6.3	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 of the relevant AML/CFT requirements.
S	23.6.4	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	23.6.5	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.
S	23.6.6	Reporting institutions must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia within ten working days of their submission to its Board.

DRAFT

	23.6.7	Reporting institutions may appoint external auditors to carry out the functions of independent audits.
	***Question 11*:** The Bank seeks the view on the implementation challenges of the independent audit function requirement.	
	24. Suspicious Transaction Report (STR)	
	24.1 General	
S	24.1.1	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	24.1.2	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, business background of the person conducting the transaction that is connected with unlawful activities.
S	24.1.3	Reporting institutions must establish a reporting system for the submission of suspicious transaction reports.

DRAFT

PG	24.1.4	Reporting institutions may refer to **Appendix II** to this AML/CFT – Money Services Business Sector which provides examples of transactions that may constitute triggers for the purpose of reporting suspicious transactions.
	24.2	**Reporting Mechanisms**
S	24.2.1	In addition to the appointment of the Compliance Officer as required under Paragraph 23, 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	24.2.2	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	24.2.3	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	24.2.4	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	24.2.5	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	24.2.6	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	24.2.7	Reporting institutions must provide additional information and documentation as may be requested by the Bank and

DRAFT

		to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.
S	24.2.8	Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.
S	24.2.9	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.
	24.3	**Tipping Off**
S	24.3.1	In cases where the reporting institution form a suspicion of ML/TF and reasonably believe that performing the CDD process would tip off the customer, the reporting institution are permitted not to pursue the CDD process and instead is required to file a suspicious transaction report.
	24.4	**Triggers for Submission of Suspicious Transaction Report**
S	24.4.1	Reporting institutions are required to establish internal criteria (“red flags”) to detect suspicious transactions.
PG	24.4.2	Reporting institutions may be guided by examples of suspicious transactions provided by the Bank.
S	24.4.3	Reporting institutions must consider submitting a suspicious transaction report when any of its customer’s transaction or attempted transaction fits the reporting institution’s list of “red flags”.

DRAFT

	24.5	**Other Issues**
S	24.5.1	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.
	25.	**Combating the Financing of Terrorism**
S	25.1	Reporting institutions are required to keep updated with the various 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 UN 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.

DRAFT

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 the AML/CFT – Money Services Business Sector will subject the reporting institutions to actions under:

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

(b) any other relevant provisions under the laws which this AML/CFT – Money Services Business Sector is subject to.

DRAFT

Appendix I

Introduction

The Financial Action Task Force (FATF) recently in February 2012 undertook a comprehensive review of the FATF Recommendations. The revision is necessary in order to enhance the clarity of the standards, address deficiencies and ensure that the standards are updated to deal with the evolving financial landscapes and regulatory requirements around the world.

One of the key changes is the requirement for the country to apply a Risk-Based Approach in managing money laundering and terrorist financing (ML/TF) risk. This will enable the country to allocate and prioritize its AML/CFT resources effectively and at the same time, applying appropriate policy response to the identified risky and vulnerable areas. In addition, the countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

Purpose

The purpose of this guide is to assist financial institutions in its assessment of ML/TF risks. This guide covers the following two mains areas of assessment:

1. the level of ML/TF risk; and
2. the application of ML/TF risk control

The guide should complement the existing procedures that the institution already have and **should not be treated as the sole reference** in conducting the ML/TF risk assessment. It should be noted that the list of factors/examples/parameters in this guide are not exhaustive.

1. Assessing the level of ML/TF risk

Assessing ML/TF risk involves identifying aspects of the institution's business that may be susceptible to ML/TF taking into consideration factors that could influence the level of institutions' susceptibility to ML/TF risk such as:

DRAFT

a) <u>The size and complexity of the institution</u>

- The size and complexity of the institution plays an important role in how attractive or susceptible the institution is to ML/TF risk.
- The size of an institution also provides a good indication of the amount of funds and its frequency flowing through the institution as well as the likelihood of having high volume and high value of transactions, which increases the likelihood of being abused by money launderers, particularly those with large amount of funds to launder.
- Naturally, a large institution set-up is less likely to know its customer, therefore could offer a greater degree of anonymity than a small institution. Similarly, institutions that offer complex transactions across international jurisdictions could offer greater opportunities to money launderers than a purely domestic institution.

b) <u>The products / services offered and the way it delivers</u>

- Cash based products/services generally leave no audit trails and are more difficult to trace, making it attractive to money launderers.
- Products/transactions that allow customer anonymity or where transactions allow the use of third parties to conduct the business could mask the origin of the funds and hence, more vulnerable to ML/TF risk.
- Products/transactions that allow non face-to-face customers (such as via internet, telephone, post etc) are more vulnerable to fraud and identity theft. Hence, more attractive to money launderers as it could avoid detection, hide the origin of the funds as well as evade the institution's scrutiny / enforcement agencies detection of their identity.
- Products/transactions with international exposure such as fund transfer services, either via remittance, digital currency and e-money are vulnerable to ML/TF risks. The ability of the customer to move funds freely could facilitate money launderers' layering process, making it more difficult to trace and therefore, are more attractive to money launderers.

DRAFT

c) <u>The type of customers / institutions / countries your institutions deal with</u>

- Certain types of customer pose higher ML/TF risk than others. This element is important to determine the extent of institution's vulnerability to the money laundering risk posed by the customers.
- In general, Politically Exposed Persons (PEPs) and high net-worth persons are considered as higher risk. The concern placed in dealing with PEPs lies with the possibility of such PEPs abusing their public powers for their own wealth.
- Although it could be complicated to determine the level of exposure of high risk customers to the sectors, it is necessary to at least assess the degree of engagement with high risk customers and PEPs. In general, the institution that have more high risk customers and more PEP customers will indirectly carry along the associated money laundering risks within the institution.
- Other categories of customers that pose a higher ML/TF risks include (but not limited to) the following:
  - ✓ Customers involved in occasional or one-off transactions above a certain threshold;
  - ✓ Customers who use complex business structures that offer no apparent financial benefits;
  - ✓ Customers involved in cash-intensive business or business with high levels of corruption; and
  - ✓ Customers whose origin of wealth/funds cannot be easily verified and/or unnecessarily layered.
  - ✓ Unregulated or shell business / institutions are more susceptible to be used as conduit for ML/TF activities.
- Apart from the institution's own definition of countries deemed as high risk, consideration also should be done if the institutions have relations with other institutions from high risk jurisdictions, such as countries subjected to sanctions or countries identified as having inadequate AML/CFT measures (i.e. UN Designated List, FATF Public Statement).

DRAFT

- Besides the above, consideration also may be given for customer from countries known for having high level of financial secrecy, drugs producing/trafficking or war conflict.

d) Geographical coverage

- The geographical concentration and accessibility of the institution attract the launderer to launder the proceeds through the sectors. High number of branches provides better opportunity for the launderer to place and layer their illegal funds as compared to institution with less number of branches.
- The total number of branches indicates the level of geographical concentration and accessibility of the institution. The greater the business premises of the institution are scattered and are highly available all over the country, the more convenient and attractive it is to be used by money launderers.
- The coverage of ML/TF risk assessment may also be extended to the location of its branches or agents particularly those located at high risk areas or border towns.

1.1 Level of ML/TF Risk Rating

Establishing the inherent ML/TF risk assessment is primarily qualitative and highly dependent on informed judgement by the assessors. There are four levels of susceptibility to ML/TF risk based, i.e. **High (Almost Certain), Above Average (Likely), Moderate (Possible)** and **Low (Unlikely)**. The definition the level of susceptibility to ML/TF Risk is described below:

The Level of Susceptibility to ML/TF Risk	Definition
High (Almost Certain)	Current information and assessment on the risk vulnerability areas indicate that there is a high chance of ML/TF occurring in this area of business operations.

DRAFT

Above Average (Likely)	Current information and assessment on the risk vulnerability areas indicate that there is a moderate chance of ML/TF occurring in this area of business operations.
Moderate (Possible)	Current information and assessment on the risk vulnerability areas indicate that there is a small chance of ML/TF occurring in this area of business operations.
Low (Unlikely)	Current information and assessment on the risk vulnerability areas indicate that there is a low chance of ML/TF occurring in this area of business operations.

2. ML/TF Risk Control and Mitigation

2.1 The institution should develop policies and procedure to control and mitigate the ML/TF risk that has been identified

2.2 The risk mitigation should be tailored according to the identified ML/TF risk level and may includes :

- Different level of CDD process to different group of customers
- Rejection of customer/transaction which involve high risk countries
- Setting transaction limit for higher risk customer/transaction
- Different level of approval process, according to the level of ML/TF risk

2.3 The institution should ensure the policies and procedures is implemented effectively by the respective employees or business units

3. Additional Resources for Guidance to Conduct Your Risk Assessment

- Information available at the following websites may provide further guidance to your assessment on ML/TF risk:

  a) Financial Action Task Force http://www.fatf-gafi.org

  - Risk-Based Approach – Guidance for Money Service Businesses
  - Global Money Laundering and Terrorist Financing Threat Assessment (GTA)

  b) The Asia Pacific Group on Money Laundering (APG)

DRAFT

http://www.apgml.org/frameworks/

- APG Yearly Typologies Report
- Articles on Alternative Remittance Systems / Underground Banking / Hawala

c) The Australian Transaction Reports and Analysis Centre (AUSTRAC)

http://www.austrac.gov.au

- AUSTRAC Guidance Note on Risk management and AML/CTF programs
- Risk management - A tool for small-to-medium sized businesses

DRAFT

Appendix II

Examples of Transactions That May Trigger Suspicion

1. Customer is evasive or unwilling to provide information when requested especially customer who is exchanging currency equivalent to RM3,000 and above.
2. Transactions conducted are out of character with the usual conduct or profile of customers carrying out such transactions.
3. Customer using different identifications each time conducting a transaction.
4. A group of customers trying to break up a large cash transaction into multiple small transactions.
5. The same customer conducting a few small transactions in a day or at different branches/locations.
6. There are sudden or inconsistent changes in remittance/wire transfer sent/received transactions.
7. Remittances/wire transfers from different customers/jurisdiction being sent to the same customer.
8. Customer frequently remitting money to non-co-operative countries/jurisdictions.
9. Customer exchanging small denomination notes into large denomination notes, in large quantity.
10. The same customer frequently exchanging local currency into foreign currency without apparent economic or visible lawful purpose.
11. Customer frequently exchanging large amount of foreign currency but not exceeding the equivalent of RM3,000 for each transaction.

DRAFT

	12. Customer exchanging cash for numerous postal money orders in small amounts for numerous other parties.

DRAFT