



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

**UPW/GP1:
STANDARD GUIDELINES ON
ANTI-MONEY LAUNDERING AND
COUNTER FINANCING OF TERRORISM
(AML/CFT)**

**UNIT PERISIKAN KEWANGAN
BANK NEGARA MALAYSIA
NOVEMBER 2006**

CONTENT

	Page
1. INTRODUCTION	1
2. APPLICABILITY	1
3. DEFINITION	1
3.1. Money laundering	1
3.2. Financing of terrorism	2
4. CUSTOMER ACCEPTANCE POLICY	3
4.1. General	3
4.2. Risk Profiling	3
5. CUSTOMER DUE DILIGENCE	3
5.1. General	3
5.2. Individual Customers	4
5.3. Corporate Customers	5
5.4. Clubs, Societies and Charities	5
5.5. Legal Arrangements	6
5.6. Beneficial Ownership and Control	6
5.7. Reliance on intermediaries for CDD	6
5.8. Non-face-to-face Business Relationship	7
5.9. Foreign Politically Exposed Persons	7
5.10. Higher risk customers	8
5.11. Existing customers	9
6. RECORD KEEPING	9
6.1. Retention Period	9
6.2. Audit trail	9
6.3. Format	10
7. ON-GOING MONITORING	10
7.1. General	10
7.2. Management Information System	10
7.3. Special Attention	11
8. SUSPICIOUS TRANSACTION REPORTING	11
8.1. General	11
8.2. Reporting mechanisms	12
8.3. Triggers for submission of suspicious transaction report	13
8.4. Other issues	13
9. COMBATING THE FINANCING OF TERRORISM	14

10. AML/CFT COMPLIANCE PROGRAMME	15
10.1. Policies, Procedures and Controls	15
10.2. Staff Integrity	16
10.3. Compliance Officer	16
10.4. Staff Training and Awareness Programmes	17
10.5. Independent Audit	19
11. NON-COMPLIANCE WITH PROVISIONS UNDER THE AMLA	20
APPENDICES	
Appendix I - Glossary	22

1. INTRODUCTION

- 1.1. The Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism (Guidelines) are issued pursuant to section 66E and section 83 of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLA).
- 1.2. The Guidelines are established and formulated to address the requirements that must be complied by the reporting institutions under the AMLA to effectively combat money laundering and financing of terrorism activities.
- 1.3. The Guidelines are drawn up in accordance with the AMLA and the Financial Action Task Force on Money Laundering's (FATF) Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.

2. APPLICABILITY

- 2.1. The Guidelines are applicable to the reporting institutions including branches and subsidiaries outside Malaysia carrying on any activity listed in the First Schedule to the AMLA.
- 2.2. Foreign branches and subsidiaries must comply with the Guidelines and where there is conflict between the Guidelines and the regulatory requirements of the host country, the more stringent requirement must be adopted to the extent that is permitted by the host country's laws and regulations. In addition, reporting institution should pay special attention to foreign branches or subsidiaries operating in countries which have insufficiently implemented the internationally accepted AML/CFT measures.
- 2.3. 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 to the Financial Intelligence Unit in Bank Negara Malaysia due to the prohibition of the host country's laws and regulations, it must issue an exception report to the reporting institution, which must inform the Financial Intelligence Unit in Bank Negara Malaysia. In addition, the reporting institution should place additional AML/CFT controls on the respective foreign branch or subsidiary and should map out a timeline for it to comply with the requirements.

3. DEFINITION

3.1. Money laundering

- 3.1.1. In general terms, money laundering is defined as the process of converting money/property, which is derived from illegal activities to give it a legitimate appearance. There are 3 stages in money laundering, which are:

- Placement - The physical disposal of proceeds derived from illegal activities;
- Layering – Separating the illicit proceeds from their sources through transactions that disguise the audit trail and provide anonymity;
- Integration – Integrating the laundered proceeds into the economy as normal funds.

3.1.2. Section 3(1) of the AMLA, defines “money laundering” as the act of a person who:

- engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity;
- acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Malaysia proceeds of any unlawful activity; or
- conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of any unlawful activity;

where –

- as may be inferred from objective factual circumstances, the person knows or has reason to believe, that the property is proceeds from any unlawful activity; or
- in respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity.

3.2. Financing of terrorism

3.2.1. Financing of terrorism generally refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.

3.2.2. Section 3(1) of the AMLA defines a “terrorism financing offence” as any offence under section 130N, 130O, 130P or 130Q of the Penal Code. Essentially, financing of terrorism includes:

- providing or collecting property for carrying out an act of terrorism;
- providing services for terrorism purposes;
- arranging for retention or control of terrorist property; or
- dealing with terrorist property.

3.2.3. In the financing of terrorism, the focus is on the determination or use of funds, which may have been derived from legitimate sources.

4. CUSTOMER ACCEPTANCE POLICY

4.1. General

- 4.1.1. Every reporting institution should develop customer acceptance policy and procedures to address the establishment of business relationship with the customer. For that purpose, the reporting institution should identify and assess risk of customers, i.e., risk profiling, especially in identifying the type of customers associated with high risk of money laundering and financing of terrorism.
- 4.1.2. Reflective of the risk profiling conducted, the reporting institution should have reasonable measures in its internal policies and procedures, including customer due diligence, to address the different risks posed by each type of customer.

4.2. Risk Profiling

- 4.2.1. In creating the risk profile of a particular customer or type of customer, the reporting institution should at least take into consideration the following factors:
- the origin of the customer and location of business;
 - background or profile of the customer;
 - nature of the customer's business;
 - structure of ownership for a corporate customer; and
 - any other information suggesting that the customer is of higher risk.
- 4.2.2. Following the initial acceptance of the customer, the reporting institution should continuously monitor each customer's transaction activity pattern to ensure it is in line with the customer's profile. Unreasonable differences should prompt the reporting institution to reassess the customer's risk profile.

5. CUSTOMER DUE DILIGENCE

5.1. General

- 5.1.1. Every reporting institution must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records, the identity and legal existence of any person applying to do business with it. Such evidence must be substantiated by reliable and independent source documents.
- 5.1.2. Every reporting institution must conduct customer due diligence, when:
- establishing business relationship with any customer;
 - carrying out cash or occasional transaction that involves a sum in excess of the amount specified by Bank Negara Malaysia under its sectoral guidelines or relevant circular;

- it has any suspicion of money laundering or financing of terrorism; or
 - it has any doubt about the veracity or adequacy of previously obtained information.
- 5.1.3. The customer due diligence undertaken by the reporting institution should at least comprise the following:
- identify and verify the customer;
 - identify and verify beneficial ownership and control of such transaction;
 - obtain information on the purpose and intended nature of the business relationship/transaction; and
 - conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant.
- 5.1.4. Unwillingness of the customer to provide the information requested and to cooperate with the reporting institution's customer due diligence process may itself be a factor of suspicion.
- 5.1.5. The reporting institution should not commence business relation or perform any transaction, or in the case of existing business relation, it should terminate such business relation if the customer fails to comply with the customer due diligence requirements and consider lodging a suspicious transaction report with the Financial Intelligence Unit in Bank Negara Malaysia.
- 5.1.6. In certain special circumstances where the risks of money laundering and financing of terrorism are low or where measures are already in place to effectively manage such risk, the reporting institution may allow its customer due diligence process to be conducted not later than 14 days (or the period specified in the Sectoral Guidelines, where applicable) after the business relationship has been established to permit some flexibilities for its customer to furnish the relevant documents.

5.2. Individual Customers

- 5.2.1. In conducting customer due diligence on an individual customer, the reporting institution should obtain from the individual customer at least the following information:
- full name;
 - NRIC/passport number;
 - permanent and mailing address;
 - date of birth; and
 - nationality.
- 5.2.2. The reporting institution should substantiate the above required information by requiring the individual to furnish the original and make a copy of the following documents:
- NRIC for Malaysian/permanent resident; or

- Passport for foreigner.

5.2.3. Where there is any doubt, the reporting institution should request the customer to produce other supporting identification documents, preferably bearing a photograph of the customer, issued by an official authority, to enable the customer's identity to be ascertained.

5.3. Corporate Customers

5.3.1. In conducting customer due diligence on a corporate customer, the reporting institution should require the company/business to furnish the original and make a copy each of the following documents:

- Memorandum/Article/Certificate of Incorporation/Partnership;
- Identification document of Directors/Shareholders¹/Partners;
- Authorisation for any person to represent the company/business; and
- Identification document of the person authorised to represent the company/business in its dealing with the reporting institution.

5.3.2. Where there is any doubt, the reporting institution should:

- conduct a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or liquidated; and
- verify the authenticity of the information provided by the company/business with the Companies Commission of Malaysia.

5.3.3. The reporting institution should also know the beneficial owners and control structure of the corporate customers and determine the source(s) of funds of the company/business in order to ascertain any suspicion concerning the changes to the company/business structure or ownership or the payment profile of its account.

5.3.4. In the event, the reporting institution's corporate customer is a public company which is subjected to regulatory disclosure, it would not be necessary for the reporting institution to identify or verify the identity of any shareholder.

5.4. Clubs, Societies and Charities

5.4.1. In conducting customer due diligence on a club, society or charity, the reporting institution should require the club, society or charity to furnish the relevant constituent documents (or other similar documents) including certificate of registration and the

¹ Shareholders with majority or more than 25 percent controlling interest, which ever is applicable.

identification of the office bearer and authorisation for any person to represent the club, society or charity.

5.5. Legal Arrangements

- 5.5.1. Legal arrangements can be used to avoid customer due diligence on the beneficiary of such transaction and disguise the source of funds involved. The reporting institution needs to establish whether the customer is acting on behalf of another person as a party to a legal arrangement, for example, a trustee or nominee.
- 5.5.2. The reporting institution should take reasonable measures to understand the relationship among the relevant parties in handling a trustee or nominee business and obtain satisfactory evidence of its legal status, the identity of the said trustee, settlor or nominee, authorised signatories, beneficiaries and the nature of their capacity and duties as trustee or nominee.
- 5.5.3. It shall be reasonable for the reporting institution to rely on the trustee or nominee to verify or confirm the identity of the beneficial owners. For this purpose, the reporting institution should require a written undertaking from the trustee or nominee that identification documents of the beneficiaries have been obtained, recorded and retained. In addition, such documentation needs to be made available promptly to the reporting institution upon request.

5.6. Beneficial Ownership and Control

- 5.6.1. The reporting institution should conduct customer due diligence on any natural person who ultimately owns or controls the customer's transaction if it suspects a transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such transaction.
- 5.6.2. The customer due diligence conducted should be as stringent as that for individual customer. In the event, the beneficial owner is identified as a foreign politically exposed person (PEP) based on the reporting institution's risk management framework, the requirement under paragraph 5.9 would apply.

5.7. Reliance on intermediaries² for CDD

- 5.7.1. The reporting institution who uses the services of intermediaries to introduce business may rely on the customer due diligence conducted by such intermediaries. However, the ultimate

² Where there is contract to outsource CDD, the requirement does not apply because the outsource or agent is regarded as synonymous with the reporting institution, i.e., the processes and documentation are those of the reporting institution itself. Where relevant, the guidelines or circulars on outsourcing issued by Bank Negara Malaysia would apply.

responsibility of customer due diligence remains with the reporting institution.

- 5.7.2. In facilitating effective oversight, the relationship between the reporting institution and its intermediaries should be governed by an arrangement/agreement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, the reporting institution must be satisfied that the intermediary:
- has an adequate customer due diligence process;
 - has a reliable mechanism to verify customer identity;
 - can provide the customer due diligence information and make copies of the relevant documentation available immediately upon request; and
 - where appropriate, is properly regulated and supervised by the respective authorities.
- 5.7.3. In addition, customer due diligence procedures should be performed, either on the reporting institution's own records or via copy of records obtained from the introducing entity.

5.8. Non-face-to-face Business Relationship

- 5.8.1. The reporting institution should pay special attention in establishing and conducting business relationship via information communication technology, for example, the internet, post, fax or telephone. Any business relationship/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 economic system.
- 5.8.2. The reporting institution should only establish business relationship upon completion of the customer due diligence process conducted through face-to-face interaction.
- 5.8.3. The reporting institution is also required to establish appropriate measures for customer verification that should be as stringent as that for face-to-face customers and implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

5.9. Foreign Politically Exposed Persons (PEPs)

- 5.9.1. PEPs are foreign individuals being, or who have been, entrusted with prominent public functions, such as heads of state or government, senior politicians, senior government officials, judicial or military officials and senior executives of public organisations.
- 5.9.2. The concern placed in dealing with PEPs lies with the possibility of such PEPs abusing their public powers for their own illicit

enrichment, especially in countries where corruption is widespread.

- 5.9.3. Hence, the reporting institution should have, in addition to their respective customer due diligence process, a risk management framework to determine whether current or new customers are PEPs. In establishing whether or not the customer is a PEP, the reporting institution should at least gather sufficient and appropriate information from the customer and through publicly available information.
- 5.9.4. Once a PEP is identified, the reporting institution should take reasonable and appropriate measures to establish the source of wealth and funds of such person.
- 5.9.5. The decision to enter into or continue business relationships with PEPs should be made by the Senior Management³ of the reporting institution at the head office.
- 5.9.6. In addition, the reporting institution should conduct enhanced on-going due diligence on PEPs throughout its business relationships with such PEPs. For such purpose, the reporting institution should note that business relationships with family members or close associates of PEPs involve similar reputational risks to those with PEPs themselves.

5.10. Higher risk customers

- 5.10.1. For higher risk customers, the reporting institution shall conduct enhanced customer due diligence.
- 5.10.2. Enhanced due diligence should include at least:
 - Obtaining more detailed information from the customer and through publicly available information, in particular, on the purpose of transaction and source of funds; and
 - Obtaining approval from the Senior Management of the reporting institution before establishing the business relationship with the customer.
- 5.10.3. Examples of higher risk customers are:
 - High net worth individuals;
 - Non-resident customers;
 - From locations known for their high rates of crime (e.g., drug producing, trafficking, smuggling);
 - Countries or jurisdictions with inadequate AML/CFT laws and regulations such as the Non-Cooperative Countries and Territories (NCCT);

³ Senior Management refers to any person(s) responsible for the management and administration of the reporting institution.

- PEPs;
- Legal arrangements that are complex – (e.g., trust, nominee);
- Cash based businesses; and
- Unregulated industries.

5.11. Existing customers

- 5.11.1. The reporting institution should take the necessary measures to ensure that the record of existing customers, including its customer's profile remains updated and relevant. In addition, further evidence in identifying the existing customers should be obtained to ensure compliance with the reporting institution's current customer due diligence standards.
- 5.11.2. The reporting institution should conduct regular reviews on existing records of customers, especially when:
- a significant transaction is to take place;
 - there is a material change in the way the account is operated;
 - the customer's documentation standards change substantially; or
 - it discovers that the information held on the customer is insufficient.
- 5.11.3. In circumstances other than those mentioned in paragraph 5.11.2, the reporting institution, based on risk assessment, may require additional information consistent with the reporting institution's current customer due diligence standards from those existing customers that are considered to be of higher risk.

6. RECORD KEEPING

6.1. Retention Period

- 6.1.1. The reporting institution should keep all records and documents of transactions, in particular, those obtained during customer due diligence procedures, for at least six years after the transaction has been completed or after the business relations with the customer have ended.
- 6.1.2. 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 it is confirmed by the Financial Intelligence Unit in Bank Negara Malaysia, that such records are no longer needed.

6.2. Audit trail

- 6.2.1. The reporting institution must ensure that the retained documents and records are able to create an audit trail on individual

transactions that are traceable by Bank Negara Malaysia, the relevant supervisory and law enforcement agencies.

6.2.2. In addition, the records kept must enable the reporting institution to establish the history, circumstances and reconstruction of each transaction. The records shall include at least:

- the identity of the customer;
- the identity of the beneficiary;
- the type of transaction (e.g., deposit or withdrawal);
- the form of transaction (e.g., by cash or by cheque);
- the instruction and the origin and destination of fund transfers; and
- the amount and type of currency.

6.3. Format

6.3.1. The reporting institution should retain the relevant document in the form that is acceptable under section 3 of the Evidence Act 1950, secure and retrievable, upon request, in a timely manner.

7. ON-GOING MONITORING

7.1. General

7.1.1. The reporting institution shall conduct on-going customer due diligence to examine and clarify the economic background and purpose of any transaction or business relationship that appears unusual, does not have any apparent economic purpose or the legality of such transaction is not clear especially with regards to complex and large transactions or higher risk customers. All findings must be documented and made available to Bank Negara Malaysia and the relevant supervisory authority upon request.

7.1.2. An effective customer due diligence process would enable the reporting institution to detect related money laundering and financing of terrorism transactions at the point of customer contact (based on the front-line staff's *ad hoc* report). Generally, most detection would be made through analysing the transaction patterns or activities of the customer.

7.2. Management Information System

7.2.1. The reporting institution should have in place an adequate management information system to complement its customer due diligence. The management information system should provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect any suspicious activity. Such information would include multiple transactions over a certain period, large transactions, anomaly in transactions pattern and transactions exceeding any internally specified threshold.

- 7.2.2. The management information system should be part of the reporting institution's information system that contains its customer's normal transaction/business profile, which is accurate and updated.

7.3. Special Attention

- 7.3.1. The reporting institution should establish internal criteria ("red flags") to detect suspicious transactions and may be guided by examples of suspicious transactions provided by Bank Negara Malaysia or sourced from other corresponding competent authorities as well as international organisations, for example, Bank for International Settlements (BIS), International Association of Insurance Supervisors (IAIS) or International Organisation of Securities Commission (IOSCO). The reporting institution should be prompted to conduct enhanced due diligence if any transaction matched the "red flags" list. Transactions that matched the "red flags" should be subjected to on-going monitoring.
- 7.3.2. The reporting institution should also conduct on-going due diligence or monitoring of transactions with regards to business relationships and transactions with individuals, businesses, companies and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT measures, such as the Non Cooperative Countries and Territories (NCCT) published on the FATF website (http://www.fatf-gafi.org/NCCT_en.htm). Such business relationships and transactions would require the reporting institution to make further enquiries, as detail as possible, about their background and purpose and to document the findings in writing. These findings should be made available to the Financial Intelligence Unit in Bank Negara Malaysia and the relevant supervisory authority.

8. SUSPICIOUS TRANSACTION REPORTING

8.1. General

- 8.1.1. The reporting institution is required to promptly submit a suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia when any of its employees suspect or have reason to suspect that the transaction or attempted transaction involves proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism.
- 8.1.2. For this purpose, the reporting institution must establish a reporting system for the submission of suspicious transaction reports to the Financial Intelligence Unit in Bank Negara Malaysia.

8.2. Reporting mechanisms

- 8.2.1. The reporting institution should appoint one officer (or more) at the Senior Management level to be the compliance officer responsible for the submission of suspicious transaction reports to the Financial Intelligence Unit in Bank Negara Malaysia. The appointed compliance officer is the single point of reference for the Financial Intelligence Unit in Bank Negara Malaysia with regards to AML/CFT matters.
- 8.2.2. In addition, the reporting institution should appoint at each branch and subsidiary carrying out any of the businesses or activities listed in the First Schedule to the AMLA, a branch/subsidiary compliance officer. The branch/subsidiary compliance officer is responsible, amongst others, 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.
- 8.2.3. Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the compliance officer should evaluate the grounds for suspicion and if suspicion is confirmed, promptly submits the suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia. In the case where the compliance officer decides that there are no reasonable grounds for suspicion, he should document his decision, ensure it is supported by the relevant documents and file the report.
- 8.2.4. The compliance officer should submit to the Financial Intelligence Unit in Bank Negara Malaysia the suspicious transaction report in the specified suspicious transaction report form through any of the following modes:
- Mail : Director
Financial Intelligence Unit
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
- 8.2.5. Where applicable and upon the advice of the Financial Intelligence Unit in Bank Negara Malaysia, the compliance officer of a reporting institution should submit its suspicious transaction reports on-line:
- Website : <https://bnmapp.bnm.gov.my/fins2/>

- 8.2.6. The compliance officer should ensure that the suspicious transaction report is submitted within the next working day, from the date the compliance officer establishes the suspicion. 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. Hence, the compliance officer must be given the independence to report suspicious transactions to the Financial Intelligence Unit in Bank Negara Malaysia without the need to go through any elaborate approval process.
- 8.2.7. The reporting institution should ensure that its compliance officer is authorised to cooperate with the Financial Intelligence Unit in Bank Negara Malaysia in providing such additional information and documentation as it may request and to respond promptly to any further enquiries with regards to any suspicious transaction report.
- 8.2.8. The reporting institution should ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy. Except for the purposes permitted in section 79 of the AMLA, the disclosure of any information or matter which has been obtained by any person within the reporting institution, in the performance of his duties or the exercise of his functions is an offence under the AMLA.

8.3. Triggers for submission of suspicious transaction report

- 8.3.1. The reporting institution should consider submitting a suspicious transaction report when it is unable to complete the customer due diligence process on any new or existing customer that is unreasonably evasive or uncooperative. The reporting institution should base such decision on normal commercial criteria and its internal policy.
- 8.3.2. The reporting institution should also 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".

8.4. Other issues

- 8.4.1. The reporting institution must ensure that the compliance officer maintains a complete file on all internally generated suspicious transaction reports and any supporting documentary evidence regardless that such reports have been submitted to the Financial Intelligence Unit in Bank Negara Malaysia.
- 8.4.2. The reporting institutions must undertake reasonable measures to ensure that all its employees involved in conducting or facilitating

the customer's transaction are aware of these reporting procedures and that failure to report suspicious transaction when they have reasonable grounds to believe that the transaction is "suspicious" is an offence under the AMLA.

9. COMBATING THE FINANCING OF TERRORISM

- 9.1. The reporting institution should ensure that the existing suspicious transaction reporting system and mechanism for the identification of suspicious transactions are extended to cover financing of terrorism.
- 9.2. The United Nations Security Council (UNSC) has passed various resolutions pursuant to UNSC Resolution 1267 (1999) to require sanctions against individuals and entities belonging or related to the Taliban, Usama bin Laden and the Al-Qaida organisation and maintains a list of individuals and entities (the Consolidated List) for this purpose. The updated and consolidated UN List can be obtained at <http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm>.
- 9.3. In ensuring efficient detection of suspected financing of terrorism, the reporting institution should maintain a database of names and particulars of terrorist in the UN Consolidated List and such orders as may be issued under sections 66B and 66C of the AMLA by the Minister of Internal Security. In addition, the reporting institution should consolidate its database with the other recognised lists of designated persons/entities.
- 9.4. The reporting institution should ensure that the information contained in the database are updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary for the purpose of identifying suspicious transactions.
- 9.5. The reporting institution should conduct regular checks on the names of new and existing customers against the names in the database. If there is any name match, the reporting institution should take reasonable and appropriate measures to verify and confirm the identity of its customer. If the customer's name fully matched any name in the database, the reporting institution should immediately:
 - a) inform the Financial Intelligence Unit in Bank Negara Malaysia, Securities Commission or Labuan Offshore Financial Services Authority, as the case may be;
 - b) reject the customer, if the transaction has not commenced; and
 - c) freeze the customer's transaction, if it is an on-going customer.Where the reporting institution suspects that a transaction is terrorist-related, it should make a suspicious transaction report to the Financial Intelligence Unit in Bank Negara Malaysia.

10. AML/CFT COMPLIANCE PROGRAMME

10.1. Policies, Procedures and Controls

- 10.1.1. The reporting institution's Board of Directors⁴ and Senior Management should be aware of the money laundering and financing of terrorism risks associated with all its business products and services and 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. It is the duty of the Board of Directors to maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institution and the duty of the Senior Management to ensure that the Board of Directors is updated with timely information.
- 10.1.2. The Board of Directors should be fully committed in establishing an effective internal control system for AML/CFT. It is the responsibility of the Senior Management to ensure such internal controls are in place and implemented effectively, including the mechanism to monitor and detect complex and unusual transactions.
- 10.1.3. The Board of Directors should ensure that the reporting institution has, at the minimum, policies on AML/CFT procedures and controls. For this purpose, the Senior Management will assist the Board of Directors in formulating the policies and ensure that the policies are in line with the risks associated, nature of business, complexity and the volume of the transactions undertaken by the reporting institution.
- 10.1.4. The Board of Directors should set minimum standards and approve the policies regarding AML/CFT measures within the reporting institution, including those required for customer acceptance policy, customer due diligence, record-keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism. The Senior Management in relation to this must ensure that such procedures are formulated and effectively implemented. For this purpose, the Board of Directors should assess the implementation of the approved AML/CFT policies through regular updates by the Senior Management and audits.
- 10.1.5. To ensure effective implementation, the Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT measures and ensuring that there is a separation of duty between those implementing the policies and procedures and

⁴ Board of Directors also includes references to Partners and Sole-proprietors.

those enforcing the controls. In line with this, the Board of Directors should ensure the:

- compliance officer at Head Office and at each branch or subsidiary is appointed; and
- effectiveness of internal audit in assessing and evaluating the controls to prevent money laundering and the financing of terrorism.

10.1.6. The Board of Directors should review and assess the AML/CFT policies and procedures in line with changes and developments in the reporting institution's products and services, technology as well as trends in money laundering and the financing of terrorism. The Senior Management is responsible to implement the necessary changes to the AML/CFT policies and procedures with the approval of the Board of Directors in ensuring that the current policies are sound and appropriate.

10.1.7. The Board of Directors and the Senior Management should ensure that there is adequate AML/CFT training provided for its employees, including promoting employees' awareness of their AML/CFT obligations.

10.2. Staff Integrity

10.2.1. The Senior Management must ensure the integrity of the reporting institution's employees at all times by establishing an appropriate employee assessment system (commensurate with the size of operations and risk exposure of the reporting institution to money laundering and financing of terrorism), that is approved by the Board of Directors to adequately screen its employees.

10.2.2. The employee assessment system should include evaluation of an employee's personal information, including criminal records, employment and financial history as part of the recruitment process.

10.3. Compliance Officer

10.3.1. The Senior Management is responsible to appoint the compliance officer at Senior Management level who is "fit and proper" to carry out his AML/CFT responsibilities and can effectively discharge it. In general, the compliance officer acts as the reference point for the AML/CFT matters, including employees training and reporting of suspicious transactions.

10.3.2. The reporting institution should inform, in writing, the Financial Intelligence Unit in Bank Negara Malaysia on the appointment or change in the appointment of the compliance officer, including such details as his name, designation, office address, office

telephone number, fax number, e-mail address and such information as may be required by Bank Negara Malaysia.

10.3.3. The reporting institution should ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The compliance officer should ensure the following:

- the reporting institution's compliance with the AML/CFT requirements;
- implementation of the AML/CFT policies;
- the appropriate AML/CFT procedures, including customer acceptance policy, customer due diligence, record-keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in money laundering and financing of terrorism trends;
- the channel of communication from the respective employees to the branch/subsidiary compliance officer and subsequently to the compliance officer is secured and that information is kept confidential;
- all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;
- internal generated suspicious transaction reports by the branch/subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence Unit in Bank Negara Malaysia; and
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

10.3.4. It is important and imperative that the compliance officer appointed by the reporting institution has the necessary knowledge, expertise and required authority to effectively discharge his responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations, the latest developments in money laundering and financing of terrorism techniques, the AML/CFT measures undertaken by the industry and timely access to customer due diligence documentation and other relevant information.

10.4. Staff Training and Awareness Programmes

10.4.1. The reporting institution must conduct awareness and training programmes on AML/CFT practices and measures for its employees, in particular, 'front-line' staff and officers in-charge-of

processing and accepting new customers as well as staff responsible to monitor transactions.

10.4.2. The Senior Management must ensure that proper channel of communication is in place to effectively communicate to all levels of employees the AML/CFT policies and procedures. The employees should be made aware that they may be held personally liable for any failure to observe the internal AML/CFT requirements.

10.4.3. In this regard, the reporting institution should make available its AML/CFT measures for all employees and its documented AML/CFT measures should at least contain the following:

- The relevant guidelines on AML/CFT issued by Bank Negara Malaysia; and
- The reporting institution's internal AML/CFT policies and procedures.

10.4.4. The training conducted for employees should be appropriate to their level of responsibilities in detecting money laundering and financing of terrorism activities and the risks of money laundering and financing of terrorism faced by the reporting institution. The reporting institution should at least adapt its training needs to the following levels of employees:

- *New Employees*
Provide a general background on money laundering and financing of terrorism, the requirement and obligation to monitor and report suspicious transactions to the compliance officer and the importance of the "Know Your Customer" policy.
- *"Front-Line" Employees*
Employees who deal directly with the customers are the first point of contact with potential money launderers and financiers of terrorism. Hence, they must be trained to conduct effective on-going customer due diligence, detect suspicious transactions and the measures that need to be taken upon determining a transaction as suspicious. Training should also be provided on factors that may give rise to suspicion, such as dealing with non-regular customers transacting in large cash, PEPs, higher risk customers and the circumstances where enhanced customer due diligence is required.
- *Employees – Establishing Business Relationship*
Employees, who are responsible for acceptance of new customers, must receive the equivalent training given to "front-line" employees. The training should be focused on

customer identification, verification and customer due diligence procedures, including when to conduct enhanced due diligence, including circumstances where there is a need to defer establishing business relationship with new customers until customer due diligence is completed satisfactorily. These employees should also be aware of the requirements and obligations to report suspicious transaction to the Financial Intelligence Unit in Bank Negara Malaysia.

- *Supervisors and Managers*
Include a higher level of instructions covering all aspects of AML/CFT procedures, in particular, the risk-based approach to customer acceptance, customer due diligence and risk profiling of customers. The other areas include the penalties for non-compliance to the AML/CFT requirements, procedures in addressing the financing of terrorism issues such as the Consolidated List, list of terrorists under the AMLA, internal suspicious transaction reporting procedures and the requirements for customer due diligence and record-keeping.

10.4.5. These training and awareness programmes should be conducted regularly and supplemented with refresher courses for employees, with special emphasis for those employees who are exposed to higher risk of potential money laundering and financing of terrorism activities, for example, the 'front-line' employees. These programmes should update staff on the latest AML/CFT developments such as products or transaction modes, which are susceptible to the risk of money laundering and financing of terrorism and remind them of their responsibilities under the AML/CFT programme.

10.5. Independent Audit

10.5.1. The Board of Directors is responsible to ensure regular independent audit of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLA, the AMLA Regulations and the relevant guidelines on AML/CFT issued by Bank Negara Malaysia as well as the requirements of the relevant laws and regulations of other supervisory authority, if any.

10.5.2. The Board of Directors should ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor should at least include:

- checking and testing the compliance with, and effectiveness of, the AML/CFT policies, procedures and controls; and
- assessing whether current measures are in line with the latest developments and changes of the relevant AML/CFT requirements.

- 10.5.3. The auditor must submit a written report on the audit findings to the Board of Directors, which should be used to highlight inadequacies of any internal AML/CFT measures and controls and the Board of Directors should ensure that necessary steps are taken to rectify the inadequacies, if any.
- 10.5.4. The reporting institution should ensure that such audit findings and reports are submitted to the Financial Intelligence Unit in Bank Negara Malaysia within two weeks of their submission to its Board of Directors.

11. NON-COMPLIANCE WITH PROVISIONS UNDER THE AMLA

- 11.1. Section 86 of the AMLA provides that any person who contravenes any provision of the AMLA, or regulations made under the AMLA, or any specification or requirement made, or any order in writing, direction, instruction, or notice given, or any limit, term, condition or restriction imposed, in the exercise of any power conferred under or pursuant to any provision of the AMLA commits an offence and shall, on conviction, if no penalty is expressly provided for the offence under the AMLA or the regulations, be liable to a fine not exceeding RM250,000.
- 11.2. Section 22 of the AMLA requires that an officer of a reporting institution takes all reasonable steps to ensure its compliance with the reporting obligation under Part IV of the AMLA. Failure of a reporting institution to comply with any of the requirements will result in Bank Negara Malaysia taking the appropriate enforcement action, including obtaining a Court order against any or all of the officers or employees of the reporting institution on terms that the Court deems necessary to enforce compliance.
- 11.3. Notwithstanding any Court order, the Financial Intelligence Unit in Bank Negara Malaysia may direct or enter into an agreement with the reporting institution to implement any action plan to ensure compliance with Part IV of the AMLA. Failure of an officer to take reasonable steps to ensure compliance with Part IV of the AMLA, or failure of a reporting institution to implement any action plan as agreed to ensure compliance, will result in the officer or officers being personally liable to a fine not exceeding RM100,000 or to imprisonment for a term not exceeding 6 months or to both.
- 11.4. In the case of a continuing offence, a further fine may be imposed on the reporting institution not exceeding RM1,000 for each day during which the offence continues after conviction. Section 92 of the AMLA further empowers Bank Negara Malaysia to compound, with the consent of the Public Prosecutor, any offence under the AMLA or its regulations by accepting from the person reasonably suspected of having committed the offence such amount not exceeding 50% of the amount of the maximum

fine for that offence, including the daily fine, if any, in the case of a continuing offence.

- 11.5. Section 66E(5) of the AMLA provides that any institution that fails or refuses to comply with or contravenes any direction or guidelines issued to it by the relevant regulatory or supervisory authority; or discloses a direction or guideline issued to it in contravention of section 66E(4), commits an offence and shall on conviction be liable to a fine not exceeding RM100,000.

Appendix I

GLOSSARY

“beneficial owner”	<p>Refers to any natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.</p> <ul style="list-style-type: none"> • For companies – the person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted includes the natural person with a controlling interest and the natural persons who comprise the mind and management of company.
“constituent document”	<p>In relation to an institution, means the statute, charter, memorandum of association and articles of association, rules and by-laws, partnership agreement, or other instrument, under, or by, which the institution is established and its governing and administrative structure and the scope of its functions and business are set out, whether contained in one or more documents;</p>
“intermediaries”	<p>Generally refers to third parties, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process;</p>
“person”	<p>Includes a body of persons, corporate or unincorporated;</p>
“property”	<p>Means:</p> <ul style="list-style-type: none"> (a) assets of every kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, however acquired; or (b) legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including bank credits, traveller’s cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit;
“reporting institution”	<p>Means any person, including branches and subsidiaries outside Malaysia of that person, who carries on any activity listed in the First Schedule to the AMLA.</p>
“terrorist property”	<p>Means:</p> <ul style="list-style-type: none"> (a) proceeds from the commission of a terrorist act; (b) property that has been, is being, or is likely to be used to commit a terrorist act; (c) property that has been, is being, or is likely to be used by a terrorist, terrorist entity or terrorist group;

	<p>(d) property owned or controlled by or on behalf of a terrorist, terrorist entity or terrorist group, including funds derived or generated from such property; or</p> <p>(e) property that has been collected for the purpose of providing support to a terrorist, terrorist entity or terrorist group or funding a terrorist act;</p>
“terrorist act”	<p>An act or threat of action within or beyond Malaysia that—</p> <p>(a) involves serious bodily injury to a person;</p> <p>(b) involves serious damage to property;</p> <p>(c) endangers a person’s life;</p> <p>(d) creates a serious risk to the health or the safety of the public or a section of the public;</p> <p>(e) involves the use of firearms, explosives or other lethal devices;</p> <p>(f) involves releasing into the environment or any part of the environment or distributing or exposing the public or any part of the public to—</p> <p>(i) any dangerous, hazardous, radioactive or harmful substance;</p> <p>(ii) any toxic chemical; or</p> <p>(iii) any microbial or other biological agent or toxin;</p> <p>(g) is designed or intended to disrupt or seriously interfere with, any computer system or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure;</p> <p>(h) is designed or intended to disrupt, or seriously interfere with, the provision of essential emergency services such as police, civil defence or medical services;</p> <p>(i) involves prejudice to national security or public safety; or</p> <p>(j) involves any combination of any of the acts specified in paragraphs (a) to (i),</p> <p>where the act or threat is intended or may reasonably be regarded as being intended to—</p> <p>(aa) intimidate the public or a section of the public; or</p> <p>(bb) influence or compel the Government of Malaysia or the Government of any State in Malaysia, any other government, or any international organization to do or refrain from doing any act,</p> <p>and includes any act or omission constituting an offence under the Aviation Offences Act 1984 [Act 307].</p>

