KNOW YOUR CUSTOMER
AND
ANTI-MONEY LAUNDERING/COUNTER FINANCING OF TERRORISM
POLICY GUIDELINES

PART A – INTRODUCTION

It is the policy of First East Export Bank (P.L.C) (the "Bank") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

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 globalization 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.

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

Besides bringing the recommendation up to date in addressing new and emerging threats, the 2012 revision of the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks, which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

AML/CFT – Banking Sector Guidelines is based on the principle that reporting institutions must conduct their business in conformity with high ethical standards and be on guard against undertaking any business transaction that is or may be connected with or may facilitate ML/TF. This is aim to ensure integrity and soundness of the Labuan International Business Financial Centre (LIBFC) and Malaysian financial system are safeguarded.

1.0 Anti-Money Laundering and Counter Financing of Terrorism Act

Malaysia, in fulfilling its international obligations and commitment to establish the FATF's 40 Recommendations, passed the Anti-Money Laundering and Anti-Terrorism Financing Act in year 2001 and subsequently the Anti-Money Laundering and Anti-Terrorism Financing (Amendment) Act 2014 (referred to as AMLATFA).

The amended AMLATFA, which came into force on 1 September 2014, criminalizes money laundering, imposes obligations for reporting and record-keeping on reporting institutions, introduced the mechanism for investigation and power for freezing, seizing and forfeiting proceeds of unlawful activities.

Bank Negara Malaysia (BNM), who was appointed as the competent authority under Section 7(1) of the AMLATFA, established the Financial Intelligence Unit to carry out its functions as the competent authority under the AMLATFA.

2.0 Money Laundering

Money laundering has become an increasing matter of concern in a number of jurisdictions particularly in many emerging financial services sectors, where criminals take advantage of the vulnerability of the financial systems to cipher their funds and distance the source of these funds from themselves.

This concern has extended to include terrorist financing following the terrorist attacks in the United States on 11 September 2001. Although not all terrorist activities are financed through illegal sources, the methods used to distance the funds from its origins are similar.

Money laundering and terrorist financing is therefore a worldwide phenomenon, where if left unchecked, will encourage criminal activities to continue and ultimately weaken the social fabric and collective ethical standards of society.

2.1 What is Money Laundering?

2.1.1 Money laundering is a process whereby funds, generated by illegal means such as drug trafficking, smuggling and corruption, are funnelled through legitimate financial transactions to conceal its illicit origins, making it appear legitimate.

2.1.2 **Section 3(1)** of the AMLATFA defines money laundering as the act of a person who –

(a) *engages, directly or indirectly, in* a *transaction that involves proceeds of any unlawful activity;*

(b) *acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Malaysia proceeds of any unlawful activity; or*

(c) *conceals, disguises* or *impedes the establishment of the true nature, origin, location, movement, disposition, title or, rights with respect to, or ownership* of, *proceeds of any unlawful activity; where –*

(i) as *may be inferred from objective factual circumstance, the person knows or has reason to believe, that the property is proceeds from any unlawful activity; or*

(ii) *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.*

2.1.3 Under **Section 4** of the AMLATFA

(1) Any person who –

(a) Engages in, or attempts to engage in; or

(b) *abets the commission of, money laundering commits an offence and shall on conviction be liable to a fine not exceeding five million ringgit or to imprisonment for a term not exceeding five years or to both*

(2) A person may be convicted of an offence under subsection (1) irrespective of whether there is a conviction in respect of a serious offence or foreign serious offence or that a prosecution has been initiated for the commission of a serious offence or foreign serious offence

2.2 How Is Money Laundered?

The money laundering process comprises of three main stages :-

- **Placement**
  Illegal profits are introduced into the financial system. This might be done by dividing large amounts of cash into less conspicuous smaller amounts that are deposited directly into a bank account or by purchasing a series of monetary instruments.

- **Layering**
  Funds, which have entered the financial system, are then distanced from their source through transactions such as purchase and sales of investment instruments or through multiple transfers of funds from different accounts around the world disguised as payments for goods or services. Such transactions are usually channelled through shell companies or companies with nominees' shareholders and/or directors.

- **Integration**
  Once the first two stages have been successful, the final stage is to integrate the illegal proceeds back into the economy as legitimate funds through legitimate transactions such as business ventures, luxury assets, lending and investing.

3.0 Financial Action Task Force On Money Laundering (FATF)

The G-7 Industrial group established the FATF as a global money-laundering watchdog in 1989, as a response to mounting concerns over money laundering. A framework, consisting 40 recommended measures, known as the "40 Recommendations", to be adopted and implement by governments around the world in combating money laundering, was established by the FATF.

Full details of the FATF's recommendations may be obtained by visiting www.fatf-gafi.org

PART B – AMLATFA COMPLIANCE FRAMEWORK

1.0 Key Elements Under the Legislation

(a) Internal controls, Policies and Accountabilities
(b) Know Your Customer
(c) Education and Training
(d) Monitoring and Detection
(e) Reporting Obligations and Procedures
(f) Record Keeping

Statutory provision :-

Section19 of the AMLATFA provides as follows –

(1) A reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls to guard against and detect an offence under this Act.

(2) The programmes in subsection (1) shall include -

(a) the establishment of procedures to ensure high standards of integrity of its employees and a system to evaluate the personal, employment and financial history of these employees;

(b) on–going employee training programmes, such as "know–your–customer" programmes, and instructing employees with regard to the responsibilities specified in sections 13, 14, 15, 16 and 17; and

(c) an independent audit function to check compliance with such programmes.

(3) A reporting institution shall implement compliance programmes under subsection (1) on its branches and subsidiaries in and outside Malaysia.

(4) A reporting institution shall also designate compliance officers at management level in each branch and subsidiary who will be in charge of the application of the internal programmes and procedures, including proper maintenance of records and reporting of suspicious transactions.

(5) A reporting institution shall develop audit functions to evaluate such policies, procedures and controls to test compliance with the measures taken by the reporting institution to comply with the provisions of this Act and the effectiveness of such measures.

2.0 Know Your Customer ("KYC")

Statutory provision :-

Section 16(2) of the AMLATFA provides as follows –

A reporting institution shall –

(a) Verify, by reliable means, the identity, representative capacity, domicile, legal capacity, occupation or business purpose of any person, as well as identifying information on that person, whether he be an occasional or usual client, through the use of documents such as identity card, passport, birth certificate, driver's licence and constituent document, or any other official or private document, when establishing or conducting business relations, particularly when opening new accounts or passbooks, entering into any fiduciary transaction, renting of a safe deposit box, or performing any cash transaction exceeding such amount as the competent authority may specify ;

(b) Include such details in a record.

2.1 Key Elements of KYC Policy

- ✓ Customer Acceptance
- ✓ Customer Due Diligence/Enhanced Customer Due Diligence
- ✓ On-Going Monitoring/Due Diligence
- ✓ Periodical Review of Risk Classification

2.2 Customer Acceptance

2.2.1 The Bank must ensure that it does not establish relationship with customers who are in anonymous or fictitious name(s); in the names of persons with a criminal background and/or having connections with terrorist organizations.

2.2.2 No financial sector business is immune from the activities of criminal elements. The level of money laundering risks that Bank is exposed to by a customer relationship depends on :-

- ☑ Type of the customer and nature of business.
- ☑ Type of product/service availed to the customer.
- ☑ Country where the customer is domiciled.

2.2.3 Based on the above criteria, the Bank is required to conduct risk profiling on its customers. A risk profile must consider the following factors :-

(a) Customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of PEP, types of occupation);

(b) Geographical location of business or country of origin of customers;

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

(d) Any other information suggesting that the customer is of higher risk.

2.2.3(1) Customers/Nature of Business

This can be classified into three risk levels as follows :-

(a) High Risk

Customers engaged in certain professions where money-laundering possibilities are high. The indicative list of high risk customers is furnished in Page 46-47.

(b) Medium Risk

The indicative list of medium risk customers is furnished in Page 48.

(c) Low Risk

All the customers who are not High/ Medium Risk customers are low risk customers. These are the type of customers whose identity and source of wealth can be easily identified and the transactions in whose accounts by and large conform to the known profile. The indicative list of medium risk customers is furnished in Page 49.

2.2.3(2) Products and Services

The products and services are also to be categorized in addition to existing system of categorizing the customers as high/ medium/ low risk as above. The indicative list of high/medium risk products and services is given in page 50 and 51.

2.2.3(3) Geographies

Customer should be subject to higher due diligence if the following criteria falls under "high risk" geographies :-

- ☑ Country of nationality (Individuals).
- ☑ Country of residential address (Individuals).
- ☑ Country of incorporation (Legal entities).
- ☑ Country of residence of principal shareholders / beneficial owners (Legal entities).
- ☑ Country of business registration such as branch/liaison/project office.
- ☑ Country of source of funds.
- ☑ Country of the business or correspondence address.
- ☑ Country with whom customer deals (e.g. over 50% of the business – trade, etc.).

2.3 Customer Due Diligence (CDD)/Enhanced Customer Due Diligence

(a) The first requirement of knowing the Bank's customer for anti-money laundering purposes is to be satisfied that a prospective customer is who he/she/company claims to be.

(b) The second requirement of knowing the customer is to ensure that sufficient information is obtain on the nature of the business that the customer expects to undertake or any expected, or predictable pattern of transaction.

(c) The Bank must be satisfied in identifying the customer and verifying his/her identity by using reliable, independent source documents, data or other form of information.

2.3.1 When CDD is Required

The Bank is required to conduct CDD on the customer and the person conducting the transaction, when : -

(a) Establishing business relations;

(b) Providing wire transfer services;

(c) It has any suspicion of ML/TF, regardless of any amount; or

(d) It has any doubt about the veracity or adequacy of previously obtained information.

2.3.2 What is Required

The CDD measures undertaken shall comprise, at least the following :-

(a) Identify the customer and verify the customer's identity using reliable, independent source documents, data or information;

(b) Verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person;

(c) Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the Bank is satisfied that it knows who the beneficial owner is; and

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

2.3.3 Timing of Verification

(a) The Bank is required to verify the identity of the customer and beneficial owner before, or during, the course of establishing a business relationship or conducting a transaction for an occasional customer.

(b) In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the Bank may complete verification after the establishment of the business relationship to allow some flexibility for its customer and beneficial owner to furnish the relevant documents.

(c) Where delayed verification applies, the following conditions must be satisfied :-

(i) This occurs as soon as reasonably practicable;

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

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

(iv) There are no suspicion of ML/TF risks.

(d) The term "reasonably practicable" under Section 2.0 Paragraph 2.3.3(c)(i) shall not be later than ten working days or any other period as may be specified by Labuan FSA.

(e) The measures that Bank may take to manage such risks of delayed verification should be limited to no more than 2 cases (only for low & medium risks) per month.

2.3.4 Specific CDD Measures

2.3.4(1) Individual Customer and Beneficial Owner

(a) In conducting CDD on an individual customer and beneficial owner, the Bank is required to obtain at least the following information :-

(i) Full name;

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

(iii) Residential and mailing address;

(iv) Date of birth;

(v) Nationality;

(vi) Occupation type;

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

(viii) Purpose of transaction;

(ix) Source of wealth (i.e if the income does not match with the occupation); and

(x) Contact number (home, office or mobile).

(b) The Bank can accept any other official documents bearing the photograph of the customer and beneficial owner under Section 2.0 Paragraph 2.3.4(1)(a)(ii) provided that the Bank is satisfied with the authenticity of the documents which contain the necessary required information.

(c) The Bank shall verify the documents referred to Section 2.0 Paragraph 2.3.4(1)(a)(ii) by requiring the customer or beneficial owner to furnish the original and make a copy of

the said document. However, where biometric identification method is used, verification is deemed to be satisfied.

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

2.3.4(2) Legal Persons

(a) For customers that are legal persons, the Bank is required to understand the nature of the customer's business, its ownership and control structure.

(b) The Bank is required to identify the customer and verify its identity through the following information :-

(i) 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;

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

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

(c) The Bank is required to identify and take reasonable measures to verify the identity of beneficial owners through the following information :-

(i) The identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person including but not limited to the following:-

- 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 Form 49 as prescribed by the Companies Commission of Malaysia or Form 13 and Form 25 as prescribed by the Registrar of Companies, Labuan FSA or foreign incorporation, or any other equivalent documents for other types of legal person are acceptable;

- Authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and

- 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 Bank.

(ii) To the extent that there is doubt under as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in Section 2.0 Paragraph 2.3.4(2)(c)(i) or where no natural person(s) exert control through ownership interests, the identity of the natural person (if any) exercising control of the legal person through other means; and

(iii) Where no natural person is identified under Section 2.0 Paragraph 2.3.4(2)(c)(i) or (ii) above, the identity of the relevant natural person who holds the position of senior management.

(d) Where there is any doubt as to the identity of persons referred to under Section 2.0 Paragraphs 2.3.4(2)(b) and 2.3.4(2)(c), the Bank shall :-

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

(ii) Verify the authenticity of the information provided by such person with the Labuan FSA, Companies

Commission of Malaysia or any other relevant agencies.

(e) The Bank is exempted from obtaining a copy of the Memorandum and Articles of Association or Certificate of Incorporation and exempted from identifying and verifying the directors and shareholders of the legal person which fall under the following categories :-

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

(ii) Foreign public listed companies :-

- listed in recognised exchanges; and
- not listed in higher risk countries;

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

(iv) Government-linked companies in Malaysia;

(v) State-owned corporations and companies in Malaysia;

(vi) An authorised person, an operator of a designated payment system, a registered person, as the case may be, under the Financial Services Act 2013 (FSA) and the Islamic Financial Services Act 2013 (IFSA);

(vii) Persons licensed or registered under the Capital Markets and Services Act 2007;

(viii) Licensed entities under the LFSSA and LIFSSA;

(ix) Prescribed institutions under the Development Financial Institutions Act 2002; or

(x) Foreign financial institutions that are not from higher risk countries.

(f) The Bank may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

2.3.4(3) Legal Arrangements

(a) For customers that are legal arrangements, the Bank must understand the nature of the customer's business, its ownership and control structure.

(b) The Bank is required to identify the customer and verify its identity through the following information :-

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

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

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

(c) The Bank is required to identify and take reasonable measures to verify the identity of beneficial owners through the following information :-

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

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

(d) The Bank may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.

(e) Where reliance is placed on third parties under Section 2.0 Paragraph 2.3.4(3)(d), the Bank is required to comply with Section 8.0 on Reliance on Third Parties.

2.3.4(4) Clubs, Societies and Charities

It Is the Bank's policy not to deal with these organizations.

2.3.4(5) Counter-party

(a) Where the Bank establishes a relationship with a counter-party, the reporting institution must be satisfied that the counter-party is properly regulated and supervised.

(b) The Bank is required to ensure that the counter-party's CDD process is adequate and the mechanism to identify and verify its customers is reliable.

2.3.4(6) Beneficiary account

(a) In the case of beneficiary accounts, the Bank is required to perform CDD on the beneficiary and the person acting on behalf of the beneficiary, on an individual basis.

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

(c) The Bank may rely on a third party when they are unable to conduct CDD on the clients or professionals, such as legal firms or accountants acting on behalf of their clients.

(d) Where reliance is placed on third party under Section 2.0 Paragraph 2.3.4(6)(c), Section 8.0 on Reliance on Third Parties must be complied with.

(e) In the event where the person acting on behalf of the beneficiary is unable or refuses to provide the information on the identity of the beneficiaries or written undertaking (where applicable), reporting institutions are to comply

with Section 12.0 on Failure to Satisfactorily Complete CDD.

2.3.5 Enhanced Customer Due Diligence (ECDD)

2.3.5(1) The Bank is required to perform ECDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include at least, the following :-

(a) Obtaining CDD information under Section 2.0 Paragraph 2.3.4;

(b) Obtaining additional information on the customer and beneficial owner (e.g. volume of assets; other information from public database);

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

(d) Obtaining approval from the Board before establishing (or continuing, for existing customer) such business relationship with the customer and in the case of PEPs.

2.3.5(2) In addition to Section 2.0 Paragraph 2.3.5(1), the Bank may also consider the following ECDD measures in line with the ML/TF risks identified :-

(a) Obtaining additional information on the intended level and nature of the business relationship;

(b) Updating more regularly the identification data of customer and beneficial owner;

(c) Inquiring on the reasons for intended or performed transactions; and

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

2.4 On-Going Monitoring/Due Diligence

2.4.1 The Bank is required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include :-

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

(b) Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

2.4.2 In conducting on-going due diligence, the Bank may take into consideration the economic background and purpose of any transaction or business relationship which :-

(a) Appears unusual;

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

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

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

2.4.3 The frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

2.4.4 The Bank is required to increase the number and timing of controls applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

2.5 Periodical Review of Risk Categorization of Customers

The Bank shall ensure maintaining and updating of customer risk profile on a continuous basis. A review of risk categorization of customers should be carried out at a periodicity of not less than once in six months.

3.0 Politically Exposed Persons (PEPs)

3.1 General

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

3.2 Foreign PEPs

3.2.1 Checks on PEPs must be done via World-Check to determine whether a customer or a beneficial owner is a foreign PEP.

3.2.2 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of ECDD as set out under Section 2.0 Paragraph 2.3.5 must be conducted.

3.3 Domestic PEPs or Person Entrusted With A Prominent Function By An International Organization.

3.3.1 Reasonable measure must be taken to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.

3.3.2 If the customer or beneficial owner is assessed as a domestic PEP or a person entrusted with a prominent function by an international organisation, the Bank must 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.

3.3.3 The assessment of the ML/TF risks, as specified under Section 3.0 Paragraph 3.3.2, shall take into accounts the profile of the customer under Section 2.0 Paragraph 3.1.3 on risk profiling.

3.3.4 The requirements of ECDD as set out under Section 2.0 Paragraph 2.3.5 must be conducted in respect of domestic PEPs or person entrusted with a prominent function by an international organisation which are assessed as higher risk.

3.3.5 CDD measures similar to other customer for domestic PEPs or person entrusted with a prominent function by an international organisation if may be applied if the Bank is satisfied that the domestic PEPs or person entrusted with a prominent function by an international organisation are not assessed as higher risk.

4.0 New Products and Business Practices

4.1 The Bank must 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.

4.2 The Bank is required to :-

(i) Undertake the risks assessment prior to the launch or use of such products, practices and technologies; and

(ii) Take appropriate measures to manage and mitigate the risks.

4.3 The risks assessment and the appropriate measures to be taken to mitigate the risks identified as specified under Section 4.0 paragraph 4.2 must be documented separately for each product.

4.4 All new products, practices and technologies together with its risk assessment must be approved by the Board.

4.5 Endorsement from Labuan FSA is required for any new products to be launched by the Bank.

5.0 Higher Risk Countries

5.1 ECDD must be conducted for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having on-going or substantial ML/TF risks.

5.2 Where ML/TF risks are assessed as higher risk, the Bank must conduct ECDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

5.3 In addition to the ECDD requirement under Section 5.0 Paragraph 5.1, the Bank must apply the following counter measures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks :-

(i) Limiting business relationship or financial transactions with identified countries or persons located in the country concerned;

(ii) Review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;

(iii) Conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the Bank, located in the country concerned;

(iv) Submit a report with a summary exposure to customers and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia as the Competent Authority and also to Supervision and Enforcement Department, Labuan FSA on an annual basis; and

(v) Conduct any other measures as specified by Labuan FSA.

6.0 Non Face-to-Face Business Relationship

6.1 The Bank may establish non face-to-face business relationships with its customers.

6.2 The Bank may obtain an attestation from the third party to satisfy itself that the requirements in Section 8.0 have been met.

6.3 The Bank must be vigilant in establishing and conducting business relationships via information communication technology.

6.4 The following measures should be followed to verify the identity of non face-to-face customer :-

(i) Requesting additional documents to complement those which are required for face-to-face customer;

(ii) Developing independent contact with the customer; or

(iii) Verifying customer information against any database maintained by the authorities.

7.0 Correspondent Banking

7.1 The Bank must take the necessary measures to ensure that it is not exposed to the threat of ML/TF through the accounts of the respondent banks such as being used by shell banks.

7.2 In relation to cross-border correspondent banking and other similar relationships, the Bank is to ensure :-

(i) Gather sufficient information about a respondent bank to understand fully the nature of the respondent's bank's business, and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

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

(iii) Obtain approval from the Board prior to establishing new correspondent banking relationships; and

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

7.3 In relation to "payable-through accounts", the Bank must satisfy itself that the respondent bank :-

(i) Has performed CDD obligations on its customers that have direct access to the accounts of the reporting institution; and

(ii) Is able to provide relevant CDD information to the Bank upon request.

7.4 The Bank shall not enter into, or continue, correspondent banking relationships with shell banks. The Bank must satisfy itself that respondent banks do not permit their accounts to be used by shell banks.

7.5 Special attention must be made for correspondent banking relationship with respondent banks from countries highlighted by the FATF or Government of Malaysia as insufficiently implementing the internationally accepted AML/CFT measures.

7.6 Extreme caution must be exercised while establishing/continuing relationships with banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing.

7.7 It must be ensured that the Bank’s respondent banks have anti-money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

8.0 Reliance on Third Parties

8.1 Customer Due Diligence

8.1.1 The Bank may rely on third parties to conduct CDD or to introduce business.

8.1.2 The ultimate responsibility and accountability of CDD measures shall remain with the Bank relying on the third parties.

8.1.3 The Bank is prohibited from relying on third parties located in the higher risk countries that have been identified as having on-going or substantial ML/TF risks.

8.1.4 The relationship between the Bank and their third parties relied upon by the Bank to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, reporting institutions must be satisfied that the third party :-

(i) Can obtain immediately the necessary information concerning CDD as required under Section 2.0;

(ii) Has an adequate CDD process;

(iii) Has measures in place for record keeping requirements;

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

(v) Is properly regulated and supervised by the respective authorities.

8.1.5 Attestation from the third party to satisfy themselves that the requirements in Section 8.0 Paragraph 8.1.4 have been met.

8.1.6 Written confirmation may be obtained from the third party that they have conducted CDD on the customer or beneficial owner as the case may be, in accordance with Section 2.0 Paragraph 2.4.

8.1.7 The requirements under Section 8.0 Paragraphs 8.1.1 and 8.1.4 may be fulfilled if the Bank relies on a third party that is part of the same financial group subject to the following conditions :-

(i) The group applies CDD and record keeping requirements and AML/CFT programmes in line with the requirements in this document;

(ii) The implementation of those CDD and record keeping requirements and AML/CFT programmes are supervised at a group level by a competent authority; and

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

8.1.8 The Bank is prohibited from relying on a third party located in the countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

8.2 On-going Due Diligence

The Bank must not rely on third parties to conduct on-going due diligence of its customers.

9.0 Private Banking

9.1 The Bank is required to conduct ECDD where the ML/TF risks of private banking customers are assessed as higher risk.

10.0 Shell Banks

10.1 The Bank shall not establish or have any business relationship with shell banks.

11.0 Wire Transfers

It is not the policy of the Bank to transact any wire transfers on behalf of its clients or 3rd parties.

12.0 Failure to Satisfactorily Complete CDD

12.1 The Bank shall not commence business relations or perform any transaction in relation to a potential customer or shall terminate business relations in the case of an existing customer, if the Bank is unable to comply with the CDD requirements.

12.2 In the event of failure to comply with the CDD requirements, the Bank must consider lodging a suspicious transaction report. Please refer to Section 16.0 Paragraph 16.2.

13.0 Management Information System

13.1 The Bank has put in place a management information system (MIS), to complement its CDD process. The MIS is to provide the Bank with timely information on a regular basis to enable the reporting institution to detect irregularity and/or any suspicious activity.

13.2 For the time being, the MIS is done manually in an Excel spreadsheet.

14.0 Accountabilities

Statutory provision :-

Section 19(4) *of the AMLATFA provides as follows –*

A reporting institution shall also designate compliance officers at management level in each branch and subsidiary who will be in charge of the application of the internal programmes and procedures, including proper maintenance of records and reporting of suspicious transactions.

14.1 Designated Compliance Officer

The Bank shall designate a senior officer/senior management staff as the Designated Compliance Officer ("DCO") for AML/CFT, with explicit responsibilities and established lines of communication with both the management and LFSA, to oversee the AML measures taken.

14.1.1 Duties of the DCO:-

(a) Coordinates planning and implementation of the Bank's compliance program;

(b) Develops, initiates, maintains, and revises policies and procedures for the general operation of the Compliance Program and its related activities to prevent illegal, unethical, or improper conduct;

(c) Ensure the compliance program consists:

- A code of ethics and professional conduct for employees.
- Procedures to ensure completeness of records and exception reporting.
- Procedures for suitability checks, including Know Your Customer (KYC) and know your employee form.
- Procedures for handling complaints, including documentation and follow-up.
- Provision for addressing conflicts of interest.

- Provisions to anticipate and prevent fraud and money laundering.

(d) Collaborates with other departments (e.g., Risk Management, Internal Audit, Operations, etc.) to direct compliance issues to appropriate existing channels for investigation and resolution;

(e) Show and awareness and understanding of ethical and moral principle consistent with the missing and values of the Bank;

(f) Acts as an independent review and evaluation body to ensure that compliance Issues/concerns within the organization are being appropriately evaluated, investigated and resolved;

(g) Identifies potential areas of compliance vulnerability and risk; develops/implements corrective action plans for resolution of problematic issues, and provides general guidance on how to avoid or deal with similar situations in the future;

(h) Monitors, and as necessary, coordinates compliance activities of other departments to remain abreast of the status of all compliance activities and to identify trends.

(i) Maintain a working knowledge of relevant issues, laws and regulations through periodicals, seminars, training programs and peer contact.

(j) Response appropriately if a violation is uncovered, including a direct report to the Board of Directors, Senior Management or external agency if deemed necessary.

14.1.2 The DCO needs to ensure and to check any updates or latest information or announcement on Labuan FSA website specifically on AML Compliance at least once daily during business hours. The person is also responsible to take necessary action (if any) upon acknowledges the information within reasonable time.

14.2 Compliance Management Arrangements

14.2.1 The DCO acts as the reference point for AML/CFT matters within the Bank.

14.2.2 The DCO must be able to effectively influence decisions relating to AML/CFT.

14.2.3 The DCO is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.

14.2.4 For the purposes of Section 14.0 Paragraph 14.2.3, "fit and proper" may include minimum criteria relating to :-

(i) Probity, personal integrity and reputation; and

(ii) Competency and capability.

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

14.2.6 The DCO is encouraged to pursue professional qualifications in AML/CFT so that he/she is able to carry out their obligations effectively.

14.3 Roles & Responsibilities of the Board of Directors

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

(b) Approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;

(c) Establish appropriate 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 the 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.

14.4 Roles & Responsibilities of Senior Management

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

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

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

(d) Undertake review and propose to the Board the necessary 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 programmes that are reflective of the size and complexity of the reporting institution's operations and risk profiles;

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

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

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

(j) Ensure that AML/CFT issues raised are addressed in a timely manner; and

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

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

15.0 Employee Screening Procedures

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

15.2 The Bank has established an employee assessment system which includes an evaluation of an employee's personal information, including criminal records and employment history:-.

(a) All staff is required to update their personal information when needed and submit to HR Department.

(b) All staff is required to submit a copy of their credit report from CTOS or similar reports from other agencies as directed by the Bank and submit to HR Department.

(c) All staff is required to signed the Confirmation & Declaration Form and submit to HR Department.

15.3 Adverse or unsatisfactory reports and findings without any supporting documents shall be reported to the Board. The Board shall decide the next course of action, if necessary.

16.0 Monitoring, Detection And Reporting Procedures

16.1 Monitoring and Detection

16.1.1 A suspicious transaction will often be one, which is inconsistent with a customer's known, legitimate business or activities.

16.1.2 All relevant staff must be aware :-

(i) That if they become suspicious of a particular customer or transaction they must report the matter to the DCO immediately;

(ii) Of the procedure for reporting;

(iii) That they do not have to be certain; only suspicious that the transaction(s) relate to criminal activity;

(iv) That if they have suspicions and fail to report them they may be committing a criminal offence and/or be liable to disciplinary action for gross misconduct;

(v) That they should not investigate the customer or the transaction(s), unless advised by the DCO to do so, nor should they inform the customer of their suspicion;

(vi) That, unless they are instructed otherwise, they should continue to deal with the customer in the normal way.

16.2 Suspicious Transaction Report

16.2.1 The Bank is required to promptly submit a suspicious transaction report ("STR") to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to Anti-Money Laundering Compliance Unit, Labuan FSA whenever the Bank suspects or have reason to suspect that the transaction (including attempted or proposed) regardless of the amount :-

(i) Appears unusual;
(ii) Has no clear economic purpose;
(iii) Appears illegal;
(iv) Involves proceeds from an unlawful activity; or
(v) Indicates that the customer is involved in ML/TF.

16.2.2 The Bank is to provide the required and relevant information that gives rise to the suspicion in the STR form, which includes but not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

16.2.3 A reporting system is to be maintained for the submission of STRs.

16.2.4 Examples of transactions that may constitute triggers for the purposes of reporting suspicious transactions can be referred to in Page 50- 53.

16.3 Reporting Mechanisms

16.3.1 The DCO is responsible for channelling all internal STR received from the employees.

16.3.2 The Bank is required to have in place policies on the duration upon which internally generated STRs must be reviewed by the DCO, including the circumstances when the timeframe can be exceeded, where necessary.

16.3.3 Upon receiving any internal STR from staff, the DCO must evaluate the grounds for suspicion. Once the suspicion is confirmed, the DCO must promptly submit the STR. In the case where the DCO decides that there are no reasonable grounds for suspicion, the DCO must document and file the decision, supported by the relevant documents.

16.3.4 The DCO must submit the STR in the specified suspicious transaction report form through the following modes :-

Mail : Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)
Fax : +603-2693 3625
E-mail : str@bnm.gov.my

AND

Mail : Director
Supervision and Enforcement Dept
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Labuan F.T.
Attention to : Anti-Money Laundering Compliance Unit
(To be opened by addressee only.)
Fax : +6087-411496
E-mail : aml@labuanfsa.gov.my

16.3.5 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and/or Anti-Money Laundering Compliance Unit, Labuan FSA, the Compliance Officer of a reporting institution must submit its suspicious transaction reports on-line :-
Website: https://bnmapp.bnm.gov.my/fins2

16.3.6 The DCO must ensure that the STR is submitted within the next working day from the date the DCO establishes the suspicion.

16.3.7 The DCO must ensure that in the course of submitting the STR, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The DCO has the sole discretion and independence to report suspicious transactions.

16.3.8 The Bank must provide additional information and documentation as may be requested by Labuan FSA and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.

16.3.9 The Bank must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

16.3.10 Where a STR has been lodged, the Bank is not precluded from making a fresh STR when a new suspicion arises.

16.4 Tipping Off

16.4.1 In cases where the Bank forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, the Bank is permitted not to pursue the CDD process. In such circumstances, the reporting institution shall proceed with the transactions and immediately file a STR.

16.4.2 Tipping off in relation to STR is not applicable if :-

(i) The purpose of the disclosure is made to inform the ML/TF risks involved in dealing with the customer within the financial group; or

(ii) Such disclosure is made to Labuan FSA or other supervisory authorities.

16.5 Internally Generated Suspicious Transaction Reports

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

17.0 Retention of Records

Statutory provision :-

Section 17 of the AMLATFA provides as follows –

(1) *Notwithstanding any provision of any written law pertaining to the retention of documents, a reporting institution shall maintain any record under this Part for a period of not less than six years from the date an account has been closed or the transaction has been completed or terminated.*

(2) A reporting institution shall also maintain records to enable the reconstruction of any transaction in excess of such amount as the competent authority may specify, for a period of not less than six years from the date the transaction has been completed or terminated.

(3) Subsections (1) and (2) will not apply where a reporting institution has transmitted the record to the competent authority or an enforcement agency.

(4) Any reporting institution which contravenes subsection (1) or (2) commits an offence and shall on conviction be liable to a *fine not exceeding one million ringgit or to imprisonment for* a *term not exceeding one year or to both.*

17.1 The Bank is required to keep the relevant records including any accounts, files and business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and beneficial owners, and results of any analysis undertaken. The records maintained must remain up-todate and relevant.

17.2 The Bank is required to keep the records for at least six years following the completion of the transaction, the termination of business relationship or after the date of occasional transaction. All records must be stored securely and be capable of being retrieved without undue delay.

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

17.4 The Bank shall retain the relevant records in the form that is admissible as evidence in court and make available to the supervisory authorities and law enforcement agencies in a timely manner.

17.5 Relevant records would include :-

(i) Copies of customer identification documentation.

(ii) Supporting documentation for all transactions carried out for customers.

(iii) All suspicion reports to the "Money Laundering Reporting Officer".

(iv) All reports to the authorities and correspondence with them.

(v) All monitoring and review work carried out.

(vi) All internal reports.

18.0 Employee Training and Awareness Programmes

18.1 Awareness and training programmes on AML/CFT practices and measures must be conducted for the Bank's employees. For this purpose, the Bank has engaged an external certified trainer to conduct training programmes regularly at least 2 times in a year and supplemented with refresher course.

18.2 All employees may be held personally liable for any failure to observe the AML/CFT requirements.

18.3 The Bank's AML/CFT policies and procedures are readily available and accessible to all employees and its documented AML/CFT measures contain at least the following :-

(a) The relevant documents on AML/CFT issued by Labuan FSA or relevant supervisory authorities; and

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

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

18.5 Training for all employees shall include a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the DCO and the importance of CDD.

18.6 In addition, training will also be provided to specific categories of employees :-

(a) **Front-Line Employees**

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

(b) **Employees that Establish Business Relationships**

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

(c) **Supervisors and Managers**

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

19.0 Internal Anti-Money Laundering Report

An internal anti-money laundering report shall be prepared by the DCO at the end of each month. All issues reported in the internal report must be highlighted to the Board.

20.0 Combating the Financing of Terrorism

20.1 The various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011) require sanctions against individuals and entities belonging or related to the Taliban, Osama bin Laden and the Al-Qaeda organisation must be kept in file and updated as and when necessary.

20.2 Screening of potential customers including directors and shareholders is required prior to establishing any banking relationship. Alternatively, the updated UN List can be obtained at :-
http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

20.3 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 must be maintained by the Bank.

20.4 All information contained in the database (paragraph 20.3) must be updated and relevant, and made easily accessible to its employees.

20.5 The Bank must conduct regular checks on the names of new and existing customer and potential customers.If there is any name match, the Bank must take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, the following actions must be taken immediately :-

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

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

(c) Submit a STR; and

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

20.6 A STR must be submitted when there is an attempted transaction by any of the listed in the Consolidated List or orders made by the Minister of Home Affairs under sections 66B or 66C of the AMLATFA.

20.7 The Bank must ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate “false positives”. Further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match must be made.

20.8 Databases with the other recognised lists of designated persons or entities issued by other jurisdictions will be checked.

21.0 Independent Audit Functions

21.1 The requirements for the independent audit functions shall be read together with the Guidelines on Minimum Audit Standards for Internal Auditors of Labuan Banks and Supplementary Guidelines to Minimum Audit Standards for Internal Auditors issued by Labuan FSA.

21.2 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, subsidiary legislations and relevant policies, circulars and directives on AML/CFT issued by the Labuan FSA as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

21.3 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 shall include, at a minimum :-

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

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

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

(a) Compliance with AMLATFA, its subsidiary institution’s subsidiary legislation and instruments issued under the AMLATFA;

(b) Compliance with the reporting institution’s internal AML/CFT policies and procedures;

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

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

21.5 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.

21.6 The Bank shall ensure that independent audits are carried out at the institution level at least on an annual basis.

21.7 The Bank must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Supervision and Enforcement Department, Labuan FSA within three months after the completion of the internal audit.

22.0 Non-Compliance

22.1 Enforcement actions can be taken against the Bank including its Directors, Officers, and Employees for any non-compliance with provisions under :-

(a) In Sections 22, 66E, 86, 87, 88, 92 and 93 of the AMLATFA; and/or

(b) Section 4B of LFSAA.

INDICATIVE LIST OF HIGH RISK CUSTOMERS

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.

2. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.

3. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.

4. Customers based in high risk countries / jurisdictions or locations.

5. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.

6. Embassies / Consulates.

7. Off-shore (foreign) corporation / business.

8. Non face-to-face customers.

9. High net worth individuals.

10. Firms with 'sleeping partners'.

11. Companies having close family shareholding or beneficial ownership.

12. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale.

13. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.

14. Investment Management/ Money Management Company/Personal Investment Company.

15. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.

16. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.

17. Trusts, Charities, NGOs/NPOs (especially those operating on a cross-border basis) unregulated clubs and organizations receiving donations (excluding NPOs / NGOs promoted by United Nations or its agencies).

18. Money Service Business: including seller of: Money Orders / Travellers' Checks /Money Transmission / Check Cashing / Currency Dealing or Exchange.

19. Gambling / gaming including "Junket Operators" arranging gambling tours.

20. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).

21. Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries).

22. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.

23. Customers that may appear to be multi-level marketing companies etc.

INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

1. Non-Bank Financial Institution.
2. Stock brokerage.
3. Import / Export.
4. Car / Boat / Plane Dealership.
5. Electronics (wholesale).
6. Travel agency.
7. Used car sales.
8. Telemarketers.
9. Providers of telecommunications service, internet café, IDD call service, phone.
10. Cards, phone center.
11. Dot-com company or internet business.
12. Pawnshops.
13. Auctioneers.
14. Sole practitioners or Law Firms (small, little known).
15. Notaries (small, little known).
16. Secretarial Firms (small, little known).
17. Accountants (small, little known firms).
18. Venture capital companies.

INDICATIVE LIST OF LOW RISK CUSTOMERS

1. Salaried employees whose salary structures are well defined.

2. People belonging to low economic strata of the society whose accounts show small balances and low turnover.

3. Government Departments and Government owned companies, regulators and statutory bodies etc.

4. Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment).

5. Customers with long term and active business relationship with the Bank (who are not categorized under High / Medium Risk).

6. NGOs promoted by United Nations or its agencies.

INDICATIVE LIST OF HIGH RISK PRODUCTS & SERVICES

1. Electronic funds payment services such as electronic cash (e.g. stored value and pay roll cards).
2. Funds transfers (domestic and international), etc.
3. Electronic Banking.
4. Private Banking (domestic and international).
5. Trust and Asset Management Services.
6. Monetary instruments such as Travelers' Cheque.
7. Foreign Correspondent Accounts.
8. Trade Finance (such as letters of credit).
9. Project Financing of sensitive industries in high-risk jurisdictions.
10. Trade Finance Services and transactions involving high-risk jurisdictions.
11. Services offering anonymity or involving third parties.
12. Services involving banknote and precious metal trading and delivery.
13. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

INDICATIVE LIST OF MEDIUM RISK PRODUCTS & SERVICES

1. Lending activities, particularly loans secured by cash collateral and marketable securities.

2. Non-deposit account services such as Non-deposit investment products and insurance.

EXAMPLES OF TRANSACTIONS THAT MAY TRIGGER SUSPICION

1. Unusual amount of remittances which does not reflect an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

2. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

3. Customers who deposit cash by means of numerous credit slips such that the total of each deposit is insignificant, but the total of all the credits is significant.

Accounts

4. Accounts that appear to act as pass through accounts with high volumes of credits and debits and low average monthly balances.

5. Customers who wish to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions which involve nominee names.

6. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total amount of credits would be large.

7. Any individual or company whose account shows no normal personnel banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

8. Reluctance to provide normal information when opening an account or providing information that is difficult or expensive for the reporting instruction to verify.

9. Customers who appear to have accounts with several reporting institutions within the same locality but choose to consolidate funds from such accounts on regular basis for onward transmission to a third party account.

10. Matching of payments out with credits paid-in by cash on the same or previous day.

11. Paying in large third party cheques endorsed in favour of the customer.

12. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpectedly large credit from abroad.

13. Company's representatives avoiding contact with branch officers.

14. Substantial increases in deposits or negotiable instrument by a professional firm or company, using client accounts or in-house company, or trust accounts, especially if the deposits are promptly transferred between other client's company and trust accounts.

15. Customers who show an apparent disregard for accounts offering more favourable terms, e.g. avoidance of high interest rate facilities for large credit balances.

16. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

17. Insufficient use of normal banking facilities.

18. Large number of individuals making payments into the same account without any adequate explanation.

International Banking/Trade Finance

19. Customers introduced by an overseas branch, affiliate or any other bank based in countries where production of drugs or drug trafficking may be prevalent.

20. Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

21. Customers who make regular and large payments, including wire transfers, that cannot be clearly identified as bona fide transactions, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs, prescribed terrorist organizations or which are tax havens.

22. Building up of large balances, which are not consistent with the known turnover of the customer's business, and subsequent transfer to accounts held overseas.

23. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing, through an account.

24. Frequent requests for travellers' cheques or foreign currency drafts or other negotiable instruments to be issued.

25. Customers who show apparent disregard for arrangements offering more favourable terms.

26. Items shipped that are inconsistent with the nature of the customer's business.

27. Customers conducting business in higher risk countries.

28. Customers shipping items through higher risk countries, including transit through non-cooperative countries.

29. Customers involved in potentially higher risk activities, including activities that may be subject to export/import restrictions (e.g. equipment for military of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles and sensitive technical data).

30. Obvious over or under pricing of goods and services.

31. Obvious misrepresentation of quantity or type of goods imported or exported.

32. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.

33. Customers request payment of proceeds to an unrelated third party.

34. Shipment locations or description of goods not consistent with letter of credit.

35. Significantly amended letters of credits without reasonable justification or changes to the beneficiary or location of payment.

Employees and Agents

36. Changes in employee's characteristics, e.g. lavish life styles or avoiding taking holidays.

37. Changes in employees or agent's performance, e.g. the salesman, selling products for cash, have a remarkable or unexpected increase in performance.

38. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

39. For private banking or trust services, sudden strong performance by employees in special relationship/confidential relationship banking services

such as trust or private banking services or sudden increase in the wealth/spending of such employees.

Private Banking and Trust Services

40. The grantors of private banking trust accounts that direct loans from their accounts to other parties or business interests of account principals or beneficiaries.

Secured and Unsecured Lending

41. Customers who repay problem loans unexpectedly and with no proper explanation as to the source of funds.

42. Request to borrow against assets held by the reporting institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

43. Request by a customer for a reporting institution to provide or arrange financial contribution to a deal which is unclear, particularly, where property is involved.

44. A customer who unexpectedly repays in part or in full a fixed loan or other loan that is inconsistent with his/her earning capacity or asset base.

45. A customer who applies for property / vehicle loan with a very low margin of finance that is not customary for the type of property / vehicle or profile of the customer.