Anti-Money Laundering and Counter Terrorist Financing (AML and CTF) Policy

Table of Contents

1 Introduction

1.1 Anti-Money Laundering Measures

(a) The International Islamic Liquidity Management Corporation ("IILM") fully endorses and commits to implement the applicable anti-money laundering and the counter-terrorist financing recommendations of the Financial Action Task Force.

(b) The Financial Action Task Force ("FATF") is an inter-governmental body established by the G-7 Summit in 1989. The mandate of the FATF is to set the standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing, as well as the financing of proliferation of weapons of mass destruction and other related threats to the integrity of the international financial system.

(c) The FATF Recommendations set out a comprehensive and consistent framework to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global benchmarks for anti-money laundering ("AML") and counter-terrorist financing ("CTF").

(d) The FATF Recommendations set out an international standard for AML and CTF for the community of nations to implement and have in place how to:

(i) Identify the risks of money laundering and terrorist financing, and develop policies and domestic coordination in respect of AML and CTF;

(ii) Prevent money laundering, terrorist financing as well as the financing of the proliferation of weapons of mass destruction;

(iii) Apply AML and CTF preventive measures for the financial sector and designated non-financial businesses and professions; and

(iv) Enhance transparency and availability of information relating to beneficial ownership of legal persons and arrangements and generally facilitate international cooperation on AML and CTF.

1.2 Financial Action Task Force (FATF) Recommendations

FATF has adopted a set of forty (40) recommendations on combating money laundering and financing of terrorism and proliferation of weapons of mass destruction ("FATF Recommendations"), which constitute a comprehensive framework for preventing, detecting and suppressing both money laundering and terrorist financing as follows -

No.	FATF Forty Recommendations
1.	Assessing risks and applying a risk-based approach
2.	National cooperation and coordination
3.	Money laundering offence
4.	Confiscation and provisional measures
5.	Terrorist financing offence
6.	Targeted financial sanctions related to terrorism and terrorist financing
7.	Targeted financial sanctions related to proliferation
8.	Non-profit organisations
9.	Financial institution secrecy laws
10.	Customer due diligence
11.	Record keeping
12.	Politically exposed persons
13.	Correspondent banking
14.	Money or value transfer services
15.	New technologies
16.	Wire transfer
17.	Reliance on third parties
18.	Internal controls and foreign branches and subsidiaries
19.	Higher-risk countries
20.	Reporting of suspicious transactions
21.	Tipping-off and confidentiality
22.	Designated non-financial Businesses and Professions ("DNFBPs"): Customer due diligence
23.	DNFBPs: Other measures
24.	Transparency and beneficial ownership of legal persons
25.	Transparency and beneficial ownership of legal arrangements
26.	Regulation and supervision of financial institutions
27.	Powers of supervisions
28.	Regulation and supervision of DNFBPs
29.	Financial intelligence unit
30.	Responsibilities of law enforcement and investigative authorities
31.	Powers of law enforcement and investigative authorities
32.	Cash couriers
33.	Statistics
34.	Guidance and feedback
35.	Sanctions
36.	International instruments
37.	Mutual legal assistance
38.	Mutual legal assistance: Freezing and confiscation
39.	Extradition
40.	Other forms of international cooperation

1.3 Scope and Purpose of Policy

(a) The provisions and procedures detailed in the Policy shall apply to -

(i) the IILM;

(ii) the subsidiary companies of the IILM; and

(iii) Staff and customers of the IILM and its subsidiaries.

Item (i) and (ii) shall be collectively known as the "IILM Group".

(b) The Governing Board, Committees of the Governing Board, the Shariah Committee, the Senior Management and the staff of the IILM Group shall be fully conscious and alert to the risks of money laundering and financing of terrorism associated with all its operations, business products and services and to prevent the IILM from being abused by money launderers and financiers of terrorism.

(c) The purpose of this Policy is to assist the IILM Group in complying with their express obligations in preventing money laundering and terrorist financing.

2 Money Laundering and Terrorist Financing: Definitions and Explanations

2.1 Money Laundering

(a) In general, money laundering is the involvement in any transaction or series of transactions by which proceeds from a criminal activity are disguised to conceal their illicit origins.

(b) Most countries subscribe to the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention) and the United Nations Convention Against Transnational Organised Crime (2000) (Palermo Convention) -

(i) The conversion or transfer of property, knowing that such property is derived from any offence and offences or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his action;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property knowing that such property is derived from an offence or offences or from an act of participation in such an offence or offences; and

(iii) The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offence or offences or from an act of participation in such offence or offences.

(c) The FATF defines the term 'money laundering" as "the processing of… criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gain of crime.

(d) The term money laundering "predicate offence" refers to the underlying criminal activity that generated the proceeds, which when laundered, result in the offence of money laundering. The predicate offences are listed in Schedule 1 of the Policy.

2.2 Terrorist Financing

(a) Terrorist financing generally refers to the financial support, in any form, of terrorism or of those who encourage, plan or engage in the commission of terrorism.

(b) Terrorist financing offences shall extend to any person who wilfully provides or collects funds by means, directly or indirectly, with the unlawful intention that they shall be used or in the knowledge that they are to be used, in full or in part -

(i) to carry out one or more terrorist acts;

(ii) by a terrorist organisation; or

(iii) by an individual terrorist.

2.3 Stages of Money Laundering

Money laundering process involves three (3) stages that may occur independently, simultaneously or may overlap with each other -

(a) Placement

This is the initial stage which involves the physical disposal of the proceeds derived from illegal activities into the financial system. Illegal activities include drug trafficking, prostitution rings, smuggling, illegal arms sale, kidnapping for ransom, embezzlement, insider trading, bribery, computer-fraud schemes, get-rich-quick schemes and sale of children and smuggling of human beings and organs. The illegal profits can be introduced into the financial system by various means. Placement may also be accomplished by the cash purchase of securities such as papers issued by the IILM group at the issuance level or at the secondary market level.

(b) Layering

This is the process of separating illicit proceeds from their source by creating a series of complex layers of financial transactions designed to obscure audit trails and to provide anonymity. It can be done through transactions such as purchase and sales of securities, other investment instruments or through multiple transfers of funds from different accounts around the world disguised as payments for goods or services.

(c) Integration

This is the stage where illegal proceeds are integrated back into the economy as legitimate funds through legitimate transactions such as business ventures, luxury assets, lending and investing.

As noted by the IMF/World Bank, "…complex international financial transactions can be abused to facilitate the laundering of money and terrorist financing, the different stages of money laundering and terrorist financing occur within a host of different countries. For example, placement, layering, and integration may each occur in three separate countries; one or all of the stages may also be removed from the original scene of the crime."

3 Know Your Customer Procedure (Customer Due Diligence)

3.1 General

(a) The IILM has a well-designed customer identification and due diligence ("Customer Due Diligence") procedure in place.

(b) The Customer Due Diligence ("CDD") is intended to assist the IILM Group in forming a reasonable belief that they have appropriate awareness of the true identity of each customer and the true nature of the matter the IILM Group is being engaged to undertake.

(c) The Policy of the IILM Group refers to the documented principles and operational rules which set out the approach of the Group to detect, deter and prevent money laundering and terrorist financing and ensure that it can effectively identify, verify and monitor its customers and the financial transactions in which they engage, relative to the risks of money laundering and terrorism financing.

(d) In accordance with the guidance of the FATF Recommendations and its related interpretative notes, the IILM Group will engage in its own assessment of money laundering and terrorist financing risk associated with the nature and size of IILM's business.[1] Therefore, for the purposes of IILM's CDD, a "customer" shall mean those financial institutions, asset providers, companies or professional service providers that purchase IILM securities directly from any member of the IILM Group, sell assets to any member of the IILM Group as the basis for the IILM programme or otherwise directly participate in the issuance of IILM securities through privity of contract with IILM.

3.2 Scope of Customer Identification and Due Diligence

(a) The IILM Group shall be required to undertake CDD measures when -

(i) establishing business relations;

(ii) there are reasonable grounds to suspect money laundering or terrorist financing; or

(iii) the IILM Group has doubts about the veracity or adequacy of previously obtained customer identification data.

(b) The CDD measures to be taken are as follows -

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

(ii) identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner;

(iii) understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

(iv) conducting ongoing due diligence on the business relationship and security of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the IILM Group knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

(c) However, a simplified due diligence may be applied where the IILM has reasonable grounds to believe that the client is -

(i) any company or institution which is subject to the same requirements as stated in the FATF Recommendations;

[1] *Interpretive Notes to the FATF Recommendations,* "Interpretive Note to Recommendation 1 (Assessing Risk and Applying a Risk-Based Approach".

(ii) a company or institution which is listed on an internationally recognised regulated market, including but not limited to the London Stock Exchange, New York Stock Exchange, Qatar Exchange and Singapore Exchange;

(iii) a public authority of a country -

(A) which has a publicly available, transparent and certain identity and is accountable to a community institution and subject to appropriate check and balance procedures; and

(B) whose operations, activities and accounting practices are transparent.

3.3 Corporate Customer

(a) The CDD shall cover at least the following details regarding each corporate customer -

(i) name of corporate customer;

(ii) company/corporate registration number;

(iii) date of incorporation or formation;

(iv) nature of business;

(v) contact details;

(vi) address of registered office; and

(vii) the principal place of business.

(b) The IILM Group shall require the corporate customer to furnish the original or certified true copies of the following -

(i) certificate of incorporation, partnership agreement or deed of trust;

(ii) memorandum of association and/or articles of association;

(iii) particulars of directors, the chief executive officer, senior managers and secretaries;

(iv) return of allotment of shares of the customer;

(v) authorisation for any person to represent the customer; and

(vi) relevant documents to identify the identity of the person authorised to represent the customer in its dealing with the IILM Group.

(c) If the IILM Group is in doubt, it may:

(i) conduct a winding up search or enquiry on the background of the corporate customer to ensure that it has not been, or is not in the process of being dissolved or liquidated; and

(ii) verify the authenticity of the information provided by the corporate customer with the relevant authorities for registration of businesses or corporations.

3.4 Existing Customers

(a) IILM Group shall conduct regular reviews on existing records of customers especially when:

(i) a significant transaction is to take place (such regular review to be conducted at minimum on an annual basis);

(ii) the customer's documentation standards change substantially; or

(iii) it discovers that information held on the customer is insufficient.

3.5 Non-Face-to-Face Business Relationships

(a) A non-face-to-face customer and business relationship is a business relationship *via* information communication technology such as the internet, post, fax or telephone.

(b) Measures that IILM Group may use to verify non-face-to-face customers include, but are not limited to -

(i) require additional documents to complement those which are required for face-to-face customers;

(ii) develop independent contact with the customer; and

(iii) verify customer information against databases maintained by authorities.

3.6 Politically Exposed Persons (PEPs)

(a) PEPs are individuals who are or 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/ corporations or political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.

(b) 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.

(c) Once a PEP is identified, additional due diligence measures shall consist of the following -

(i) identifying the PEPs;

(ii) establish the source of wealth and funds of such PEP;

(iii) consult the CEO or the Governing Board of the IILM in deciding to enter into or continue business relationship with PEPs; and

(iv) conduct enhanced ongoing due diligence on PEP throughout the IILM business relationship with such PEP. The IILM Group is fully aware that business relationship with family members or close associates of PEPs involve similar reputational risks to those with PEPs themselves.

3.7 Higher Risk Customers

(a) The factors for high risk customer are as follows -

(i) the business relationship is conducted in unusual circumstances;

(ii) companies that have nominee shareholders or shares in bearer form; or

(iii) the ownership structure of the company appears to be unusual or excessively complex given the nature of the company's business.

(b) For higher risk customers, IILM Group shall -

(i) obtain more detailed information from the customer (e.g. occupation, volume of assets, etc.) and through publicly available information and updating more regularly the identification data of the customer;

(ii) obtain information on the source of funds or source of wealth of the customer;

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

(iv) obtain approval from the CEO of the IILM before establishing business relationship with the customer.

(c) The IILM Group shall not establish business relationships with a high risk customer until a CDD is completed satisfactorily.

3.8 Higher Risk Countries

(a) The factors for high risk countries are as follows -

(i) countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML and/or CTF systems. Examples of credible sources include FATF or FATF-styled regional bodies' mutual evaluation or detailed assessment reports or published follow-up reports.

(ii) countries subject to sanctions, embargos or similar measures issued by the United Nations.

(iii) countries identified by credible sources as having significant levels of corruption or other criminal activity.

(iv) countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country

(b) The type of enhanced due diligence measures to business relationships and transactions with high risk countries shall be effective and proportionate to the risks involved and the Sanctions Policy of the IILM Group.

4 Suspicious Transactions

(a) The IILM Group may regard a transaction as suspicious if -

(i) the identity of the person involved in the transaction; or
(ii) the transaction itself; or
(iii) any other circumstances concerning the transaction,

gives the Group reason to suspect that the transaction involves proceeds of an unlawful activity.

(b) "Reason to suspect" is more than mere speculation but falls short of actual proof of knowledge. The IILM Group practises the principle that there must be a degree of satisfaction of suspicion, even if it does not amount to belief.

(c) In case of suspicious transactions, IILM Group may first ask for additional information or perform such other diligence necessary regarding the suspected transaction. After examining such additional information, the IILM Group may form a suspicion that money laundering or terrorist financing is involved.

(d) The IILM Group is not required to investigate into a particular transaction before having a reason to suspect. However, the IILM Group shall review the information available, obtain clarification or explanations from related parties if necessary, and exercise professional judgment or forming an opinion on the information in hand, as to whether or not there is a basis for "reason to suspect".

5 Reporting Obligations and Procedures

5.1 Reporting of Suspicious Transactions

(a) If the IILM Group suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it shall report its suspicions to the appropriate Financial Intelligence Unit (FIU) in the related jurisdiction. The Governing Board shall provide guidance to the IILM Group on which the Financial Intelligence Unit, a suspicious transaction report ("STR") should be lodged with or whether any other action is to be taken.[2]

(b) All suspicious transactions, including attempted transactions, shall be reported regardless of the amount of the transaction

(c) The IILM Group shall ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

(d) In pursuing any STR, the IILM Group shall follow the procedures specified in Appendix I hereto.

5.2 Tipping Off and Confidentiality

(a) The IILM Group and officers shall not -

(i) be subject to any criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative position, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(ii) disclose (tipping-off) the fact that a STR or related information is being filed with the FIU.

[2] See Appendix I, "Reporting Mechanisms for Suspicious Transactions" for procedures for reporting suspicious transaction pursuant to the guidance of the Governing Board.

6 Record Keeping

(a) The IILM Group shall maintain all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish background and purpose of complex or unusual large transactions), for at least five (5) years after the business relationship is ended or after the date of the occasional transaction.

(b) All records maintained shall be kept in such a manner to enable a swift access and retrieval so as to attend in a timely manner to the information requests from competent authorities.

7 Internal Controls, Compliance and Audit

(a) The IILM Group has an internal procedure including ongoing training that keeps the staff and officers of the IILM Group informed on the developments in AML and CTF. The training shall:

(i) describe the nature and processes of money laundering and terrorist financing;

(ii) explain AML and CTF laws and regulatory requirements; and

(iii) explain the policies and systems with regards to the reporting requirements regarding suspicious activity, with emphasis on customer identification and due diligence.

(b) The IILM Group shall designate a Group AML and CTF Compliance officer, who shall be a top management officer as the AML and CTF compliance officer at the management level. The compliance officer shall ensure that appropriate management attention is devoted to compliance efforts within the IILM Group.

Appendix I

Reporting Mechanisms for Suspicious Transactions

Pursuant to the guidance and resolutions of the Governing Board from its meeting on 2 of April 2013, the IILM shall refer any substantiated suspicious transactions to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia (FIED) for enforcement action or liaising with other appropriate FIU's. Although the IILM is not a reporting institution pursuant to FIED guidelines, the following procedures have been stipulated in reference to the FIED's guidelines for banks and other account-holding institutions ('Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1)'). In accordance with Sections 4 and 5 of the Policy, the IILM shall take the following steps with regards to any incident involving a suspicious transaction:

1. Any officer, employee or agent of the IILM Group, upon observing or receiving information regarding a suspicious transaction involving the IILM Group, will submit a STR (in the form as it appears at Schedule A of this Appendix I) directly to the IILM compliance officer;

2. Upon receiving any STR, the IILM compliance officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the IILM compliance officer must promptly submit the substantiated STR to the IILM management committee with the recommendation that such STR be submitted to the FIED. In the case where the IILM compliance officer decides that there are no reasonable grounds for suspicion, the IILM compliance officer must document and file the decision, supported by the relevant documents and inform the related department manager regarding such unsubstantiated STR.

3. After review by the IILM management committee, the IILM compliance officer will submit the substantiated STR to the FIED through any of the following modes:

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

   Fax : +603-2693 3625
   E-mail : str@bnm.gov.my

4. The IILM management committee shall promptly inform the Governing Board of any substantiated STR to be delivered to the FIED and shall similarly inform the

Governing Board of any subsequent information from or enforcement action by the FIED or other appropriate FIU.

5. The IILM compliance officer must ensure that the substantiated STR is submitted to the FIED within the next working day from the date the IILM compliance officer submitted such STR to the IILM management committee.

6. The IILM will ensure that in the course of submitting the STR to the FIED, utmost care is undertaken to ensure that the STR is treated with the highest level of confidentiality. Notwithstanding any exigent circumstances or instruction from the Governing Board, the IILM compliance officer has the sole discretion and independence to report suspicious transactions.

7. The IILM will provide additional information and documentation as may be reasonably requested by the FIED and respond promptly to any further enquiries with regards to any STR received by the FIED.

8. In cases where the IILM reasonably believes that performing an additional CDD process would tip off the Customer, the IILM is permitted not to pursue the CDD process. In such circumstances, the IILM shall proceed with the transaction and immediately conduct the STR process as specified in this Appendix I.

9. The IILM will ensure that the IILM compliance officer maintains a complete file on all STRs and any supporting documentary evidence regardless of whether such STR has been submitted to the FIED. If there is no STR submitted to FIED, the unsubstantiated STR and the relevant supporting documentary evidence will be made available to the FIED upon request.

10. The IILM compliance officer will periodically submit a report with all unsubstantiated STRs which occurred during such period to the IILM management committee.

Schedule A

Form of IILM STR

SUSPICIOUS TRANSACTION REPORT

- This STR is made pursuant to the requirement to report suspicious transaction under the IILM Anti-Money Laundering and Counter Terrorist Financing (AML and CTF) Policy.

- No civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith.

PART A: CUSTOMER INFORMATION

Nationality or Country of Origin:

Customer type: (Individual/Corporate/GRE/Other)

Name:

Previous name(s):

New NRIC no.: Old NRIC no.:

Other identification: Other identification type:

Gender:

Contact information

Address/ Principal place of business:

Correspondence address:

Other address: Previous address:

Email address:

Contact no.: (Off) (Res) (Mob)

Fax no.:

Employment information (If customer not an individual, go to Part B)

Business/ employment type:

Occupation:

Occupation description:

Employer name:

Employment area:

Other known employment:

Marital information

Marital status:

Spouse identification

Spouse name:

New NRIC no.:

Old NRIC no.:

Other identification:

Other identification type:

Passport no.:

Country of issue:

PART B: IILM PERSONNEL REPORTING THE TRANSACTION

Nationality:

Name:

Other/previous name:

NRIC or Passport No.:

Gender:

Contact information

Correspondence address

Residential address

Other address

Previous address

Email address:

Contact no.: (Off) (Res) (Mob)

Marital information

Marital status:

Spouse name:

Spouse identification

New NRIC no.: Old NRIC no.:

Other identification: Other identification type:

Passport no.: Country of issue:

PART C: TRANSACTION DETAILS

Attempted but not completed transaction? (No/Yes)

Transaction Related to IILM Issuance Program? (No/Yes)

Series Designation: Currency type:

Transaction date: Total amount:

Type of transaction:

PART D: DESCRIPTION OF SUSPICIOUS TRANSACTION	
Grounds for suspicion	(Activity inconsistent with customer profile)
	(Regular/unusual activity)
	(Large/unusual inward/outward order)
	Others (specify)
Others (please specify)	
Description of suspected criminal activity	
Details of the nature and circumstances surrounding it	
Date of reporting	