AIIB Directive on
Anti-Money Laundering and Combating the Financing of Terrorism
Dec. 28, 2018

1. Overriding Objective and Purpose

1.1 The Directive on Anti-Money Laundering and Combating the Financing of Terrorism (the AML/CFT Directive) establishes the Anti-Money Laundering and Combating the Financing of Terrorism Framework (the AML/CFT Framework) of the Asian Infrastructure Investment Bank (AIIB or the Bank).

1.2 This AML/CFT Directive shall be read in conjunction with the Operational Policy on International Relations regarding compliance with measures decided by the UN Security Council under Chapter VII of the Charter of the United Nations.

1.3 With reference to international guidance[1], this AML/CFT Directive and its implementing processes and procedures are intended to establish principles and guidance to safeguard AIIB (including its personnel) from money laundering, the financing of terrorism or other illicit activities that would constitute a predicate offence for money laundering or the financing of terrorism.

2. Applicability and Scope

2.1. The AML/CFT Directive is applicable to all operations and activities of the Bank, and it applies to all personnel of AIIB, including the President, officers, staff, consultants, and other personnel employed or acting on behalf of the Bank.

3. Definitions

3.1. Beneficial Owner (BO) is the natural person(s) who ultimately owns or controls a counterparty and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.[2]

3.2. Counterparty Due Diligence (CDD) is the process of identifying and verifying the true identity of a counterparty to assess and evaluate the risk of ML/FT associated with that counterparty.

3.3. Money Laundering (ML) is defined, based on the relevant United Nations definition, in the following manner:

[1] Such guidance includes the Recommendations of the Financial Action Task Force (FATF) "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" and the Basel Committee on Banking Supervision's Guidelines on "Sound Management of Risks related to Money Laundering and Financing of Terrorism".
[2] Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.

"(a)(i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;
(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
(b) (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;
(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article." [3]

3.4. Financing of Terrorism (FT) refers to a person who, by any means, directly or indirectly, unlawfully and willfully, provides or collects (or attempts to provide or collect) funds with the intention or knowledge that such funds are to be used to carry out any terrorist acts[4].

3.5. Risk-based Approach (RBA) in respect of AML/CFT procedures is the process of identifying, assessing and understanding ML/FT risk to which AIIB is exposed and to take measures commensurate to those risks in order to mitigate them effectively.

4. The AML/CFT Framework

The AML/CFT Framework shall contain the following key measures:

4.1. Counterparty Due Diligence (CDD) – Know Your Counterparty (KYC). AIIB shall carry out CDD/KYC in respect of all counterparties and, if appropriate, their Beneficial Owners, in advance of entering into a relationship and/or a transaction with such counterparties. AIIB shall apply the Risk-based Approach for CDD/KYC in accordance with their ML/FT risk vulnerabilities.

4.2. Rolling Review and On-going Monitoring. AIIB shall review the CDD/KYC in respect of all counterparties on an on-going basis and ensure the information is up-to-date. The Bank shall monitor on an on-going basis the counterparty activities to identify any suspicious activities and/or transactions, and to report as required as further described herein. That may include the use of automated systems, if appropriate, to facilitate the review and/or the monitoring.

4.3. Terrorist lists and economic sanctions screening. Prior to the on-boarding of, or entry into any business or transactional relationship with, any counterparty, AIIB

[3] 2003 United Nations Convention against Transnational Organized Crime (Article 6) and 2005 United Nations Convention against Corruption (Article 23).
[4] See Article 2 of the International Convention for the Suppression of the Financing of Terrorism.

shall screen such counterparty against relevant terrorism and economic sanctions lists. Such screening shall also be performed on an on-going basis.

5. Reporting Obligations

5.1. AIIB shall put in place processes to enable AIIB personnel to report suspicion of ML or FT in any activities or transactions. Such suspicious activity reports shall be reported to the CRO in a confidential manner who shall then take appropriate action.

6. ML/FT Risk Management – Governance and Oversight

6.1. For ML/FT risk management, AIIB shall apply the three lines of defense model as set out in AIIB's Risk Management Framework.

6.2. The Risk Committee shall fulfil its role and carry out the function of risk oversight in respect of ML/FT risk as defined in the Terms of Reference of the Risk Committee.

6.3. The Heads of Departments, as further defined in the respective AGs, shall be responsible for ML/FT risk applicable to them, and ensure effective internal control pertaining to their functions will be put in place and operated effectively. A specialist AML/CFT function of Compliance shall support the departments in meeting this responsibility.

6.4. Roles and responsibilities of AIIB functions and personnel for managing ML/FT risk shall be detailed in the relevant AGs.

7. Staff awareness training

7.1. AIIB shall take risk-based measures to raise the awareness of the Personnel on ML/FT. Compliance function of AIIB shall train the relevant personnel specifically on an on-going basis.

8. Record Keeping

8.1. AIIB shall retain records of all transaction data and documentation obtained for the purposes of AML/CFT, including CDD, for at least five years after the end of the relationship or completion of the transactions.

9. Data Protection, Confidentiality and Privacy

9.1. The Bank shall ensure that all counterparty information obtained in order to fulfill AML/CFT requirements is protected and kept confidential in accordance with applicable regulations, including those related to data protection and privacy.

10. Review

10.1. The CRO shall review and propose to amend, if necessary, this AML/CFT Directive at least once every two years.

11. Information Disclosure

11.1. The Bank's Policy on Public Information and its related Directive and Administrative Guidance governs the disclosure of all information in the Bank's possession, including with respect to this Directive.

12. Implementation and Authority

12.1. The CRO shall

(i) oversee this Directive;

(ii) monitor its implementation;

(iii) make all final decisions regarding the interpretation and application of this Directive; and

(iv) prepare and issue any relevant Administrative Guidance to ensure the efficient implementation of this Directive.