PUBLIC

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM (AML/CFT) FRAMEWORK

INTER-AMERICAN DEVELOPMENT BANK
ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM FRAMEWORK

I. Introduction

1.1 **Purpose**. The purpose of this Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)[1] Framework is to formalize the IDB's commitment to the management of the risks related to Money Laundering and Terrorist Financing (ML/TF) in its operations in a manner aligned with international best practices that applies coordinated and consistent risk-management practices. The IDB will adopt mechanisms to carry out that commitment by:

(i) ensuring that each IDB business unit[2] (BU) applies AML/CFT controls that are appropriate for the ML/TF risks presented by the activities of that BU;
(ii) creating a process by which BUs will engage the support of the Office of institutional Integrity (OII) and the Office of Risk Management (RMG) to determine the appropriate AML/CFT controls for their distinct operations and corporate transactions; and
(iii) establishing a governance structure whereby OII performs an AML/CFT compliance function, pursuant to which it will oversee the AML/CFT system, provide advice to BUs regarding the management of ML/TF risks and be the designated unit to which ML/TF red flags are escalated when required.

1.2 **Background.** Money Laundering and Financing of Terrorism are global problems that have significant economic and social consequences, including increased crime and corruption, financial system instability, market distortions, and lost tax revenue. They both involve the misuse of the financial system to facilitate criminal activity, which results in harm to individuals, states, and the international financial system. These negative consequences are particularly severe for developing countries with fragile financial systems.

1.3 The Financial Action Task Force (FATF[3]) and other international bodies have developed international norms to address money laundering and terrorist financing. These norms have focused largely (but not exclusively) on financial institutions as the primary gatekeepers to the financial system and have sought to reduce ML/TF risks through improved controls within financial institutions. Increased international efforts to strengthen financial regulatory systems followed the 2001 terrorist attacks in the U.S. and continued

[1] For the purposes of this document, "Money Laundering" refers to the process by which the proceeds of a crime are converted into assets which appear to have a legitimate origin; "Financing of Terrorism" refers to the provision or collection of funds, by any means, with the intention that they should be used, or in the knowledge that they are to be used, directly or indirectly, to carry out terrorist activities.

[2] A "Business Unit" or "BU" is defined as an organizational unit, division or group of individuals that report to a single supervisor and that engage in the same or a similar line of activity.

[3] The FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and to promote the effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

thereafter as terrorism attacks expanded internationally. Similar efforts followed the 2008 financial crisis. Currently, financial institutions are subject to enhanced scrutiny on AML/CFT issues and those financial institutions that fail to comply with these standards face significant regulatory penalties and reputational damage.

1.4 **AML/CFT Risks in IDB Operations and Activities.** As a multilateral development institution, the IDB has a unique duty to ensure that its operations and corporate transactions are not used to facilitate Money Laundering or Terrorist Financing. Moreover, the IDB is also the administrator of donor trust funds, for which it has a fiduciary responsibility to establish and comply with appropriate AML/CFT controls.

1.5 Because the Bank is a participant in the international financial system, ML/TF risks and the associated reputational impacts are inherent in its activities. ML/TF risks are present whenever the Bank deals with third parties including clients, donors, financial institutions, employees, retirees, corporate vendors, service providers, consulting firms and executing agencies.

1.6 However, there are important differences between the Bank's ML/TF risks and those of commercial financial institutions. The Bank does not take customer deposits and does not conduct transactions under the direction of its clients, except for direct payments to suppliers in its development operations. Therefore, many of the AML/CFT risks that commercial banks face do not apply to the IDB. In addition, the Bank is not subject to national AML/CFT laws and it does not fall under any specific AML/CFT regulatory regime. Nevertheless, the Bank seeks to comply with financial industry best practices and donor requirements in order to protect its reputation, maintain the business profile element of its credit rating and ensure its access to financial markets and donor contributions. With that in mind, this Framework establishes AML/CFT controls that are commensurate to the ML/TF risks that the IDB faces and considers the IDB's legal status as an international financial institution.

II. Managing ML/TF Risk

2.1 **Scope of Application.** This Framework is intended to manage: (i) the risk that the Bank could be used to facilitate Money Laundering or Terrorist Financing, and (ii) the reputational impact that may arise from conducting operations with entities and individuals associated with Money Laundering or Terrorist Financing or other criminal activity. The Framework requires that BUs apply AML/CFT controls when dealing with third parties, and in particular when transactions with third parties are contemplated. Specifically, potential transactions with the following third parties are subject to the controls set forth in this document:

(i) Bank clients;
(ii) Vendors, individual consultants, consulting firms and other providers to which the Bank is requested by a borrower, beneficiary or other party to make direct payments for goods and/or services;
(iii) Recipients of grants and/or technical cooperation operations;
(iv) Donors or third parties providing funds to be managed by the Bank;
(v) Vendors, individual consultants, consulting firms and other providers from which the Bank purchases goods or with which it contracts services, whether through corporate procurement or IDB-executed operational procurement;

(vi) Treasury counterparties and entities eligible for investment, banking, trading or cash management; and
(vii) IDB work force, including staff and complementary workforce.

2.2 The AML/CFT controls contemplated in this Framework generally are not applicable or apply in a simplified manner when the IDB engages in disbursements or other transactions directly with government entities in Sovereign Guaranteed Operations, depending on the type of counterparty, type of transactions and perceived risk.

2.3 This determination – and all other determinations regarding AML/CFT controls – will result from a two-step process: (i) an assessment of AML/CFT risks presented by different types of financial relationships, and (ii) a process by which business units, with the support of OII and RMG, will design controls that correspond to the risks presented by their operations.

2.4 **Risk Assessments**. This Framework reflects a risk-based approach, which means that enhanced vigilance and mitigation measures are applied where risks are greater, and simplified controls are applied where risks are lower[4]. This allows the Bank to allocate resources effectively and apply controls that correspond to the risk presented by each type of transaction. The Framework also seeks to follow the three lines of defense approach adopted by the Bank to manage its risks more broadly[5]. To implement this approach, each BU – with the support of OII and RMG – will conduct an AML/CFT risk assessment regarding its activities with third parties. In this risk assessment – which will be updated periodically with such frequency as determined during the risk assessment – each BU will:

(i) identify the business relationships it has with third parties, whether in connection with IDB operations (*e.g.*, loans, guarantees, non-reimbursable investment grants, technical cooperation operations, etc.) or corporate activities (*e.g.*, employee recruitment, corporate procurement, treasury operations, etc.)
(ii) assess whether and to what extent such relationships present ML/TF risk, taking into consideration factors such as the type of counterparty, the purpose of the business relationship, the type of product or transaction, etc.
(iii) prepare a risk matrix reflecting the results of its risk assessment, which will be incorporated into the risk matrix for the IDB.

2.5 **Determining AML/CFT Controls.** Based on the result of the risk assessment and the advice of OII and RMG, the BU will determine the appropriate AML/CFT controls for their different types of transactions with third parties and will implement and monitor such controls. Three types of AML/CFT controls are contemplated by this Framework: Sanctions Screening, Counterparty Due Diligence, and Know your Employee Due Diligence.

2.6 Sanctions Screening**.** The baseline control to be applied in all cases is sanctions screening, which involves comparing the identity of IDB Counterparties to lists of sanctioned entities and individuals. This control is intended to avoid funding or receiving funds from individuals or entities included in international sanctions lists. The IDB currently electronically screens Counterparties against the IDB Group's list of Sanctioned Firms and

[4] For example, this approach includes thresholds that exclude the application of controls to low risk transactions below certain monetary amounts.
[5] See GN-2547-13: Risk Taxonomy of the Inter-American Development Bank. June 2016 Update.

Individuals and the sanctions lists (hereinafter jointly referred to as the "Internationally Recognized Sanctions Lists") maintained by:

(i) the United Nations Security Council Committee (UN list);
(ii) the European Commission (EU list);
(iii) the Office of Foreign Asset Control (OFAC) of the U.S. Department of Treasury (OFAC list); and
(iv) the Treasury of the United Kingdom (UK list).

2.7 The IDB may consider, on a case-by-case basis, screenings against other international or national sanctions lists.

2.8 Counterparty Due Diligence. This control involves conducting due diligence over any IDB counterparty (whether an entity or an individual) who interacts financially with the Bank (a "Counterparty") to determine the nature and background of such Counterparty. BUs may incorporate counterparty due diligence ("CDD") controls as part of their existing onboarding procedures for new Counterparties if such controls are appropriate, based on the risk assessment described in section 5 above.

2.9 This process comprises the following:

(i) gathering and verifying information regarding the IDB Counterparty to detect risk indicators, and
(ii) assessing the risk that they present to the IDB in the context of the proposed transaction.

2.10 Where CDD controls are merited, based on the risk assessment described in section 5 above, BUs, with the support of OII, shall determine whether some or all of the following CDD controls shall apply:

(i) verifying the identity of the Counterparty using independent source documents, data or information.
(ii) identifying and screening through appropriate databases the Counterparty's beneficial owners, its directors and managers.
(iii) obtaining an understanding of the ownership and control structure of legal entities and legal arrangements.
(iv) determining the Counterparty's source of wealth and source of funds.
(v) obtaining information on the Counterparty's business and reputation.
(vi) verifying the Counterparty's criminal, compliance and enforcement history.
(vii) obtaining references, including personal or commercial references, or third-party reports.
(viii) identifying politically exposed persons ("PEPs") associated with the Counterparty.
(ix) assessing the AML/CFT controls of financial institution Counterparties and their compliance with applicable AML/CFT regulations.
(x) assessing any AML/CFT regulatory deficiencies in the Counterparty's jurisdiction.
(xi) interviewing Counterparty representatives and visiting the Counterparty's sites of operations.

2.11 The specific CDD controls applicable to each BU and the frequency with which such CDD measures should be updated shall be determined during the risk assessment described in Section 5. Such CDD controls shall be rolled out over time and become effective once

the corresponding BU has formalized them in an internal guideline as described in Section 19.

2.12 Know Your Employee (KYE) Due Diligence. This control involves conducting due diligence on Bank staff and complementary workforce. HRD and/ or BUs may incorporate KYE controls as part of their existing hiring procedures for new staff and complementary workforce if such controls are appropriate, based on the risk assessment described in section 5 above.

2.13 The KYE process may include the following:

(i) Gathering sufficient information to identify the individual.
(ii) Verifying employment history, criminal background checks and enhanced screening for PEPs.
(iii) Managing potential conflicts of interests and declarations of interests of potential employees.

2.14 **Control Implementation.** BUs will be responsible for conducting sanctions screenings prior to the commencement of any business relationship, and for updating such screenings periodically during the life of the business relationship, in accordance with the corresponding risk assessment.

2.15 The Finance Department (FIN) is responsible for (i) screening each payee (client and/or beneficiary) and financial intermediary immediately prior to executing a disbursement or payment, and (ii) screening all relevant payees and Counterparties daily, using an automated (batch) screening system.

2.16 BUs (including FIN with regards to transactions screenings) shall use the automated software system designated by OII to screen Counterparties. If those screens result in an apparent match, the BU shall take reasonable measures to gather additional information to exclude "false positives" (*e.g.* where the screen resulted in a match with an entry in the sanctions lists, that clearly applies to a different entity/person.)

2.17 **Monitoring and Escalation of Red Flags.** IDB staff responsible for carrying out AML/CFT functions shall remain alert for any ML/TF red flags that may arise through the application of AML/CFT controls, and shall immediately raise such red flags, along with any relevant information, to the BU's management and to OII for resolution. The presence of a red flag does not preclude the Bank from carrying out the proposed activity, but does require further analysis by OII, working with the BU to allow for an informed decision.

2.18 If OII determines that a match is positive, the Bank will generally refrain from making or receiving a payment or otherwise transacting with the individual or entity. However, if the BU intends to proceed with the transaction, the decisions regarding particular payments or other interactions should be elevated to the BU's Manager or above. OII will report regularly to the ORMC regarding the resolution of any positive matches.

2.19 While it is not possible to provide a comprehensive list of red flags, the following are provided as examples.

2.20 <u>Red Flags regarding Sanctions Screening</u>

(i) Counterparty whose identity or identity of its affiliates/related entities appears on a sanctions list.
(ii) Counterparty whose identity is significantly similar to a name on a sanctions list.

2.21 Red Flags regarding other aspects of Counterparty Due Diligence

(i) Counterparty that uses a bank account in jurisdictions other than its home jurisdiction.
(ii) Counterparty that requests payment to, or makes payment from, the account of a third party.
(iii) Information indicating that a Counterparty may have engaged in criminal activity.
(iv) Information indicating that a Counterparty is linked to a politically exposed person.
(v) Counterparty for which it is not possible to determine the identity of its beneficial owners.

2.22 Red Flags regarding other aspects of Know Your Employee Due Diligence. Prospective employees – or previous employers of prospective employees – that have been alleged or found to have committed crimes or other violations involving ethical or financial misconduct.

2.23 **Ongoing Assessments.** OII will undertake periodic sampling reviews of the controls implemented by BUs (including FIN with respect to transactions screenings). These sampling reviews are intended to assess the effectiveness of the controls and validate the correct application of this Framework.

2.24 **Record Retention.** BUs and OII shall be responsible for maintaining, for at least 5 years, all records pertaining to all transactions and all records relating to the application of CDD and KYE controls, including any information related to any analysis undertaken in connection with any transaction or counterparty.

2.25 **Coordination with other risk management efforts and controls.** To the extent that existing controls may serve to mitigate AML/CFT risks, the Bank will explore synergies to reduce costs and increase control effectiveness.

III. Roles and Responsibilities

3.1 **General Responsibilities.** IDB Management shall promote a culture of compliance in relation to AML/CFT. IDB staff and complementary workforce with specific responsibility for administering AML/CFT controls shall also be responsible for reporting AML/CFT red flags to OII.

3.2 **OII's AML/CFT Compliance Function.** OII is responsible for performing an AML/CFT compliance function, according to which it will:

(i) lead the ML/TF risk assessment process in conjunction with each BU,
(ii) define, in consultation with each BU the controls that the BU should apply to manage identified ML/TF risks,

(iii) serve as an advisory resource to BUs and relevant committees regarding the management of ML/FT risks,
(iv) provide advice to BUs regarding the assessment of and reaction to specific ML/FT risks,
(v) conduct reviews and investigations of ML/FT red flags brought to its attention, and issue recommendations to BUs,
(vi) determine how to record and manage false positives (*e.g.*, by adopting whitelists),
(vii) ensure, to the extent practicable, consistent application of the Framework across different BUs and activities,
(viii) develop AML/CFT training programs for relevant staff, together with the Knowledge and Learning Sector (KNL).
(ix) liaise with external stakeholders regarding inquiries about the AML/CFT controls implemented by the Bank,
(x) coordinate with the IT department regarding the establishment, maintenance, integration and calibration of IT systems for applying ML/FT controls, as well as ensuring that BUs have access to software necessary for them to perform AML/CFT controls.
(xi) conduct periodic sampling reviews of the monitoring performed by BUs and FIN,
(xii) adapt systems (*e.g.*, whitelists) to manage false positives,
(xiii) keep records, for at least five years, of all red flags submitted to it by BUs, all accompanying documentation, and the basis and justification for each recommendation issued, and
(xiv) stay abreast of international developments and best practices with regard to AML/CFT.

3.3 **Responsibilities of Business Units.** Each relevant BU shall:

(i) cooperate with OII and RMG in the performance of ML/FT risk assessments regarding the BU's business relationships with third parties, whether in connection with IDB operations or corporate activities,
(ii) discuss with OII the appropriate AML/CFT controls for its activities, based on the risk assessment, and
(iii) implement and monitor such controls by:

a. engaging OII to periodically update the AML/CFT risk assessment and reassess the adequacy of the controls applied,
b. designating employees who will be responsible for gathering information or otherwise carrying out activities required for implementation of AML/CFT controls,
c. escalating ML/FT red flags to OII,
d. liaising with counterparties to obtain information necessary to assess ML/FT risks,
e. maintaining, for at least five years, all records pertaining to all transactions and all records obtained through CDD measures, including any information related to any analysis undertaken in connection with any transaction or counterparty,
f. assessing any additional workload triggered by implementation of these controls, and any additional support that the BU may require, and
g. ensuring, with the support of the Legal Department, that agreements with third parties – including standard forms of agreement – incorporate provisions that reflect the principles of this Framework and protect the IDB

from any liability arising from any measures taken to mitigate ML/TF risks (*e.g.*, nonpayment to entities and individuals included in the Internationally Recognized Sanction Lists.)

3.4 **Responsibilities of RMG.** To mitigate operational risk that could arise from the inadequacy of this Framework or the BU's risk assessments, RMG will:

(i) facilitate, with OII, an initial assessment of AML/CFT risks and controls and its regular updates,
(ii) periodically assess the adequacy of the design of AML/CFT controls and their operative effectiveness, and
(iii) periodically assess the adequacy of this Framework.

RMG will also coordinate with OII and KNL the delivery of AML/CFT training programs to relevant staff.

3.5 **Internal Audit (AUG)** will evaluate the implementation of this Framework pursuant to the Charter of the Office of the Executive Auditor.

3.6 **Operational Risk Management Committee.** The Operational Risk Management Committee (ORMC) will be responsible for overseeing the implementation and execution of the Framework across the Bank. OII, in coordination with RMG, will report regularly to the ORMC regarding: (i) the results of sampling reviews; (ii) the number and resolution of any positive matches identified through screening; and (iii) other issues regarding the management of AML/CFT risks and on their respective responsibilities assigned by the Framework.

3.7 The ORMC will (i) receive and consider Framework implementation reports submitted by OII and RMG, and (ii) provide recommendations to ensure that the Framework is adequately and consistently implemented across the Bank.

IV. Dissemination, Effectiveness, and Training

4.1 **Dissemination.** The IDB shall make this Framework available to the public on its website and through any other channels deemed appropriate.

4.2 **Effectiveness.** The AML/CFT controls to be implemented by each BU will be defined through a risk assessment that will be conducted with each BU and will become applicable upon (i) the provision of adequate training to relevant personnel in the BU, and (ii) the formalization of the relevant controls in an internal guideline, which shall be approved by each BU's head. The controls contemplated by this Framework should be fully implemented within two years from its approval.

4.3 **Training activities for employees.** OII, with the support of RMG and KNL, will offer training to employees on the implementation and application of this Framework. The main objective of the training will be to strengthen employees' understanding, with respect to AML/CFT risks and applicable controls.