2015
COMPLIANCE POLICY

CARIBBEAN DEVELOPMENT BANK

STRATEGIC FRAMEWORK FOR INTEGRITY, COMPLIANCE AND ACCOUNTABILITY

PILLAR II

COMPLIANCE POLICY

To combat Money Laundering, the Financing of Terrorism
and for monitoring in order to avoid violations of Financial Sanctions

MAY 2015

TABLE OF CONTENTS

COMPLIANCE POLICY

A Policy to Combat Money Laundering, Financing of Terrorism and for monitoring in order to avoid violations of Financial Sanctions

1. INTRODUCTION

1.01 The Caribbean Development Bank (the Bank) adheres to the highest standards of integrity, ethics, compliance, transparency and accountability, with zero tolerance for money laundering, financing of terrorism and similarly corrosive conduct.

1.02 The Bank has introduced a comprehensive Strategic Framework for Integrity, Compliance and Accountability (the Strategic Framework) and established the Office of Integrity, Compliance and Accountability (OICA) to operationalise and manage the Strategic Framework. This Compliance Policy (the Policy) is issued pursuant to the Strategic Framework.

2. KEY DEFINITIONS[1]

2.01 For the purposes of this Policy:

Affiliate	means in relation to an entity, its direct or indirect controller, shareholder, owner, parent, or subsidiary, or any other entity it controls or with which it is under common control.
Allegation	means an unproved assertion against someone related to suspected wrongdoing.
Associate	means a person who is publicly known or actually known to the Bank to be closely connected to a Politically Exposed Person.
Beneficial Owner	means the person who ultimately owns and controls an account, Property or other asset, or who exercises ultimate control over a legal person or legal arrangement.
Business Relationship	means any arrangement between the Bank and any person for conduct by the Bank of financial transactions on a regular basis.
Compliance	means the Bank's adherence to this Policy and the procedures issued pursuant to it, which adopt relevant rules, regulations, standards, codes and norms to combat Money Laundering and the Financing of Terrorism, and for monitoring in order to avoid violations of Financial Sanctions.
Correspondent Bank	means a bank involved in the provision of Correspondent Banking services.
Correspondent Banking	means the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank").
Counterparty	means any individual or entity seeking funding for a Project or who is being funded by a Bank-financed operation or Project or other activity of the Bank, and includes any supplier, contractor or consultant for, or beneficiary of, a Project and any Affiliate thereof who has engaged directly or indirectly with the Bank

[1] Adopted as far as possible from the FATF Recommendations (2012)

	including through its policies and procedures for external project-related procurement or internal or corporate procurement by the Bank for its own account. The term "Counterparties" shall be construed to mean more than one Counterparty
Country	means a territory or jurisdiction recognised as such under international law. The term "Countries" used in this Policy shall be construed accordingly to mean territories or jurisdictions.
Customer/Counterparty	means any individual or entity seeking funding for a Project or who is being funded by a Bank-financed operation or Project or other activities of the Bank, and includes any supplier, contractor or consultant for, or beneficiary of, a Project and any Affiliate thereof who has engaged directly or indirectly with the Bank including through its policies and procedures for external project procurement or internal corporate procurement by the Bank for its own account. The term "Counterparties" shall be construed to mean more than one Counterparty.
Customer/Counterparty Due Diligence	or CDD, means the application of certain measures to better understand a customer/counterparty. CDD is a process, not a single activity. It can be conducted in conjunction with other risk mitigating activities, e.g. Integrity Due Diligence.
Director	means a member of the Bank's Board of Directors. Every reference to a "Director" means the Director and his/her alternate and advisors.
Due Diligence	means activities and investigation intended to obtain adequate knowledge about a Person or Counterparty including their Business Relationships, Transactions, funding sources, and other business activities to help determine that they are not connected to Money Laundering/Financing of Terrorism (ML/FT) and other illicit practices. Due Diligence is conducted using measures that are intended to be effective and proportionate to the risks identified.
Enhanced Due Diligence	or EDD, means elevated due diligence measures usually applicable to Persons classified as high risk.
Financial Action Task Force	or FATF, means the intergovernmental body that develops and promotes policies to protect the global financial system against Money Laundering and Terrorist Financing.
Financial Sanctions	means the internationally recognised targeted sanctions restricting the conduct of financial business as issued by national governments, and international and regional organisations, the deliberate violation of which may damage the Bank's reputation.[2] Such targeted sanctions are imposed against countries, regimes, entities, groups and individuals particularly money launderers, terrorists and narcotics traffickers who may

[2] Internationally recognized financial sanctions lists to which IFIs will have regard are those issued by the Office of Foreign Assets Control (OFAC) of the United States of America, the United Kingdom, the United Nations, the European Union and the World Bank.

	also seek directly or indirectly to engage with the Bank. Financial Sanctions include asset freezing measures and prohibitions to prevent funds or other financial assets from being made available, directly or indirectly, for the benefit of money launderers, terrorists and narcotics traffickers.
Financing of Terrorism	or FT, means providing or collecting funds with the intention that they be used, or in the knowledge that they are to be used for the financing of Terrorists, terrorist organisations and Terrorist Acts. Financing of Terrorism is also referred to as Terrorist Financing.
Integrity Due Diligence	means Due Diligence that concerns Integrity conducted on a Customer/Counterparty or with respect to a Transaction;
Money Laundering	or ML, means the use of any system, process, procedure or operation of the Bank directly or indirectly for the acquisition, possession, use or processing of proceeds derived from criminal activities or from participation in criminal activities in order to legitimise them and disguise their illegal origin. [3] This process may more specifically be defined as the: (a) conversion or transfer of property, knowing[4] that such property is derived from criminal activities or from an act of participation in any such activities 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 criminal activities to evade the legal consequences of his actions; (b) 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 a criminal offense; and (c) acquisition, possession or use of property, knowing at the time of receipt that it was derived from criminal activities or from participation in a crime.
Politically Exposed Persons	or PEPs, are persons who are or have been entrusted with prominent public functions and with whom the Bank is likely to interact. PEPs are defined as individuals who are or have been entrusted with prominent: (a) public functions by a country, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials, senior

[3] FATF Recommendations (2012).
[4] In the context of this definition of Money Laundering, knowledge can be derived from objective factual circumstances.

executives of state owned corporations, important political party officials; and

(b) functions by an international organisation which includes members of senior management, directors, deputy directors and members of the board or equivalent functions.

PEPs include but are not limited to Heads of State (President); Heads of Government (Prime Minister); Senior Members of the Legislature (e.g. President of the Senate; Speaker of the House and Deputy Speaker); Judicial Officials (e.g. Judges and Magistrates); Senior Politicians (e.g. Members of Parliament; Government Ministers; Opposition Leader; Parliamentary Secretaries; and Mayors); Senior Government officials (e.g. Permanent Secretaries; Chief Technical Officers; Ambassadors or High Commissioners; Commissioners of Police and their Deputies and Assistants; Military Officials; Senior executives of State-owned corporations; and Senior political party officials (e.g. Chairman, Political Leader and Deputy Political Leader). PEPs do not include individuals in a medium or subordinate rank to the categories outlined above.

Proceeds means any property derived from or obtained, directly or indirectly, through the commission or suspected commission of an offence under national laws.

Person means any individual or entity and shall include a Director, a member of Staff, a body corporate, a trust and any other entity legally recognised as having the capacity to contract.

Project means any activity which the Bank has financed or committed to finance from its Ordinary Capital Resources or Special Funds Resources, trust funds or from other funds administered by the Bank.

Property means any asset of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such asset.

Reputationally Exposed Persons or REPs, means Persons against whom there is adverse publicity in relation to matters that specifically concern or question their ethics, integrity or financial conduct relating to ML/FT that have the potential to introduce or heighten operational risks, particularly reputational risks for the Bank.

Sanctions List means any list of sanctioned Persons maintained by OICA, as updated from time to time and as may be provided for in the Bank's Compliance Procedures.

Shell Bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective

	consolidated supervision. In this context physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Staff	means the management, (including the President and Vice-Presidents), professional and support staff, temporary employees, other contracted employees, consultants, secondees, interns and personnel on exchange assignments without regard to their position, rank, title, duration of contract with, or length of service to, the Bank.
Suspicious Transaction	means a Transaction about which any Person suspects or has reasonable grounds to suspect that the funds involved are the Proceeds of a criminal activity or are related to the Financing of Terrorism.[5]
Terrorist	means any natural person who participates in, contributes to, organises, commits, or attempts to commit, a Terrorist Act.
Terrorist Act	means: (i) an act which constitutes an offence within the scope of, and as defined in, treaties from time to time recognised by the Financial Action Task Force; and (ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict when the purpose of such act by its nature or context is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act.
Transaction	means an engagement entered into by the Bank for its own internal account and treasury operations and for its external Bank-financed operations, including both its public sector operations and its private sector operations.

3. PRINCIPLES

3.01 The Strategic Framework is founded on the following four principles which also underpin this Policy:

(a) integrity;

(b) accountability;

(c) excellence; and

(d) transparency.

4. PURPOSE

4.01 This Policy enables the Bank to promote Compliance with internationally recognised standards for Anti-Money laundering and Countering the Financing of Terrorism (AML/CFT) and thereby enhance its governance and stewardship of development resources and the protection of its reputation.

[5] See FATF Recommendation 20. Criminal activity refers to: (a) all criminal acts that would constitute a predicate offence for ML in the relevant country; (b) at a minimum those offences that would constitute a predicate offence as required by the FATF Recommendation 3.

4.02 Specifically, this Policy outlines the Bank's own standards for the prevention and detection of Money Laundering and the Financing of Terrorism (ML/FT) and for monitoring in order to avoid violations of Financial Sanctions. It enables the Bank to exercise robust oversight and management of ML/FT and Financial Sanctions risks to ensure that the flow of funds to, and from, the Bank and the Bank's own business and assets are not tainted by ML/FT and to ensure that the Bank and its financial counterparties have established adequate mechanisms to protect themselves from ML/FT risks.

5. ROLE OF OICA

5.01 OICA does not perform frontline work at the operations level but will assist Staff at the operations level. Primary responsibility for the identification, monitoring, mitigation and remediation of ML/FT and Financial Sanctions risks in frontline operations work on Transactions lies with the functional heads of each of the Bank's internal units, divisions, departments and offices.

5.02 In addition to its oversight obligations OICA works to assist all units, divisions, departments, and offices that have primary responsibility for, and conduct of, portfolio management, to collaborate promptly to mitigate and remediate ML/FT and Financial Sanctions risks.

5.03 OICA leads the collaboration across all relevant units, divisions, departments and offices in the Bank to:

(a) conduct ongoing risk-based monitoring, mitigation and remediation of ML/FT and Financial Sanctions risks;

(b) respond to potential ML/FT vulnerabilities;

(c) respond to queries from Correspondent Banks and other financial institutions conducting Due Diligence on the Bank; and

(d) ensure that as far as possible the Bank does not knowingly violate Financial Sanctions during its operations.

5.04 OICA shall collaborate with other International Financial Institutions (IFIs) and development partners in outreach programmes and for the development of international best practices to enhance the effectiveness of this Policy and the procedures issued pursuant to it.

6. GENERAL APPLICATION OF THIS POLICY

6.01 This Policy is expected to be applied broadly and in a manner that takes account of factors such as the specific type of Transaction and the nature and level of risks involved.

6.02 Application of this Policy and the procedures issued pursuant to it will at times require judgment, particularly about the need to escalate concerns internally and to keep information confidential.

7. SCOPE OF APPLICATION - ACTIVITIES

7.01 This Policy applies to all Transactions.

7.02 This Policy applies to the conduct of Customer/Counterparty Due Diligence and investigations related to all of the Bank's internal and external activities particularly with respect to ML/FT and Financial Sanctions and the risks arising from the receipt of funds by the Bank and use of funds provided by the Bank as lender, grantor, donor or otherwise in or for projects financed by the Bank, the Bank's external project-related procurement and internal or corporate procurement.

8. SCOPE OF APPLICATION - PERSONS

8.01 This Policy covers due diligence and investigations conducted on any of the parties listed below and any person connected to them (each a Person and, where applicable, a Counterparty or Counterparties):

(a) financial parties engaging with the Bank on any Transaction including as financial intermediaries;

(b) borrowers, contractors, sub-contractors, consultants, vendors, suppliers, service providers, project promoters, sponsors, beneficiaries and, in general, relevant persons or entities dealing with the Bank in its own internal or corporate procurement or in external or project-related procurement or otherwise involved in activities financed by the Bank;

(c) counterparties and other organisations or entities with which the Bank deals in its borrowing, lending, grant-financing, equity, treasury or accessing of donations activities; and

(d) parties not mentioned above but otherwise bound by special provisions, including integrity clauses, in the Bank's contracts and technical cooperation or assistance agreements.

9. RISK-BASED APPROACH

9.01 This Policy is consistent with the Bank's risk-based approach including to operationalising Compliance as articulated in the Strategic Framework. The Bank's risk-based approach sets the foundation for the Bank to undertake due diligence, mitigation and remediation measures commensurate with the risks identified, and to enable management to make tailored decisions about how to effectively allocate its resources.[6]

9.02 The procedures issued pursuant to this Policy will, where relevant, be underpinned by appropriate risk assessments. These assessments will enable the Bank to better identify and mitigate key ML/FT and Financial Sanctions risks before they materialize and help to determine how the Bank should manage their consequences or remediate them if they arise.

10. RISK-BASED KNOW YOUR CUSTOMER/COUNTERPARTY (KYC) AND DUE DILIGENCE

10.01 Pursuant to this Policy, the Bank adopts a risk-based approach to designing its KYC and CDD procedures.

11. KNOWING THE CUSTOMER/COUNTERPARTY

11.01 OICA will work to ensure that the Bank, as far as possible and as necessary, knows any material Counterparty and where applicable the Persons exercising effective control over that Counterparty.

11.02 Pursuant to this Policy the Bank will issue procedures to enable it to ascertain, as far as possible and obtain information on, the purpose, intended nature and full scope of its Business Relationships with Counterparties.

[6] This is consistent with FATF Recommendation 1 and the Interpretive Note to Recommendation 1. See FATF recommendations 2012 p.31.

12. CUSTOMER/COUNTERPARTY DUE DILIGENCE

12.01 OICA will work to ensure that the Bank applies risk appropriate KYC procedures for CDD, which are measures undertaken to better understand a Customer/Counterparty, including for the identification and understanding of ownership and the control (effective) structure of a Customer/Counterparty and generally to:

(a) avoid anonymous and fictitious Customers/Counterparties;

(b) understand appropriate Business Relationships with third parties related to the Customer/Counterparty; and

(c) monitor ongoing Business Relationships with Customers/Counterparties.

12.02 The Bank will undertake risk-appropriate measures for CDD when:

(a) establishing Business Relationships in new Transactions;

(b) reviewing current Transactions and monitoring established relationships with Counterparties;

(c) there is suspicion of ML/FT or other connection to ML/FT in relation to any new or current Transaction; or

(d) the Bank has doubts about the veracity or adequacy of Counterparty identification data being provided, whether for a new or established Transaction.

12.03 The Bank will ensure that as far as possible legal terms, conditions and covenants used in Transactions are appropriate to the level of risk and suitably crafted to mitigate any potential reputational and other financial risks from ML/FT that may arise from the engagement.[7]

13. BENEFICIAL OWNERSHIP

13.01 The Bank shall work to ensure as far as possible, accurate identification of the ultimate legal and beneficial ownership of its Customers/Counterparties and check their legitimacy and repute using all appropriate measures to do so including reliance on independent source documents (whether public or private), data or information from the Counterparty or other internal and external data sources.

13.02 The Bank will investigate and take appropriate steps to avoid, where possible, current or proposed Transactions about which there are Allegations, suggestions, suspicions or risks that opaque corporate structures or corporate vehicles (regardless of the degree of sophistication or complexity) are being misused to disguise beneficial ownership of a Customer/Counterparty.

14. PERSONS CONVICTED OR SUBJECT TO CRIMINAL INVESTIGATION

14.01 The Bank will not engage in Transactions nor enter into relationships with convicted money launderers, Terrorists or any Person convicted of a serious criminal offence related to ML/FT.

14.02 The Bank shall take appropriate steps to avoid engaging in Transactions and relationships with Persons under investigation for a serious criminal offence related to ML/FT.

[7] This will enable the bank to have contractual recourse to address ML/FT conduct through conditions precedent, representations and covenants. For instance there may be a provision to ensure that counterparties and anyone acting on their behalf represent that they have not engaged in nor are they in breach of any applicable law relating to money launder or financing of terrorism.

15. SANCTIONED AND DEBARRED PERSONS

15.01 The Bank may monitor Sanctions Lists, conduct risk assessments and determine in its own discretion whether and how to engage in Transactions or relationships with any Person appearing on a Sanctions List and/or otherwise debarred by another International Financial Institution (IFI), including any Person against whom: (a) a Financial Sanction has been imposed or was imposed and subsequently removed, regardless of the reason for such removal; and (b) an adverse public statement has been issued by a country, international organisation or other recognised sanctioning body.

15.02 If the Bank engages with any sanctioned or debarred person, the Head of OICA shall notify the Committee of the Board of Directors with oversight for integrity, ethics, Compliance and accountability (Oversight Committee) in its periodic report to the Oversight Committee.

16. PERSONS LINKED TO ORGANISED CRIME

16.01 The Bank will not engage in Transactions where there is relevant credible evidence of existing links to organised crime and criminal activities. Relevant credible evidence may be provided by official sources including law enforcement and national authorities, international organisations and disinterested persons.

17. PERSONS CONVICTED OF ILLEGAL TAX PRACTICES

17.01 The Bank will not engage in Transactions nor enter into relationships with any Person convicted of illegal tax practices related to ML/FT.

18. POLITICALLY EXPOSED PERSONS

18.01 The Bank will pay special attention to PEPs and their Associates with whom the Bank engages and take steps to ensure that PEPs do not exercise any form of effective control over any privately-owned Counterparties.[8]

19. REPUTATIONALLY EXPOSED PERSONS

19.01 The Bank shall pay special attention to REPs.

20. HIGH RISK PERSONS

20.01 The Bank will pay special attention to (and undertake risk appropriate measures, including choosing not to engage with) any Person or any Transaction classified by OICA and/or the Office of Risk Management (ORM) to be "high risk" for the purposes of this Policy and the procedures issued pursuant to it.

20.02 The Bank will pay special attention to Transactions undertaken in sectors classified by OICA and/or the ORM to be "high risk".

20.03 The Bank will take into account of any relevant mitigating factors for its classification of a Person, Transaction or sector as "high risk".

[8] The definition of PEPs for the purposes of this Policy is consistent with the FATF-Recommendations as currently used and which may be amended from time to time by FATF and adopted by OICA.

21. MONITORING PROJECTS WHERE PERSONS ARE SUBJECTED TO ENHANCED DUE DILIGENCE

21.01 Where a Person involved with a Transaction, project of other engagement has been subjected to EDD and the Bank proceeds with the Transaction project or other engagement, the Bank may monitor any ML/FT risks and any relevant Financial Sanctions for the life of the Transaction, project or other engagement.

22. USE OF FICTITIOUS NAMES

22.01 The Bank shall not conduct business with any anonymous Counterparty or a Counterparty that uses a fictitious name.

23. SUSPICIOUS TRANSACTIONS

23.01 The Bank shall take pre-emptive steps to ensure that it avoids engaging in Transactions which can reasonably be believed to be regarded as Suspicious Transactions.

23.02 All Transactions reasonably believed to be Suspicious Transactions shall be immediately reported to OICA.

23.03 The Bank is not subject to any law or other regulatory requirement to report Suspicious Transactions to any external competent authorities however, OICA may, after consulting with the President, notify the competent authority in any Member Country or other country of the existence of a Suspicious Transaction without prejudice to the privileges, rights and immunities of the Bank as an international organisation.[9]

24. SHELL BANKS

24.01 The Bank shall not conduct Transactions with or on behalf of Shell Banks and their Affiliates.

25. CORRESPONDENT BANKS

25.01 The Bank shall conduct appropriate risk-based KYC and CDD measures when dealing with Correspondent Banks including the undertaking of measures to:

(a) gather sufficient information about the Correspondent Bank's business to (i) determine from public information the reputation of the Correspondent Bank; and (ii) to understand fully the nature of its business and quality of its supervision/regulation including whether the institution has been the subject of an investigation or regulatory action related to ML/FT;

(b) assess the Correspondent Bank's AML/CFT controls including through the use of periodic surveys and questionnaires; and

(c) ensure that the Correspondent Bank does not permit its accounts to be used by Shell Banks.

[9] The competent authority to be notified in these circumstances is typically a Financial Intelligence Unit or Commissioner of Police.

26. COUNTERPARTY COMPLIANCE[10]

26.01 The Bank shall apply appropriate procedures to confirm counterparty compliance with internationally accepted ML/FT standards and best practices.

26.02 Where applicable the Bank shall ensure that its Counterparties which are regulated financial institutions and those with whom it holds correspondent banking relationships are compliant with their local laws and regulations and with international standards and best practices for ML/FT compliance.[11]

27. NOTIFICATION OF COMPLIANCE

27.01 The Bank may from time to time, notify its Counterparties of its own compliance status.[12]

28. FINANCIAL SANCTIONS

28.01 The Bank shall take appropriate steps to monitor Financial Sanctions on its Sanctions List in order to avoid deliberately violating those Financial Sanctions which are relevant to the Bank's role and functions as an IFI.

29. RETENTION OF RECORDS

29.01 The Bank shall apply risk appropriate procedures for dealing with retention of records.

29.02 The Bank shall maintain for at least ten (10) years all necessary records on Transactions and information obtained through CDD measures or under this Policy.[13]

30. TRAINING

30.01 OICA will ensure that training is provided to the Directors and Staff to enhance awareness about this Policy and to ensure its effectiveness.

31. REVIEW

31.01 The Board of Directors through its Oversight Committee, may commission a review of this Policy, within the first three years of its operationalisation and at least once every five years thereafter, as necessary, to help ensure its effectiveness.

32. OVERSIGHT AND IMPLEMENTATION

32.01 Pursuant to the Strategic Framework, OICA directly oversees this Policy.

32.02 Management of the Bank bears primary responsibility for working with OICA to ensure effective implementation of, and adherence to, this Policy.

---

[10] Consistent with international best practice including the Wolfsberg Principles, Definitions and Questionnaire.

[11] For this purpose the procedures may provide for the Bank to conduct any appropriate ML/FT due diligence on such Counterparties including requiring them to complete and submit to the Bank answers on the Bank's questionnaire that requests such relevant information as provided for in the procedures issued pursuant to this Policy.

[12] The procedures may provide that where applicable the Bank may publish a copy of its own completed ML/FT Questionnaire or provide a copy of its own completed ML/FT Questionnaire to an enquiring Counterparty to assist that Counterparty with its due diligence of the Bank.

[13] The procedures may provide for such records to be maintained in an appropriate format (including electronic scans) sufficient to permit, as far as possible, reconstruction of individual Transactions.