Integrity Due Diligence Policy

Canada Infrastructure Bank

1. Introduction

1.1 Status of the Canada Infrastructure Bank

1.1.1 The Canada Infrastructure Bank ("**CIB**") is a federal Crown corporation established under the *Canada Infrastructure Bank Act*. Its mandate is to invest, and seek to attract investment from private sector and institutional investors, in infrastructure projects in Canada or partly in Canada that will generate revenue and that will be in the public interest.

1.1.2 The CIB operates independently from the federal government in its day-to-day operations and investment decisions, while remaining accountable through its Board of Directors. The Board of Directors is responsible for overseeing the CIB's strategic direction, approving investments and ensuring compliance with its legislative mandate.

1.1.3 As a federal Crown corporation, the CIB is not designated as a reporting entity under the Proceeds of Crime (*Money Laundering*) and *Terrorist Financing Act* ("**PCMLTFA**"). However, as a Crown corporation ultimately accountable through the Minister to Parliament for the conduct of its affairs, the CIB has a legal, corporate and ethical responsibility to promote the highest ethical standards of business conduct throughout its activities. The CIB has deliberately aligned its practices (including Know Your Client ("**KYC**") standards and requirements) with those adopted by comparable Crown corporations as a matter of best practice, to ensure risk-appropriate controls, effective oversight and public confidence in the CIB's execution of its mandate.

1.2 Purpose of the Integrity Due Diligence Policy

1.2.1 As stewards of public resources, the CIB is committed to implementing strong processes and controls to promote the highest ethical standards of business conduct throughout its activities. Money laundering, terrorist financing, transacting with sanctioned individuals or organizations, corruption and fraud are serious crimes that affect the security and safety of all Canadians.

1.2.2 The purpose of this Integrity Due Diligence Policy (the "**Policy**") is to implement specific measures to identify, mitigate and manage Integrity Risks in accordance with best practices and the Government of Canada's laws and regulations intended to prevent money laundering, financing terrorism or other financial crimes, including bribery, fraud and corruption. Although the procedures and controls established under this Policy cannot eliminate all Integrity Risks, consistent application of this Policy will contribute to effective risk management and prudent decision-making.

1.3 Scope and related instrument

1.3.1 This Policy establishes the guiding principles, risk tolerance and governance framework for:

- risk acceptance, authority levels;
- the use of third-party due diligence providers; and
- escalation thresholds for managing potential Integrity Risks with regards to investment decision-making.

Specific operational requirements are set out in the Know Your Client (**KYC**) Due Diligence Procedure (the "**KYC Procedure**"), including the processes, tools and methodology for conducting Counterparty Identification and Verification, Enhanced Due Diligence, ongoing monitoring and record-keeping standards.

1.3.2 This Policy applies to all Personnel. In addition to this Policy, the guidelines regarding Personnel's general expectations regarding Integrity and ethical business conduct are set out in the **Code of Conduct for Personnel**.

1.3.3 The capitalized terms and other common terms used but not otherwise defined in this Policy are defined in section 5.

2. Risk tolerance

2.1 Meaning of "Integrity" and "Integrity Risk"

2.1.1 For the purpose of this Policy, the terms "**Integrity**" and "**Integrity Risk**" are defined as follows:

- "**Integrity**" refers to the Counterparty's compliance with laws, regulations, rules and codes of conduct governing ethical business practices and transparency. This includes managing conflicts of interest and preventing money laundering, terrorist financing, sanctions violations, corruption and fraud in its operations and activities.
- "**Integrity Risk**" refers to the risk of facing legal or regulatory penalties, material financial losses or reputational harm due to the failure to comply with laws, rules and standards related to Integrity. This includes risks arising from business dealings with Counterparties involved in money laundering or terrorist financing, sanctions violations, corruption or fraud, tax evasion or aggressive avoidance, opaque corporate structures, improper political influence, or other unlawful or unethical conduct.

2.2 Risk appetite and the CIB's expectations of counterparties

2.2.1 Consistent with the CIB's Risk Appetite Statement adopted by the Board of Directors: *"The CIB's appetite for legal, regulatory, ethics and compliance risk is low. The CIB has no appetite for any breaches of the law, regulation, professional standards, negligence, corruption or fraud. The CIB is committed to maintaining the highest standards of integrity, compliance and ethics. The CIB manages these risks through policies and processes, including counterparty due diligence, reputational risk assessments and anti-money laundering rules to promote high ethical and professional standards and protect the integrity of the CIB, as well as the confidence in the CIB."*

2.2.2 The CIB expects all Counterparties, including their agents and representatives, to conduct business in compliance with the applicable laws, rules and regulations of the jurisdictions in which they operate, and to take all appropriate measures to observe the highest standards of Integrity. The CIB will not transact, directly or indirectly, with individuals, entities and/or restricted countries designated in applicable Canadian government money laundering, terrorist financing, sanctions lists or United Nations resolutions. Moreover, the CIB will not knowingly transact business with Counterparties who offer, give or accept bribes or participate in any other form of corruption. The CIB requires that all Counterparties disclose promptly to the CIB any known issues of non-compliance with this Policy.

2.2.3 To mitigate Integrity Risk, the CIB has established risk-based controls that are proportionate to the nature, scale and complexity of the CIB's activities and the groups of persons and entities with whom the CIB transacts business. Not all Integrity

Risks are binary or outcome-determinative. Where Integrity Risks are identified, the CIB will determine based on the Inherent Integrity Risk and Residual Integrity Risk assessed and the effectiveness of proposed risk mitigations. Decision outcomes include:

- Proceeding with the transaction;
- Proceeding with conditions and/or enhanced monitoring where the Integrity Risk is acceptable or within the CIB's risk tolerance;
- Pausing pending additional information or Enhanced Due Diligence; or
- Not proceeding with the transaction or terminate the transaction/relationship with a Counterparty where the Integrity Risk is outside the CIB's risk tolerance, unacceptable, or the Counterparty provides information that is materially false, misleading or cannot be reasonably corroborated.

2.2.4 Reputational risk is assessed in light of the CIB's legislated mandate and accountability to Parliament. The CIB may determine that a transaction presents unacceptable Integrity Risk based on credible information that could materially impair public confidence in the CIB or the CIB's ability to carry out its mandate, even where the conduct does not result in criminal conviction or regulatory penalty.

3. Governance – Roles and responsibilities

3.1 Three Lines of Risk Governance

3.1.1 The CIB has adopted the Three Lines of Risk Governance Model designed to ensure a balance between those involved in taking and managing risk (1st Line), those responsible for risk policy setting and independent oversight (2nd Line) and those providing assurance (3rd Line). The roles and responsibilities for the management of Integrity Risks are described in this Policy and the KYC Procedure.

3.2 Chief Executive Officer (First Line of Defence)

3.2.1 The Chief Executive Officer ("**CEO**") is accountable to the Board of Directors for the management of the legal and reputational risks associated with Integrity Risks. The CEO is the decision authority for (i) transactions assessed as presenting Residual Integrity Risk outside of the CIB's risk tolerance; (ii) any decision to proceed with a Counterparty where an exception under section 4.3 of this Policy is requested; and (iii) any decision to decline or terminate a relationship with a Counterparty due to Integrity Risk concerns.

3.2.2 The CEO is also responsible for providing leadership to ensure appropriate measures and sufficient resources are in place to identify, mitigate or manage Integrity Risk in accordance with industry standards. To this end, the CEO has designated the Chief Legal and Information Officer as the compliance officer (the "**CAMLO**") responsible for the Policy, including its development, implementation and administration.

3.3 Personnel (First Line of Defence)

3.3.1 Personnel are responsible for complying with this Policy and the guidelines set in the **Code of Conduct for Personnel**, including promoting transparent business practices and ensuring the highest standards of ethical conduct are applied throughout the CIB's business activities.

3.3.2 As the First Line of Defence, Personnel undertaking project advisory, investment and asset management activities are responsible for mitigating Integrity Risk. To this end, they are responsible for:

- supporting the Counterparty Identification and Verification process by collecting complete and accurate information and promptly escalating concerns to the CAMLO;
- ensuring that all Counterparties are identified and verified pursuant to the processes and controls described in the KYC Procedure;
- identifying any unusual or suspicious dealings with Counterparties and escalating their concern immediately to the CAMLO and the CEO; and
- reporting any instances of non-compliance with this Policy in accordance with the process described in the **Disclosure of Wrongdoing Policy**.

3.4 Chief Legal and Information Officer (Second Line of Defence)

3.4.1 The Chief Legal and Information Officer is the CIB's compliance officer (the "**CAMLO**") responsible for the development, implementation and administration of the Policy, as well as the oversight of compliance with the Policy and reporting requirements, including with respect to:

- developing processes and controls for mitigating Integrity Risk, including this Policy and the KYC Procedure;
- implementing a risk-based approach to quality assurance testing as noted below; and
- reporting to the Board, through the Finance and Audit Committee, on the overall effectiveness of the CIB's compliance activities for mitigating Integrity Risk.

3.4.2 The CAMLO has delegated to the Manager, Compliance and KYC (the "**Policy Manager**") the authority for the following activities:

- implementing tools intended for Personnel to comply with this Policy and the KYC Procedure;
- completing risk assessments with respect to money laundering, terrorist financing, bribery and corruption and implementing appropriate controls;
- completing or overseeing the completion of due diligence, Counterparty Identification and Verification procedures, including Enhanced Due Diligence for those parties presenting higher risks, as described in the KYC Procedure; and
- developing and delivering training and awareness sessions for Personnel in relation to this Policy and the KYC Procedure.

3.4.3 The CAMLO has authority to approve (i) KYC due diligence risk assessments and ratings for projects or counterparties with low and medium Residual Integrity Risk, and (ii) exceptions permitted under the KYC Procedure, subject to any escalation requirements set out in this Policy. Where Residual Integrity Risk is assessed as high or outside risk tolerances, or where a proposed exception to this Policy is requested, the CAMLO will escalate the matter to the CEO with a documented recommendation.

3.4.4 The CAMLO may delegate or outsource Second Line of Defense functions to internal or external resources, as appropriate. Nevertheless, the CAMLO retains overall accountability for ensuring these functions are effective, properly supervised, and appropriately managed.

3.4.5 Where third-party service providers are used to support Counterparty due diligence, the CAMLO is responsible for ensuring appropriate vendor governance measures are established, including:

- Defined scope of work and deliverable standards;
- Confidentiality, privacy and information security requirements, appropriate to the sensitivity of the information;
- Conflict of interest disclosure and management requirements;

- Quality assurance and performance monitoring; and
- Final risk assessments, and authority for final decision-making remains with the CIB (CAMLO and, where applicable, the CEO).

3.4.6 In performing Second Line of Defense functions, the CAMLO and delegated resources operate independently from transaction origination to ensure Counterparty due diligence is conducted objectively, based on evidence, and without improper influence.

3.5 Internal Audit (Third Line of Defence)

3.5.1 Internal Audit conducts periodic independent reviews of the CIB's administration of this Policy in accordance with the priorities contained in the CIB's risk-based audit plan.

3.6 Board of Directors

3.6.1 The Board of Directors (the "**Board**") has ultimate responsibility for ensuring that CIB maintains an effective Integrity Due Diligence framework. Specifically, the Board, through the Finance and Audit Committee:

- approves this Policy and material amendments;
- oversees the effectiveness of the Integrity Due Diligence framework;
- receives reporting on material Integrity Risk issues, exceptions and compliance effectiveness.

3.6.2 Where the Board has delegated authority to the Investment Committee, or similar management decision-making body, to approve investments, the decision-making body will consider KYC due diligence findings for individual transactions, including findings and proposed mitigation measures, within their delegated authorities and will escalate matters to the Investment Committee and/or Board where required.

4. Activities

4.1 Compliance program

4.1.1 The CIB's compliance program to identify, mitigate or manage Integrity Risks is based on the following activities:

- developing and implementing this Policy and associated risk-based procedures and controls (described in the KYC Procedure);
- designating a compliance officer (CAMLO) responsible for the design, monitoring, compliance and reporting functions of this Policy;
- designating a Policy Manager responsible for the operational effectiveness and the day-to-day administration of this Policy and the KYC Procedure;
- implementing Counterparty due diligence and controls;
- implementing controls to comply with applicable legislative requirements regarding Ministerial Directives, and reporting requirements for suspicious transaction reports (STRs), and terrorist property reports (TPRs);
- monitoring the effectiveness of the Policy and the KYC Procedure; and
- reporting on the implementation and the effectiveness of the Policy and the KYC Procedure to the Board, through the Finance and Audit Committee.

4.2 Risk assessment and approach

4.2.1 The CIB engages with a broad spectrum of project Counterparties, including but not limited to federal, provincial, territorial, municipal and Indigenous governments, as well as private sector and institutional investors within Canada and internationally. The CIB is able to use a wide breadth of financial instruments, including loans, equity investments, and where appropriate, loan guarantees to attract private investment in infrastructure projects. As a result, implementing a one-size-fits-all approach to managing Integrity Risk is not practicable. Instead, the CIB has adopted a risk-based approach that aligns with the specific level of risk identified or assumed for a Counterparty or CIB investment activity. This risk-based approach is informed by factors including the nature of the financing or transaction, the type of Counterparty and its jurisdiction of incorporation, the geographical scope of the Counterparty's operations, and other industry-specific risks.

4.2.2 The Policy Manager is responsible for conducting regular risk assessments based on the KYC Procedure, including Counterparty risk, product/service risk (including new investment products and services), geographic risk, and other relevant risk factors (for example, industry rules and regulations).

4.3 Exemption and exceptions

4.3.1 Certain Counterparties are exempt from specified Counterparty Identification and Verification Requirements based on their regulated or public status, as set out in the KYC Procedure.

4.3.2 The CEO may grant non-substantive exceptions to this Policy. An exception is a case-specific departure from procedural requirements that does not alter the CIB's risk tolerance, permit engagement with prohibited Counterparties, or undermine the objectives of this Policy. Exceptions require a documented recommendation from the CAMLO and approval by the CEO. All exceptions granted during the reporting period will be recorded and reported to the Finance and Audit Committee for oversight purposes.

4.4 Counterparty due diligence (KYC)

4.4.1 The CIB has adopted due diligence procedures, outlined in the KYC Procedure, to identify Counterparties and assess potential Integrity Risks associated with a particular Counterparty. The CIB has adopted a risk-based approach for Counterparty due diligence whereby Counterparties exhibiting higher Integrity Risks are subjected to increased levels of scrutiny and control.

4.4.2 Counterparty due diligence includes the following activities:

- **Counterparty identification and verification**. This process involves collecting personal identification and business information about a Counterparty. The information and documentation are used to; (i) identify the Counterparty; (ii) verify through reliable and independent sources whether any adverse Integrity- related information concerning the Counterparty exists, such as criminal charges or convictions, ongoing investigations for serious wrongdoing or other material adverse Integrity events and (iii) identify any Politically Exposed Persons ("**PEPs**").
- **Sanctions screening.** Pursuant to applicable laws, sanctions screening is performed to prevent the CIB from transacting with persons or entities involved in, among other things, money laundering, terrorism or terrorist financing, human rights violations and crimes against territorial integrity, security and independence.
- **Enhanced due diligence.** As applicable, Counterparties who are currently, or have previously been, the subject of one or more material adverse Integrity events, will be subject to Enhanced Due Diligence review. The scope of the Enhanced Due Diligence review will be determined on a case-by-case basis and will consist of collecting and reviewing additional information regarding the identified risk factors, e.g., by requesting information directly from the Counterparty, obtaining information from independent sources and/or through an external service provider with relevant expertise, or by reviewing the Counterparty's anti-corruption and AML-ATF policies.
- **CAMLO review.** Integrity Risks identified, including any recommended actions for mitigation and management, are reported to the CAMLO for approval. Situations where Integrity Risks are assessed as high or outside risk tolerance, or where a proposed exception to this Policy is requested, the matter will be escalated to the CEO with a documented recommendation.

4.5 Contractual representations and covenants

4.5.1 Definitive legal documentation (e.g., credit agreements) for all CIB financing arrangements will include market standard representations, warranties and covenants regarding compliance with applicable laws, as well as additional CIB-specific representations, warranties and covenants to ensure that Counterparties are in compliance with, and have a contractual obligation to adhere to, the CIB's risk tolerance and general expectations set forth in section 2.2 above and promptly disclose to the CIB any known issues of non-compliance with this Policy or the provisions thereof.

4.6 Ongoing monitoring

4.6.1 The Policy Manager is responsible for monitoring the Integrity Risk of Counterparties and project risk assessments, as applicable. For transactions with a higher risk profile, this review occurs at least once every year; for projects with no adverse risk findings, reviews may be less frequent. The process for ongoing monitoring follows the internal guidelines established in the KYC Procedure.

4.7 Training and education

4.7.1 The Policy Manager will develop and maintain a written, ongoing compliance training program for Personnel that is kept up to date to help them understand the legal requirements, the KYC Procedure, their accountabilities including not tipping off, and how to report suspicious activities.

4.7.2 At a minimum, Personnel will be provided with training within six months after the day on which their employment begins and at least once every two years thereafter.

4.8 Record keeping

4.8.1 The CIB will maintain full and accurate records of the investment transaction and information obtained for Counterparty Identification and Verification processes, as further described in the KYC Procedure, as well as monitoring and compliance with this Policy. All records relating to this Policy will be maintained in accordance with the activities described in the **Information Management Policy** and supporting procedures.

4.8.2 Records that are required to be kept under applicable laws and regulations will be maintained for at least the required period of time[1] and in a way that makes them accessible within the time frames set out in the applicable laws and regulations.

[1] *In accordance with the record-keeping requirements for departments and agents of the Crown (fintrac-canafe.gc.ca), records will be maintained for at least five years from the date the record was created, the suspicious transaction report was submitted or business transaction conducted.*

4.9 Self-assessment

4.9.1 The CAMLO, with the support of the Policy Manager and other resources, is responsible for completing a self-assessment of the CIB's compliance activities under this Policy (or assessment conducted by the CIB's internal audit function or independent third party) every two years to evaluate its effectiveness. The results of the self-assessment, including any action plan(s), will be reported to the Finance and Audit Committee.

4.10 Monitoring and reporting

4.10.1 The CIB will make disclosures or reports where required by law, and will maintain controls and procedures (set out in the KYC Procedure) governing escalation, confidentiality and documentation of any reporting decisions.

4.10.2 The CAMLO reports to the Board of Directors, through the Finance and Audit Committee, at least every two years on the administration of this Policy, including any exceptions granted under section 4.3.

4.10.3 Material KYC due diligence findings for individual transactions, including any exceptions and exemptions under this Policy, and situations where the Residual Integrity Risk is assessed as high despite significant mitigation measures or outside risk tolerances, will be summarized for the Management Investment Committee and/or Investment Committee as part of the investment memorandum supporting the investment decision.

4.11 Non-compliance

4.11.1 Personnel must report any potential or suspected non-compliance under this Policy to the CAMLO and, in their absence, the CEO. Personnel may also report instances of non-compliance in accordance with the process described in the **Disclosure of Wrongdoing Policy**.

4.11.2 The consequences of non-compliance with this Policy and the KYC Procedure can include any measure described in the **Code of Conduct for Personnel** determined as appropriate in the circumstances.

5. Definitions

Bribery: means giving, offering, soliciting or accepting, anything of value as a means of improperly influencing an outcome or improperly obtaining or retaining an advantage.

Corruption: means the abuse of entrusted power for private economic or political gain.

Counterparty(ies): refers to any person or legal entity that has a material contractual relationship with the CIB in connection with an investment or infrastructure project. In the context of the CIB's investment activities, this includes any contractual counterparty that:

a. receives financing or other financial support from the CIB, or

b. provides financing, credit support, or other material financial commitments in respect of the infrastructure project, including any person that directly or indirectly controls such contractual counterparty.

Counterparties include, as applicable, the borrower, investee, equity sponsors or investors, guarantors and other third parties that play a significant implementing or operational role in the infrastructure project (such as core construction contractors, key suppliers or operations and maintenance providers) that directly or indirectly receive project funds from the CIB. For the purposes of Counterparty due diligence, the scope of a Counterparty also extends to directors, officers, senior management and controlling individuals of the foregoing entities, as further described in the KYC Procedure. For greater certainty, individuals included for due diligence purposes under this Policy are not, by that fact alone, contractual counterparties of the CIB. This definition is intended to be applied in a risk-based and proportionate manner, consistent with the CIB's investment activities.

Counterparty identification and verification: refers to the process used to establish and authenticate the identity of a person or entity involved in a transaction or contract. This includes collecting personal, organizational and risk-relevant information to assess the presence of any Integrity Risks associated with the Counterparty.

Enhanced due diligence: means an advanced form of due diligence that goes beyond standard due diligence processes to provide a more comprehensive understanding or assess concerns related to Integrity Risks identified in the initial screening and standard due diligence. It is primarily applied in situations where there is a higher likelihood of risk, such as dealing with PEPs, persons in high-risk jurisdictions, or complex corporate structures.

Inherent integrity risk: refers to the natural level of risk associated with an activity, process or situation before any measures are taken to control or reduce it. For the purpose of this Policy, it represents the potential for reputational risk that exists in the absence of any risk mitigation strategies or controls, such as Enhanced Due Diligence.

Money laundering: is defined by the United Nations as any act or attempted act designed to conceal or disguise the source of money or assets derived from criminal activity. Essentially, money laundering is the process whereby "dirty money" – produced through criminal activity – is transformed into "clean money," the criminal origin of which is difficult to trace [see FINTRAC Guidance Glossary].

Personnel: means any person who is part of the workforce of the CIB, including any officer, whether working on a full-time, part-time, permanent or temporary basis, and including the Chief Executive Officer.

Politically Exposed Person (PEP): means a person who holds, or has held within the last 5 years, a specific office or public position (political or high-level professional appointment) or has family ties or close association to such an individual and as such may be in a position that could be abused for the purpose of money laundering, corruption, bribery and activities related to terrorist financing.

Residual integrity risk: refers to the level of risk that remains after the CIB has implemented controls and mitigation strategies to address inherent risks.

Sanctions: refer to prohibitions on trading and contracting with an individual, entity or country which are defined by the government as a penalty for the violation of the law, a breach of generally accepted international standards of conduct or to reflect security concerns. Sanctions lists are maintained by the Government of Canada, as well as the United Nations Security Council (UN), the European Union (EU), the United States of America (US) and the United Kingdom (UK).

Terrorist financing: refers to knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion [see FINTRAC Guidance Glossary]

6. Questions

For questions or interpretation of any aspect of this Policy, contact the Chief Legal and Information Officer.

7. Review

This Policy is reviewed and updated, as necessary, at least once every two years following the self-assessment described in section 4.9, or earlier if circumstances dictate that a review take place more frequently.

8. Approval and effective date

This Policy was initially adopted on January 15, 2019, and was last reviewed and approved by the Finance and Audit committee of the Board of Directors on June 17, 2026.

Control table	Description
Policy name:	Integrity Due Diligence Policy
Policy sponsor:	EVP & Chief Legal and Information Officer
Policy monitor:	Manager, Compliance and KYC
Date implemented:	January 15, 2020
Version:	4.0
Prior versions:	January 15, 2020; August 12, 2021; June 19, 2024
Approved by (date):	Finance and Audit committee in accordance with delegated authority from the Board of Directors (June 17, 2026)
Next review date:	June 2028 or earlier
File name:	CIB_Integrity_Due_Diligence_Policy_Final_06-17-2026_EN