NORDIC INVESTMENT BANK

FINANCING THE FUTURE

Integrity Due Diligence Policy

Approved by the Board of Directors on 8 March 2018
with entry into force on 1 May 2018

Preamble

NIB follows international standards and good practices regarding know-your-customer principles. While the manner in which NIB adopts these general principles is established in this Integrity Due Diligence ("IDD") Policy, the implementation of such principles is described in internal procedures.

The application of the different elements of the IDD, described in this Policy, is determined based on the risk that each NIB activity and operation presents. For this reason, the Bank has adopted a risk-based approach, focusing efforts and resources on those activities and cases that present more Compliance Risk.

Furthermore, taking note of the recent developments with respect to tax and transparency related risks; NIB joins the international and national efforts to promote transparency and fight tax avoidance and aggressive tax planning. Nevertheless, it is important to mention that NIB is not against the avoidance of double-taxation.

The purpose of this Policy is to protect NIB's reputation and promote a transparent business practice.

Table of Contents

Integrity Due Diligence Policy

1 Introduction

The Nordic Investment Bank (**"NIB"** or **"the Bank"**), as part of the international financing community, adheres to good international practices regarding Know-Your-Customer (**"KYC"**), Anti-Money Laundering (**"AML"**), Counteracting Terrorist Financing (**"CTF"**), and tax related matters. Furthermore, NIB also adheres to the Uniform Framework for Preventing and Combating Fraud and Corruption signed in 2006 by the major Multilateral Development Banks (**"MDBs"**)[1] with the purpose of setting ground rules for Integrity Due Diligence (**"IDD"**) and investigations of Prohibited Practices.

NIB's Integrity and Compliance Policy describes the manner in which NIB carries out its preventive work, and, investigates and sanctions when its counterparties and/or its staff engage in a Prohibited Practice or Misconduct. Moreover, the Compliance, Integrity and Anti-corruption Policy provides the ground for the adoption of IDD policies and procedures in order to manage integrity and reputational risks (hereinafter **"Compliance Risk"**) related to its borrowers and counterparties.

Based on the results of a review of NIB's internal AML/CTF and KYC controls and procedures conducted during 2015 and 2016, NIB has decided to adopt a risk-based approach regarding the application of AML/CTF and KYC controls. With this approach, NIB's intention is to conduct enhanced due diligence on counterparties and operations that present higher Compliance Risk.

2 Definitions

"Beneficial Owner" means any natural person or legal entity (when there is no natural person) controlling or owning, directly or indirectly, ten percent (10%) or more in NIB's counterparty. Beneficial Owner also means to include the natural person on whose behalf a transaction is being conducted, and those persons who exercise ultimate effective control over a legal person or arrangement.

"Cross-border link" means when (i) the counterparty, (ii) the entity controlling or owning, directly or indirectly, ten percent (10%) or more of the counterparty, or (iii) any other party that is of relevance for the NIB operation or activity (for example, a subsidiary, sponsor or a fund manager if the counterparty is a fund) is established in a jurisdiction other than the country where the NIB-financed operation or activity will take place.

"Financial Institution (FI)" means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

a. Acceptance of deposits and other repayable funds from the public.
b. Lending.
c. Financial leasing.
d. Money or value transfer services.
e. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
f. Financial guarantees and commitments.
g. Trading in:
   (a) money market instruments (checks, bills, certificates of deposit, derivatives etc.);

[1] The Multilateral Development Banks signatories to the Uniform Framework for Preventing and Combating Fraud and Corruption are the African Development Bank (AfDB), the Asian Development Bank (ADB), the European Bank for Reconstruction and Development (EBRD), the European Investment Bank (EIB), the Inter-American Development Group (IADB), the International Monetary Fund (IMF), and the World Bank Group (WB).

(b) foreign exchange;
(c) exchange, interest rate and index instruments;
(d) transferable securities;
(e) commodity futures trading.

h. Participation in securities issues and the provision of financial services related to such issues.
i. Individual and collective portfolio management.
j. Safekeeping and administration of cash or liquid securities on behalf of other persons.
k. Otherwise investing, administering or managing funds or money on behalf of other persons.
l. Underwriting and placement of life insurance and other investment related insurance.
m. Money and currency changing.

"Operational Unit(s)" means Lending, Treasury and any other unit engaging with a counterparty through the procurement of goods, works and/or services for NIB's internal use.

"Politically Exposed Person (PEP)" means any natural person who is or has been entrusted with prominent public functions and immediate family members, or person known to be close associates with such person. Examples include central and local government officials, members of the parliament, senior executives of state owned enterprises and of international organisations, judicial or military officials, and high-ranking political party officials.

"Sanctions Lists" means to include the sanctions lists maintained by the United Nations Security Council (UN), the European Union (EU), any NIB Member country, the United States of America (US), the United Kingdom (UK) and NIB.

"Senior Management" means to include the CEO, CFO, COO, CRO, CIO, CCO, President, General Counsel, Secretary General and Treasurer, or its equivalents according to the company's organizational structure.

3 Purpose and Scope

The purpose of this Policy is to describe the manner in which NIB manages the Compliance Risk arising in the context of its lending activities, trust fund activities, treasury operations, and internal procurement processes.

NIB's Integrity Due Diligence is comprised of four (4) elements:

1. General Integrity Review,
2. Anti-Money Laundering and Counteracting Terrorist Financing (**"AML/CTF"**) Review,
3. Cross-border Structural Review, and
4. Sanctions Screenings.

Each of these elements has the objective of gathering specific information and identifying risks in connection with NIB counterparties and other related parties. Based on the results of these reviews, an Enhanced Due Diligence (**"EDD"**) may be triggered.

The applicability of these elements and the specific requirements are described in detail in the internal procedures of each Operational Unit. The Integrity & Compliance Office (**"ICO"**), in coordination with the Operational Units, prepares these procedures which shall be approved by the President.

Below is a summary of the principles applicable under each integrity review.

Any personal data collected, processed and/or stored in the course of conducting an IDD procedure shall be duly protected and handled in accordance with NIB's regulations[2].

3.1 General Integrity Review

Based on the *know-your-customer* principle, NIB shall conduct appropriate due diligence on its counterparties. This General Integrity Review consists in identifying: (i) the Beneficial Owners of the counterparty; (ii) any past criminal charges or convictions, or ongoing investigations for serious wrongdoings against the counterparty, any Beneficial Owner, any member of the Board of Directors, Senior Management and any other individual involved in the operation or activity; (iii) sanctions imposed by national and international bodies and other IFIs on the counterparty, any Beneficial Owner, any member of the Board of Directors and Senior Management; and (iv) the presence of Politically Exposed Persons (**"PEP(s)"**).

3.2 Anti-Money Laundering and Counteracting Terrorist Financing (AML/CTF) Review

Financial Institutions (**"FI(s)"**) play a key role in preventing and identifying money laundering and terrorism financing. Whenever NIB's direct counterparty in a Lending activity is a FI, NIB shall assess the counterparty's AML/CTF policies and controls. The Bank considers the following in the AML/CTF assessment: (i) whether the Borrower is a regulated FI or not, (ii) regulatory or compliance history indicating weak controls or poor implementation of AML/CTF systems, and (iii) failure to respond or adequately answer AML/CTF-related questions.

NIB also considers the jurisdiction of incorporation of the FI counterparty and the recommendations made by the Financial Action Task Force (**"FATF"**)[3].

Under certain circumstances, and when the FI counterparty engages in on-lending, NIB may require the adoption of additional integrity checks to the end-beneficiaries.

3.3 Cross-border Structural Review

Taxpayers may sometimes take advantage of disparities between national tax systems in order to reduce their tax base. As a result, cross-border corporate structures may be used, in some cases, for tax evasion, tax fraud, aggressive tax planning or other harmful practices. The risk arising from the use of cross-border corporate structures increases when (i) there is no business rationale for the use of entities established in multiple jurisdictions; (ii) there are indications of profit shifting via foreign related-parties transactions; and/or (iii) the cross-border corporate structures include entities established in jurisdictions identified by specialised international organizations as presenting tax-related risks. The presence of the latter jurisdictions poses Compliance Risk due to the potential unwillingness to exchange tax information with the tax authorities in other jurisdictions.

As a result, NIB assesses if the cross-border corporate structures, when related to the operation or activity financed by the Bank (a **"Cross-border link"**), has a legitimate purpose or use. For the purposes of this Policy, there is a Cross-border link when (i) the counterparty, (ii) the entity controlling or owning, directly or indirectly, ten percent (10%) or more of the counterparty, or (iii) any other party that is of relevance for the NIB operation or activity (for example, a subsidiary, sponsor or a fund manager if the counterparty is a fund) is established in a jurisdiction other than the country where the NIB-financed operation or activity will take place.

[2] Relevant NIB regulations currently under preparation.
[3] For more information regarding the FATF visiting the following website: http://www.fatf-gafi.org/

When conducting the Cross-border Structural Review, NIB relies on the recommendations of specialized international organizations and efforts such as the Council of the European Union[4], the Global Forum on Transparency and Exchange of Information (**"Global Forum"**)[5], and the OECD's Base Erosion and Profit Shifting (**"BEPS"**) Actions[6].

3.4 Sanctions Screening

NIB supports the actions taken by international and national bodies against individuals and entities involved in among other things, terrorism or terrorism financing, human rights violations, crimes against world peace, political and economic stability, and territorial integrity, security and independence. The Bank establishes mechanisms to ensure that its counterparties are not entities or individuals included in a Sanctions List. NIB considers as Sanctions Lists the lists adopted by the United Nations Security Council (UN), the European Union (EU), any NIB Member country, the United States of America (US), and the United Kingdom (UK). Furthermore, NIB does not involve itself with counterparties that have engaged in a Prohibited Practice and have been sanctioned by NIB[7].

For this purpose, NIB has established automatic sanctions screening to Treasury and Lending incoming and outgoing payments.

4 Risk ratings

Based on the reviews described in Sections 3.1 - 3.4, the Operational Units, as the first line of defense, shall assess the risk arising from any identified risk indicator or gap in information.

Risk indicators and counterparties present different degrees of risk. For this purpose, NIB has established three (3) risk ratings that determine the depth of the IDD and the frequency of the monitoring.

NIB has the following Compliance Risk Ratings:

- **High Compliance Risk**; whenever a risk indicator presents Compliance Risk that falls outside NIB's risk tolerance. In cases where the Compliance Risk is High, the activity or operation shall not move forward. Indicators presenting High Compliance Risk are considered 'deal-breakers'. Although deal-breakers may vary from operation to operation, NIB has identified a number of them that are described in Section 5 below.

- **Medium Compliance Risk**; whenever a risk indicator presents some degree of Compliance Risk. Indicators presenting Medium Compliance Risk could remain within or outside NIB's risk tolerance subject to the outcome of an Enhanced Due Diligence. In some instances, and based on the results of the EDD, mitigating measures could be recommended or required to maintain the risk within NIB's risk tolerance. Any risk indicator presenting Medium Compliance Risk shall be informed to the committee or body making the decision regarding the activity or operation. Section 6 below describes the EDD.

- **Low Compliance Risk**; whenever there are no risk indicators identified, or when the identified risk indicators do not pose any or low compliance and integrity risk for NIB.

[4] For more information regarding the Council of the European Union's activities on tax issues, visit the following website: http://www.consilium.europa.eu/en/council-eu/
[5] For more information regarding the Global Forum visit the following website: http://www.oecd.org/tax/transparency/
[6] For more information regarding BEPS Actions visit the following website: http://www.oecd.org/tax/beps/
[7] NIB imposes sanctions according to the Bank's Investigations and Enforcement Policy.

5 Deal-breakers - High Compliance Risk

As a general rule, NIB shall not engage with a counterparty when any of the risk indicators below is identified. The applicability of these principles is further described in the internal procedures of each Operational Unit.

a. The counterparty's beneficial owners are unidentifiable

Identifying the ultimate beneficial owners of NIB counterparties is one of the core elements of the IDD. This principle includes identifying any intermediate legal entity used in the ownership structure. Beneficial Owner means any natural person controlling or owning, directly or indirectly, ten percent (10%) or more in NIB's counterparty. If there is no natural person crossing the threshold indicated above, the ultimate legal entity controlling or owning, directly or indirectly, ten percent (10%) or more in the counterparty will be considered the ultimate Beneficial Owner. Beneficial Owner also means to include the natural person on whose behalf a transaction is being conducted, and those persons who exercise ultimate effective control over a legal entity or arrangement. Identifying the Beneficial Owners prevents NIB from entering into a relationship with a counterparty whose source of funds is of dubious origin, or whose beneficial owners are related to money laundering, terrorism, organized crime or any other serious wrongdoing.

b. The counterparty is included in a Sanctions List

NIB shall not initiate a relationship if the counterparty itself or any Beneficial Owner is included in a Sanctions List.

c. The counterparty has repeatedly been subject to criminal investigations, charges or convictions for a serious wrongdoing

While it is not uncommon that large companies are subject to investigations, fines or sanctions, NIB expects that its counterparties apply national and international laws and regulations when conducting their businesses. NIB shall not enter into a relationship with a counterparty that has been repeatedly subject to criminal investigations, charges or convictions for serious wrongdoings such as, corruption, money laundering, terrorist financing, fraud, tax evasion, tax fraud, collusion, human, drug and firearm trafficking, cybercrime, among others. NIB will consider the corporate behavior and culture of the counterparty as a whole.

d. The counterparty has a Cross-border link to a Tax Prohibited Jurisdiction

Whenever NIB's counterparty has a cross-border corporate structure that includes entities incorporated in a Tax Prohibited Jurisdiction**,** NIB will refrain from entering into a relationship with such counterparty. A "Tax Prohibited Jurisdiction" is any jurisdiction that:

- The Global Forum has identified as (i) having failed the Phase 1 Global Forum peer review, or (ii) having received a *non-compliant* rating in the Phase 2 Global Forum peer review. The Global Forum is a key international body working on the implementation of the international standards on tax transparency.

- The Council of European Union has included in its "EU list of non-cooperative jurisdictions for tax purposes".

e. The Financial Institution (FI) counterparty is established in an AML/CTF Prohibited Jurisdiction

NIB shall not enter into a relationship with a FI counterparty that is established in a jurisdiction for which the FATF is calling "*to apply counter-measures due to on-going and substantial money laundering and terrorism financing risks"* (i.e. "AML/CTF Prohibited Jurisdiction"). The FATF is an international body that reviews the money laundering and terrorist financing techniques and counter-measures of its member countries, and monitors the progress of the member countries in

implementing necessary measures to prevent these crimes. Some of the jurisdictions' AML/CTF regulatory frameworks have strategic deficiencies that pose a risk to the international financial system. Since AML/CTF requirements are mostly applicable to FIs, FIs established in jurisdictions that pose a risk to the international financial systems are of major concern to NIB.

6 Enhanced Due Diligence - Medium Compliance Risk

An EDD shall be carried out whenever a risk indicator presents Medium Compliance Risk. Although it is not possible to have an exhaustive list of risk indicators or circumstances that could trigger an EDD, examples of these risk indicators are described in the internal procedures of each Operational Unit.

NIB considers for example, that the following risk indicators present Medium Compliance Risk: past or ongoing investigations or convictions for serious wrongdoings, presence of PEPs, sanctions imposed to any member of the Board of Directors or Senior Management, regulatory history related to AML/CTF, jurisdictional AML/CTF risks, and complex ownership or corporate structures.

NIB may also take into account the Transparency International's Corruption Perceptions Index[8] and the Basel AML Index[9].

An EDD consists of gathering additional information regarding the risk indicators by, for example, requesting information directly from the counterparty, consulting independent sources or hiring an external service provider.

The Operational Units shall consult with ICO when conducting an EDD.

6.1 External IDD reports

NIB may request an IDD report from an external service provider when local or specialized knowledge is required. Operational Units, in coordination with ICO, will select the external service provider in accordance with internal selection procedures.

7 Assessing and mitigating the Compliance Risks

After an Enhanced Due Diligence has been conducted (if applicable), the Operational Units are responsible for re-assessing the Compliance Risk and assigning a final risk rating. Operational Units shall take into account any mitigating or aggravating factor.

Based on the results of the EDD, risk indicators could remain to present Medium Compliance Risk, or could also present lower or higher Compliance Risk. As mentioned in Section 3 above, each of the risk ratings triggers different actions and/or requirements:

- If it is concluded that the Compliance Risk is Low, no further action is required;
- If the Compliance Risk remains Medium, mitigation may be recommended or required in order to move forward with the activity or operation. In these cases, the decision-making bodies or committees must be informed. Mitigation could include for example, reviewing the counterparty's anti-corruption or KYC policies and requesting the improvement of such policies if necessary, or the removal of any individual involved in a serious wrongdoing from any decision-making process related to the NIB-financed activity; and

[8] For more information regarding the TI's Corruption Perceptions Index visit the following website: https://www.transparency.org/
[9] For more information regarding the Basel AML Index visit the following website: https://index.baselgovernance.org/

- If it is concluded that the Compliance Risk is High (a “deal-breaker”), the activity or operation shall not move forward.

8 Informing Decision-Making Bodies

When the Compliance Risk is Medium, each Operational Unit shall include a description of the indicators presenting Compliance Risk in the corresponding documents (e.g. in the documentation presented to the Credit Committee, Executive Committee, the President and the Board of Directors). The text shall include (i) a description of the risks, (ii) any mitigating factors or measures, and (iii) the conclusion with the final Compliance Risk rating (Low, Medium or High). ICO shall be consulted regarding the risk rating and the text proposed by the Operational Units to be included in the proposals for approval.

ICO may also decide to provide a separate opinion to the decision-making committees or bodies if the Operational Unit and ICO differ in opinion.

9 Monitoring

The Compliance Risk shall be monitored, as applicable, at least once a year during the life of NIB’s operations and activities. Counterparties presenting Medium Compliance Risk shall be monitored with more frequency.

10 Record Keeping

The Operational Units are responsible for keeping record of the identified risk indicators, any mitigating measures undertaken and the conclusions reached. The Operational Units shall keep these records for at least five (5) years in the designated formats and systems, as established internally in coordination with ICO.

11 Roles

As the first line of defense, Operational Units are responsible for gathering the information, assessing, mitigating, disclosing and monitoring the Compliance Risk.

The Integrity & Compliance Office shall serve as a second line of defense and as an advisory body to the Operational Units, management and the Board of Directors. Specifically, Operational Units shall consult with ICO when risks indicators presenting High (“deal-breaker”) or Medium Compliance Risk are identified.

ICO shall, from time to time, conduct quality checks on the IDDs conducted by the Operational Units, and present its findings as part of its annual reporting to the Board of Directors and the Control Committee.

ICO is responsible for monitoring the efforts of the leading international organizations regarding the fight against corruption, money laundering, financing of terrorism, tax evasion, aggressive tax-planning and any other harmful activity, and taking these developments into account when drafting and updating NIB’s policies and procedures.

ICO shall coordinate the development of procedures with each of the Operational Units subject to this Policy.

12 Periodical Assessment of the Policy

ICO is responsible for this Policy, which shall be reviewed every five (5) years or earlier if so suggested by ICO, or requested by the President or the Board of Directors.