**INTERNATIONAL INVESTMENT BANK**

# Policy for Anti-money Laundering, and Combating The Financing of Terrorism, Fraud and Corruption

2016

# Contents

# 1. GENERAL PROVISIONS

## 1.1. SCOPE OF APPICATION

1.1.1. This document (hereinafter – the Policy) establishes basic standards, approaches and requirements to combat money laundering, the financing of terrorism, fraud, corruption and other Prohibited Practices.

1.1.2. The Policy applies to all employees of the Bank and its subsidiaries. The Policy applies to IIB Counterparties. All Policy requirements with respect to Counterparties also apply to all entities and parties involved in IIB's own activities, projects and investments (parties to civil-law contracts, contractors, sub-contractors, consultants, suppliers, service providers, etc.).

1.1.3. The Policy is produced on the basis of recommendations and requirements developed in this field by recognized international organizations like the Council of Europe (COE), Organization for Economic Cooperation and Development (OECD), Financial Action Task Force (FATF), Basel Committee on Banking Supervision, member states of the Bank, and by Anti-corruption task force of international financial institutions, and based on other practical methods used by leading international financial organizations.

1.1.4. Compliance department is an initiator of this Policy and is responsible for timely its updating.

## 1.2. TERMS AND DEFINITIONS

Below is a list of terms and definitions used in this Policy:

| Term | Definition |
|---|---|
| ***Prohibited Practices*** | Corruption, Coercion, Collusion, Financing of terrorism, Fraud and Money laundering |
| ***Corrupt practice (corruption)*** | The offering, giving, receiving, or soliciting, directly or indirectly, anything of value to improperly influence the actions of another party. Corruption includes abuse of authority, extortion, bribery, abuse of power, commercial bribery or other prohibited use by a person of his official position to obtain benefits in the form of cash, valuables, other property or property services for themselves or for third parties. |
| ***Identification*** | A list of measures taken to identify information about entities and persons, their representatives, and beneficiaries and to keep this information updated (Know your customer) |
| ***Counterparty*** | A person with whom the Bank is executing or plans to execute transactions |
| ***Money laundering (ML)*** | Placing a veneer of legality on the possession, use or disposal of money or any other property obtained through committing an offence |
| ***Limit of non-banking transactions for the purposes of AML/CFT/F/C*** | A maximum amount of non-banking contracts with a Counterparty or maximum amount of procurements from a Counterparty within a calendar year, approved by the IIB Board, the exceeding of which requires Counterparty identification and an AML/CFT/F/C risk assessment |
| ***Fraudulent practice (Fraud)*** | Any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation |
| ***Misconduct*** | Failure by a staff member to observe the rules of conduct and the standards of behavior prescribed by the IIB |
| ***Politically exposed persons (public officials)*** | Individuals who are entrusted with prominent public functions within the country of their residence or within other countries, as well as their close family (sisters and brothers, children, parents, a spouse) acting in their own name or on behalf of a Counterparty, in favor of a Counterparty, or being shareholders or beneficiaries of a Counterparty |

| | |
|---|---|
| ***Coercive practice (coercion)*** | Any impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of any party to improperly influence the actions of a party |
| ***Collusive practice (collusion)*** | Any informal arrangement between two or more parties designed to achieve an improper purpose, including improperly influencing the actions of another party |
| ***Financing of terrorism (FT)*** | The provision or collection of financial services, knowing that the funds are intended to finance the organization, preparation and commitment of terrorist acts |

1.2.1. In order to counter Prohibited Practices, the Bank takes into account that money laundering as a rule is effected by changing the form of ownership, relocating, distributing or consolidating money, gained through illicit types of activities such as drug trafficking, illicit arms trafficking, illegal enterprise, piracy, production infringement, etc. Money laundering shall mean the following activities, including the participation therein:

– property transactions (money, precious metals, securities, etc.), if this property is known to have been obtained illegally as well as the acquisition, possession, disposal and/or use of which is associated with the violation of applicable law;

– the suppression or concealment of the origin, location, and other information about property gained through Prohibited Practices;

– the acquisition, possession and use of property gained through Prohibited Practices.

1.2.2. In order to counter Prohibited Practices, the Bank takes into account the fact that terrorism can be financed either through money laundering or by directly financing the organizations created to support terrorism.

Terrorism is financed to commit crimes, aimed at disrupting the political, economic, constitutional framework of governments and society, by threatening people and/or exercising pressure on governments or local authorities.

1.2.3. In order to counter Prohibited Practices, the Bank takes into account the fact that fraud includes a sufficiently broad list of crimes committed to gain any benefit (mainly, financial).

1.2.4. Over the course of its operations, the Bank may encounter external fraud committed by the parties independent from the Bank, internal fraud by its employees, or a combination of both. The Bank is most exposed to the following types of fraud:

– fraud committed by employees of the Bank (for instance, willful misrepresentation of information in reports, deliberate omission of entering a deal in the accounting system, document forgery, theft of confidential information);

– fraud committed by counterparties (for instance, delivery of low quality products, forgery of documents for misrepresentation of creditworthiness, provision of invalid information);

– fraud in the security area (forged pass to the Bank, unauthorized access to the Bank's information resources).

1.2.5. In order to counter Prohibited Practices, the Bank takes into account the risks of corruption among parties and/or employees (personal corruption), corruption of governmental authorities (systemic corruption) and corruption of certain representatives of separate countries or international unions (international corruption).

1.2.6. The Bank recognizes the following cases as corruption, wherein money, property and services are received/offered by an employee for stimulating prohibited transactions or illicit actions, and are, therefore, performed as compensation for: receipt of money, taking of gifts in violation of procedures specified in internal documents of the Bank, excessive gratitude (a travel voucher, provision of property for free) and other situation, defined by internal regulations of the Bank.

## 1.3. ABBREVIATIONS

This Policy uses the following abbreviations:

| Abbreviation | Meaning |
|---|---|
| **Bank, IIB** | International investment bank |
| **AML/CFT/F/C** | Anti money laundering, the financing of terrorism, fraud and corruption |

## 1.4. BASIC PRINCIPLES

1.4.1. The primary objective of this Policy is to determine and develop standards for efficient internal control system to protect against money laundering, the financing of terrorism, fraud and corruption, compliance with which will reduce the risk of the Bank and its services being used in the Prohibited Practices.

1.4.2. The basic standards and requirements for preventing and deterring Prohibited Practices include:

– adhering to the highest standards of integrity for staff, the Bank's own activities and the activities of all parties involved in IIB projects;

– prohibiting any actions by Counterparties, employees of the Bank or third parties involved in IIB projects related to Prohibited Practices;

– regular preventing the use of the Bank for any Prohibited Practices;

– адекватность и достаточность принимаемых мер возникающим угрозам;

– determining the relevance of measures taken and threats that may arise;

– конфиденциальность сведений о конкретных шагах Банка в области противодействия Запрещенным практикам;

– maintaining the confidentiality of information on actual efforts made by the Bank to prevent Prohibited Practices;

– establishing an independent department within the Bank and appointing an officer thereto responsible for ensuring internal control to prevent Prohibited Practices and to conduct investigations;

– investigating Prohibited Practices independently, fairly, impartially and in accordance with the principles and standards of investigations generally adopted by the leading IFIs.

1.4.3. The Bank ensures that agreements with Counterparties include obligations not to engage in any Prohibited Practices, to inform the Bank of any fact or suspicion of Prohibited Practices and to cooperate within ongoing investigations. Agreements shall also include provisions to prevent and deter Prohibited Practices and apply sanctions.

1.4.4. While performing job responsibilities, employees of the Bank, Counterparties and all entities and parties involved in IIB's activities, projects and investments shall:

– maintain the highest level of integrity;

– avoid any actions which, in accordance with this Policy, may be recognized as Prohibited Practices;

– report any fact or suspicion of committing actions related to Prohibited Practices to the Bank as this is also required of staff by the Code of Conduct [1];

– comply with the requirements of the Policy and other internal regulations related to preventing Prohibited Practices and Misconduct.

1.4.5. In addition to the requirements of paragraph 1.4.4., the staff of the Bank shall:

– know the requirements of the risk-based approach to assessing the general level of Counterparty risk and identifying a Counterparty;

– recognize the activities of the Bank which give rise to the key risks of Prohibited Practices and which of the Bank's activities are most exposed to risk from Prohibited Practices;

– attend training on the internal control measures for AML/CFT/F/C;

– be aware of the repercussions for failing to comply with any requirements of this Policy or other internal regulations regarding preventing Prohibited Practices.

1.4.6. Each employee of the Bank shall be held personally responsible in cases when he or she knew, suspected or had serious grounds to suspect the involvement of any employees or Counterarties of the Bank in Prohibited Practices, and:

– agreed to and processed the deals/transactions with the funds related to the above activity;

– rendered any assistance or help in the agreement, processing, controlling or use of the above funds;

– impeded any investigation of the above activity;

– failure to disclose such information to an employee of the Bank, responsible for carrying out internal control measures in order to counter Prohibited.

1.4.7. IIB staff, Counterparties and any person or entity involved in IIB's activities or in IIB's projects should report any detected risks of corruption, fraud, money laundering, financing of terrorism and other Prohibited Practices to the Bank:

– by letter;
– by email to compliance@iibbank.com;
– through the online form available on the IIB website;
– by telephone (+7 495 604-75-80).

1.4.8. The Bank shall ensure an independent, timely, fair consideration and decision upon receiving information and conducting an investigation in accordance with the internal regulations of the Bank.

## 2. ORGANIZATION OF INTERNAL CONTROL FOR AML/CFT/F/C

### 2.1. SYSTEM OF POWERS

2.1.1. Decisions related to countering Prohibited Practices and the functioning of the AML/CFT/F/C system are made by:

– The Council of the Bank;
– The Board of the Bank;
– The Chairman of the Board of the Bank;
– Committees.

2.1.2. The Council's jurisdiction covers consideration and approval of the Policy as well as review and approval of changes proposed for inclusion in the Policy.

2.1.3. The jurisdiction of the Board of the Bank covers:

– approval of the Bank's regulations and measures to counter Prohibited Practices;

– approval of decisions permitting transactions with a Counterparty to start, continue or terminate in light of the risks identified and related to Money Laundering, Financing of Terrorism, Fraud and Corruption;

– approval of non-banking transaction limits for purposes of AML/CFT/F/C;

– review of reports and decision-making on IIB systems, procedures and regulations for countering Prohibited Practices;

– review of results of investigations of suspected and actual participation of the employees of the Bank or Counterparties in the Prohibited Practices, making decisions thereon and imposing disciplinary sanctions.

2.1.4. The Chairman of the Board of the Bank has overall responsibility for managing IIB's risks of Prohibited Practices and is responsible for the creation and efficient operation of internal control system to counter Prohibited Practices.

2.1.5. The Committees within their jurisdictions are responsible for considering and accepting transactions with high-risk Counterparties.

2.1.6. The powers and functions of the departments of the Bank related to countering Prohibited Practices are defined by IIB's internal regulations.

2.1.7. Department heads are responsible for proper managing the risks of Prohibited Practices on a daily basis in accordance with set rules and regulations.

2.1.8. The business departments shall be the first line of defense for IIB to detect and prevent potential risks of Prohibited Practices.

2.1.9. The supporting units provide detection and protection IIB of Prohibited practices in accounting, processing and control operations.

2.1.10. The Compliance Department (CD) is responsible for identifying, estimating, controlling and reporting these risks to the relevant IIB bodies.

## 2.2. RISK ASSESSMENT

2.2.1. The risk of prohibited transactions is assessed by the Bank in accordance with the risk-based approach, which assumes the identification of the Bank's exposure to transactional risks based on the assessment of key factors affecting the level of this risk. A list of these factors may include the country in which a Counterparty is registered, its type of business, reputation, key clients, services requested, total time in business, credit history and other factors enumerated in the internal regulations.

2.2.2. The risk-based approach uses the principle of a commensurate level of Counterparty risk and the depth of due diligence performed in relation of the Counterparty: the higher the Counterparty's risk, the more detailed information about the Counterparty and its operations should be available to the Bank.

2.2.3. To measure the risks of Money Laundering, Financing of Terrorism, Fraud and Corruption and other compliance concerns, the Bank uses the following 3-level scale:

1. Low risk;
2. Medium risk;
3. High risk.

2.2.4. The Bank's internal regulations define criteria for estimating a Counterparty's risk level, procedures for conducting due diligence and monitoring their transactions, a list of requested documents and procedures for assessing the risk of Politically Exposed Persons.

2.2.5. The Bank may use a list of Counterparties, with whom it executes no transactions regardless of the level of risk assigned thereto, or a list of transactions that the Bank executes with none of the Counterparties.

2.2.6. The risks of Prohibited Practices are reviewed and assessed within the framework of initial Counterparty assessments and their subsequent monitoring in accordance with the procedures established within the Ban.

2.2.7. Integrity risks for the Bank's staff are assessed based on their exposure to respective risks. Using various preventive and verification mechanisms, the Bank controls employee activities, especially the activities of those who are involved in Counterparty relations and process their transactions.

## 2.3. KNOW YOUR CUSTOMER

2.3.1. The Bank performs the Know Your Customer procedure on all new Counterparties, entities and persons related to the Bank's activities, investments and projects. Due diligence is conducted on all new operations and products in order to reveal possible compliance risks and risks of Prohibited Practices.

2.3.2. The Bank has no relations and executes no transactions with a Counterparty until the level of risk assigned thereto is assessed and the Identification process is completed. This requirement does not apply to non-banking transactions with a Counterparty, provided that the volume of planned transactions with the Counterparty in question does not exceed the AML/CFT/F/C Limit for non-banking transactions established by the Board of the Bank.

2.3.3. The Bank uses all required measures to confirm that a Counterparty or a third party acting in the interests of the Counterparty is exactly the person declared in the transaction documentation (Know Your Customer). These measures are an important AML/CFT/F/C control tool that minimizes the risks of Prohibited Practices and protects the Bank from exposure to possible financial and reputational risks.

2.3.4. The Know Your Customer procedures assume that:

– the Bank has collected all information that supports the conclusion that a Counterparty or a third party acting in the interests of the Counterparty has been fully identified and all adherent risks are detected and assessed;

– the Bank understands that the Counterparty and third party acting in the interests of the Counterparty do not conduct any transactions related to Prohibited Practices;

– the funds used in the transaction were acquired by the Counterparty and third party acting in the interests of the Counterparty as a result of transactions that are not prohibited;

– the Counterparty, its participants, beneficiaries and top management and third party acting in the interests of the Counterparty have been cleared against specialized lists of international organizations or individual countries imposing sanctions or limitations on Counterparties/countries;

– the Bank understands that the Counterparty is acting in its own interests or in the interests of third parties.

2.3.5. Depending on a Counterparty's level of risk, the Bank may frame the Counterparty Identification process in accordance with a simplified, standard or enhanced procedure (applicable to high-risk Counterparties).

2.3.6. The Bank may define criteria based on compliance therewith, regardless of the general Counterparty risk level, such that the Identification process may follow simplified, standard or enhanced procedures or may ultimately be omitted.

2.3.7. The Bank's internal regulations establish a list of documents and information about a Counterparty to be requested.

2.3.8. The Bank refuses to execute transactions with Counterparties related to financial institutions that fail to perform AML/CFT measures according to the information provided thereby. The Bank establishes no relationships with financial organizations that, which have no physical presence in the states where they are registered (so called "shell banks") or with Counterparties acting on their behalf. The Bank opens no accounts for anonymous holders.

2.3.9. The Bank also takes appropriate measures to identify agents of Counterparties and, if a Counterparty or its agents act for the benefit of third parties, the Bank also identifies the third parties.

## 2.4. MONITORING

2.4.1. In order to identify transactions and risks related to Prohibited Practices and to detect integrity and compliance concerns and misconduct, the Bank regularly monitors transactions by its Counterparties,entities and persons involved in the Bank's projects and of its staff.

2.4.2. The Bank uses various monitoring procedures, whose scope and frequency depend on the level of risk assigned to a Counterparty and an employee's exposure to the Counterparty's transactions. In addition, certain types of monitoring depend on the availability of automated system within the Bank and particular transaction parameters or Counterparty categories.

2.4.3. To identify Prohibited Practices the Bank develops and applies transactional and situational attributes that may serve as a basis for suspecting that a Counterparty or a Bank employee is performing actions involving Prohibited Practices.

2.4.4. The Bank reviews and checks information regarding the suspected involvement of Counterparties or Bank employees in Prohibited Practices. Any material integrity or compliance concerns are promptly reported to the governing bodies of the Bank with recommendations and risk mitigating measures in accordance with the Bank's internal documents.

2.4.5. In addition to regular monitoring to prevent and detect Prohibited Practices, the Bank conduct an Integrity review of the Bank's products and projects. The objective of the Integrity review is:

– to determine if contracts were implemented according to their approved terms, to ensure that IIB financing is used properly;

– to recommend improvements to IIB policies and procedures to mitigate the risks of potential Prohibited Practices;

The frequency of such compliance reviews are determined by the Bank, as necessary, taking into account identified compliance risks in respect of banking products and projects.

2.4.6. The Bank takes appropriate measures to protect the parties (whistleblowers), who report on Counterparties and/or employees suspected of or actually executing Prohibited Practices.

### 2.5. TRAINING

2.5.1. The Bank defines categories of its employees who undergo regular trainings on how to prevent Prohibited Practices.

2.5.2. The training is designed to reflect the program developed and is updated by the Bank's accounting function to cover the types of transactions performed by the trainees and the level of knowledge they should attain.

2.5.3. The Bank develops knowledge examination procedures, the results of which are reported to the Chairman of the Board of the Bank.

2.5.4. To ensure a high-level of integrity in its activities, the Bank may provide training to employees of its Counterparties and/or other entities engaged in the Bank's projects.

### 2.6. SANCTIONS

2.6.1. In order to prevent and exclude Prohibited Practices in the future, the Bank stipulates terms in the agreements and accordingly applies sanctions to wrongdoers.

2.6.2. IIB includes certain remedies in agreements for dealing with breaches that may consist of disbursement suspensions or early reimbursements, granting or refusal of cooperation.

2.6.3. IIB and IIB Counterparties shall include terms in agreements with entities and persons participating in IIB's activities and projects that give IIB the right to withhold approval of these entities and parties, or to declare them ineligible or to exclude them from participating in IIB projects.

2.6.4. IIB may exclude Counterparties or any other entities or persons from participating with IIB and in IIB projects if they are found to be involved in Prohibited Practices, or are included in lists of excluded entities that are filed with international organizations.

## 3. INFORMATION HANDLING AND CONFIDENTIALITY

### 3.1. INFORMATION HANDLING

3.1.1. When requesting information from its Counterparties for the purposes of preventing Prohibited Practices, the Bank takes appropriate measures to reduce the risk of receiving invalid or outdated information.

3.1.2. When collecting information for countering Prohibited Practices, the Bank uses the data received from a Counterparty. Information from third parties and electronic data are only used if received from reliable information sources. The Bank refers to reliable sources of information including, among others, the Bankers Almanac electronic guidebook, WorldCheck, the LexisNexis and SPARK databases, information from the supervisory bodies, regulators, state registration chambers and services.

3.1.3. The Bank generates and archives the documents within the appropriate periods of time, as defined in the internal regulations of the Bank.

### 3.2. CONFIDENTIALITY

3.2.1. The Bank treats any information obtained about a Counterparty, an employee and the transactions between them, information about Counterparties or employees suspected of performing actions related to Money Laundering, Financing of Terrorism, Fraud and Corruption as confidential information.

3.2.2 The Bank does not disclose information about the persons reporting the Counterparties and/or employees suspected in actually conducting Prohibited Practices.

3.2.3. The Bank does not disclose information to the Counterparties about the forms, methods and procedures performed in order to prevent Prohibited Practices.

## 4. FINAL PROVISIONS

4.1. In case of amendments to the Bank's regulations or the Agreement Establishing the IIB and its Charter, this Procedure, along with amendments hereto, shall be applicable to the extent that does not contradict the newly approved regulations, the Agreement Establishing the IIB, or its Charter.

## 5. LIST OF REFERENCES

1. Code of Conduct of the International Investment Bank (OND-32), approved by Order No. 100 dated 7/11/2013.

## 6. LIST OF THE BANK'S REGULATIONS SUPERSEDED BY THIS DOCUMENT

This document supersedes the Policy for Anti-money Laundering, and Combating The Financing of Terrorism, Fraud and Corruption, approved by the Resolution 100 of the IIB Council.