International Investment Bank

POLICY
on Anti-Money Laundering, Combating the Financing of Terrorism, Fraud and Corruption

Moscow
2019

Table of Contents

1. GENERAL PROVISIONS

1.1. Scope of Application

1.1.1. The Policy on Anti-Money Laundering, Combating the Financing of Terrorism, Fraud and Corruption (hereinafter referred to as the "Policy") establishes basic standards, approaches and requirements to internal control arrangements at International Investment Bank (hereinafter referred to as the "Bank" or "IIB") for anti-money laundering, combating financing of terrorism, fraud and corruption.

1.1.2. The Policy is applicable to all employees of the Bank and its subsidiaries as well as to the persons working under civil law agreements. If necessary, the Bank applies the Policy's requirements to its Counterparties as well as to the persons involved in IIB's projects (contractors, counselors, suppliers, etc.).

1.1.3. When implementing this Policy, the Bank takes into account aims and obligations of IIB's members assumed under the signed international agreements and conventions on anti-Corruption, anti-Money Laundering and combating Financing of Terrorism.

1.1.4. The Policy is based on the recommendations and requirements developed in this field by widely recognized international organizations like the Organization for Economic Cooperation and Development (OECD), Financial Action Task Force (FATF), Basel Committee on Banking Supervision, and as well as on the recommendations and requirements of the Bank's member states and best practices adopted by leading international financial organizations.

1.1.5. The Bank considers Corruption, Fraud, Money Laundering, and Financing of Terrorism as acts unacceptable in its activities, which are fully and unconditionally prohibited. The Bank executes transactions so that the assumed Compliance Risks are identified, assessed and are at the least possible level acceptable for the Bank. In this regard, since it is impossible, as a rule, to fully exclude the detected risks, their acceptance at the approved level does not mean that the Bank considers the Prohibited Practices as permissible.

1.1.6. The unit-owner of this Policy responsible for its timely updating is the Compliance Department.

1.2. Basic Terms and Definitions

Below there is a list of terms and definitions used for the purposes of the Policy

Term	Definition
Prohibited Practices	Corruption, Coercion, Collusion, Obstructive Actions, Fraud, Money Laundering, Financing of Terrorism.
Identification	A complex of measures aimed at vetting the Counterparties, their representatives and beneficiaries, confirming the validity of such information (Know your customer).
Compliance Risks	Risks of sanctions, or significant financial losses, or damage to reputation, to which IIB may be exposed due to non-compliance or improper compliance with the established compliance rules. The Bank defines the risks of corruption, fraud, money laundering, financing of terrorism, employees' misbehavior, etc. as the Compliance Risks.
Counterparty	A person, with which the Bank executes or plans to execute transactions or with which the Bank has entered into an agreement/contract or negotiates entry into an agreement/contract.
Corruption	Exerting pressure on a third party in a form of offering, giving, receiving, or soliciting, directly or indirectly, anything of value as payment for their illegal or criminal actions. Corruption includes the following actions: • Abuse of official authority/position/power,

	• Blackmail, • Giving or taking bribe in a form of money, securities, valuables, other possessions or illegal provision of monetizable services or by provision of any other property rights for themselves or for any third parties, • Commercial bribery, • Facilitating payments, • Any other illicit misuse of a person's official capacity/position/status in order to gain benefits in a form of money, securities, valuables, other possessions or monetizable services or provision of any other property rights for themselves or for any third parties.
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 agreements/contracts with a Counterparty or procurements from a Counterparty within one calendar year, exceeding of which requires the Counterparty's Identification and AML/CFT/F/C risk assessment.
Fraud	Any act or omission of a party, including providing false data, that knowingly or recklessly misleads, or attempts to mislead, any other party to obtain a tangible or intangible benefit, including to mitigate liability, for the first party (or associated persons).
Misconduct	Failure by the Staff to observe the established rules of conduct and the standards of behavior adopted by IIB.
Staff	Employees of IIB, including its branches and representative offices, employees of IIB's subsidiary as well as natural persons providing services to the Bank and/or the Bank's subsidiary under civil law agreements.
Coercion	Impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party in order to force this party to act in a criminal or unlawful manner.
Politically exposed persons (PEP)	Natural persons entrusted, including previously, with a prominent public function in the country of stay of the Bank or other countries or in international organizations, as well as their next of kin (parents, sisters and/or brothers, children), spouse(s) acting in their own right, acting on behalf of a Counterparty, or being a shareholder or beneficiary of a Counterparty.
Collusion	An arrangement between two or more parties, designed to take criminal or improper actions to gain a benefit.
Facilitating Payment	A payment made to facilitate taking/failure to take by any person of the decision, which should be taken by this person in virtue of the duties imposed on such person without receiving such payment. As a rule, such payment may be made to a Politically Exposed Person to ensure or accelerate taking of any decision.
Financing of Terrorism	Provision or collection of finance or financial support knowing that the funds are intended to financing a terrorist organization, preparation and commitment of terrorist acts.

1.2.1. When implementing measures to prevent the Prohibited Practices, the Bank acknowledges that the Money Laundering usually happens through altering ownership, transferring, fractionalizing or consolidating monetary funds gained from criminal activities like

drug trafficking, including drug trade, illegal arms trade, illegal business practices, piracy, illegal use of trademarks, counterfeit production, etc.

1.2.2. Money Laundering refers to, in particular, the following activities, and preparation to participate or participation in such activities:

– Executing transactions with property (money, precious metals, securities, etc.), where such property is known to be the proceeds of illegal operations, as well as when acquisition, possession, disposal and/or use of which relates to the violation of the applicable law;

– 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.

1.2.3. When implementing measures to combat the Prohibited Practices, the Bank acknowledges that Financing of Terrorism may be executed either through Money Laundering or via direct financing of the organizations established to support terrorism.

Financing of Terrorism happens in order to commit crimes aimed at destabilizing a state and/or nation's political, economic, constitutional bases by means of population intimidation and/or exerting pressure on governments or local authorities.

1.2.4. When implementing measures to combat the Prohibited Practices, the Bank acknowledges that Fraud includes quite a broad list of crimes aimed at gaining benefits (usually, tangible benefits).

1.2.5. In the course of its activities, the Bank may encounter external fraud on the part of the independent persons as well as internal fraud on the part of the Staff, or a combination of these types of fraud. The Bank could most be prone to the following kinds of fraud:

–Staff's fraud (for instance, deliberate misrepresentation of information in statements, deliberate omission of a transaction, when registering it the record keeping system, document forgery, confidential information theft);

–Fraud of the Counterparties and persons involved in the Bank's projects (for instance, providing poor-quality goods or services, document forgery in order to misrepresent credibility, misrepresentation of information);

–Security fraud (forgery of a Bank's pass, unauthorized access to the Bank's information network).

1.2.6. When implementing measures to combat the Prohibited Practices, the Bank acknowledges the risks arising from the Counterparty's and/or Employees' corruption (individual corruption), government corruption (system-related corruption) as well as corruption on the part of representatives of certain states or international associations (international corruption).

The Staff may encounter Corruption, when money, property or services received (offered) are aimed at inducing the Prohibited Practices/illegal actions and used as bribe for such actions, taken or planned (Facilitating Payments): for instance, receiving money, gifts in amounts exceeding the permitted values and breaching the procedures established at the Bank, demonstration of excessive gratitude (provision of a package tour, provision of property, services, vehicles, privileges, etc. for use).

1.2.7. The Bank exercises internal control measures to mitigate the risks of Prohibited Practices at all corporate governance levels based on the three lines of defense model. Each governing body, department of the Bank and the Staff acts so as to most effectively and responsibly prevent and mitigate the Prohibited Practices as well as arising Compliance Risks.

1.3. Abbreviations

For the purposes of this Policy the following abbreviations are used:

Abbreviation	Explanation
Bank, IIB	International Investment Bank, its subsidiaries and representative offices

CD	IIB's Compliance Department
AML/CFT/F/C	Anti-Money Laundering, Combating the Financing of Terrorism, Fraud and Corruption
FT	Financing of Terrorism

1.4. Basic Provisions and Requirements

1.4.1. The Bank observes the following standards and requirements to internal control arrangements for AML/CFT/F/C:

– Adhering to the highest standards of integrity for Staff. The general ethical rules and regulations of the employees' conduct are set forth by the Code of Conduct (1);

– Prohibiting any actions aimed at implementing the Prohibited Practices by the Counterparties, employees or third parties involved in the Bank's projects;

– Preventing the use of the Bank for any Prohibited Practices;

– Determining the relevance and adequacy of measures taken to counter threats that may arise;

– Implementing ongoing countermeasures to prevent any threat of involving the Bank in the Prohibited Practices;

– Confidentiality of information on actual efforts made by the Bank for AML/CFT/F/C;

– Personal responsibility of the employees for implementing the measures for AML/CFT/F/C;

– Forming an independent department within the Bank and appointing an officer thereto responsible for ensuring internal controls for AML/CFT/F/C — the Compliance Department;

– Investigating the Prohibited Practices independently, fairly, impartially and in accordance with the principles and standards of investigations generally adopted by the leading international financial institutions.

1.4.2. When performing job responsibilities, the Staff, the Counterparties and third parties involved in the projects shall:

– Take necessary internal controls measures agreed upon with CD and/or established by the applicable regulations, aimed at prevention, detection of, and control over risks of the Prohibited Practices;

– Maintain the highest level of integrity;

– Avoid any actions, which under this Policy may be deemed as the Prohibited Practices;

– Report any fact or suspicion of committing actions related to the Prohibited Practices as provided for, in particular, by the Code of Conduct [1] and the Procedure (4);

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

1.4.3. In addition to the requirements stipulated in paragraph 1.4.2., the Staff shall:

– Recognize the activities of the Bank which give rise to risks related to the Prohibited Practices and which of the Bank's activities are most exposed to such risks so that they could be prevented;

– Annually undergo training arranged by the Bank on the internal control measures for AML/CFT/F/C and on the Compliance Risks as well as the relevant tests;

– When assessing the Counterparty's Compliance Risk and during its Identification, use a risk-based approach.

1.4.4. The employees of the Bank shall be held personally responsible in cases when they knew or had serious grounds to suspect involvement of the Staff or the Counterparties in the Prohibited Practices or Misconduct, 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;

– Failed to report such information to their senior official or the Compliance Department.

CD is responsible for arrangement of investigations with regard to the Employees' involvement or participation in the Prohibited Practices and their Misconduct.

1.4.5. The Staff, the Counterparties and the persons involved in IIB's projects should report to the Compliance Department any detected risks of Corruption, Fraud, Money Laundering, Financing of Terrorism and other Prohibited Practices as well as Misconduct relevant to the Bank, using one of the following means:

– By email to compliance@iibbank.com;

– By filling in an online form available on IIB's website;

– By telephone (+7 495 604-75-80).

1.4.6. The Bank shall ensure that the received information will be timely assessed and an independent and fair investigation will be conducted as per the internal regulations and based on the principles approved by the leading international financial organizations in this field.

2. INTERNAL CONTROL ARRANGEMENTS FOR AML/CFT/F/C

2.1. Authority System

2.1.1. Decisions related to AML/CFT/F/C are made by:

– Board of Directors;
– Chairperson of the Management Board;
– Management Board;
– Dedicated Committees of the Bank to the extent applicable to their jurisdiction;
– Compliance Department.

2.1.2. The jurisdiction of the Board of Directors covers:

– Approving this Policy and amendments hereto;

– Decision-making on lending projects submitted for the Board's consideration subject to the provisions of this Policy and taking into account the detected Compliance Risks;

– Considering reports on the Compliance Risks assumed by the Bank and proposed actions (on an annual basis);

– Controlling implementation by the Bank of the internal control measures for AML/CFT/F/C and assessment of their effectiveness.

2.1.3. The jurisdiction of the Chairperson of the Management Board covers:

– Implementing general coordination of and control over the effectiveness of the Compliance Risk management system formed at the Bank and ensuring promotion of the compliance culture at the Bank;

– Providing resources to CD to prevent the Prohibited Practices and Misconduct (personnel, financial, and technology resources);

– Ensuring external and internal communications with regard to the provisions of this Policy, its importance, binding nature, and need to comply with it;

– Approving the Bank's regulations and taking measures related to AML/CFT/F/C within his/her jurisdiction;

– Ensuring that the whistleblower employees who have duly fulfilled their duties to comply with the Policy's requirements shall be protected from retaliation, discrimination, or unjustified disciplinary actions;

– Reviewing reports on the Compliance Risks, results of the investigations conducted on suspicions and/or facts of the Staff's or the Counterparty's involvement in the Prohibited Practices and making decisions on them, including taking disciplinary actions;

– Approving Limits of Non-Banking Transactions for AML/CFT/F/C.

2.1.4. The jurisdiction of the Management Board covers:

– Approving the Bank's regulations and taking measures related to AML/CFT/F/C within its jurisdiction;

– Ensuring the integration of the functions related to AML/CFT/F/C into the Bank's business processes;

– Taking decisions on lending projects submitted for their consideration subject to the provisions of this Policy and taking into account the detected Compliance Risks;

– Reviewing reports on the Compliance Risks to prevent the Prohibited Practices.

2.1.5. The Committees of the Bank within their jurisdictions consider and approve transactions with the Counterparties taking into account the detected Compliance Risks.

2.1.6. The CD's functions are determined in the Bank's internal regulations, and CD:

- Prepares compliance recommendations with regard to the existing rules, standards, practices subject to their application by any other international financial organizations;
- Prepares the system of reporting on the Compliance Risks and provides the information to the Bank's governing bodies;
- Identifies, assesses, monitors, and controls the Compliance Risks in the Bank's activities, transactions and projects as well as provides the authorized bodies with recommendations how to mitigate such Risks;
- Trains and consults the Staff on compliance issues;
- Improves the regulatory frame and the Bank's Compliance Risk management system in order to enhance their effectiveness and to ensure their correspondence to the Bank's objectives and goals;
- Prepares recommendations and requirements on application of the documents that establish the standards of business conduct;
- Arranges the system of complaints and reports of the Prohibited Practices and risks thereof, including fraudulent and corrupt practices and Misconduct of the employees and third parties;
- Participates in investigation of facts or suspicions of Prohibited Practices and Misconduct.

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

2.1.8. Department heads are responsible for properly managing the risks of Prohibited Practices in accordance with the approved internal regulations of IIB.

2.1.9. The structural divisions initiating transactions with the Counterparties shall be the first line of defense for the Bank to detect and prevent the Compliance Risks.

2.1.10. The Compliance Department shall be the second line of defense and shall be responsible for detecting, assessing, controlling and reporting such Compliance Risks to the relevant governing bodies of IIB. Supporting departments shall detect and prevent the Prohibited Practices at IIB when registering, processing and monitoring transactions.

2.1.11. The Internal Control Department shall be the third line of defense and shall audit compliance of the Bank's departments, including CD, with the requirements of this Policy.

2.2. Internal Control Measures.

2.2.1. The Bank shall take necessary internal control measures for AML/CFT/F/C. However, recognizing that it is impossible to eliminate such risks, the Bank strives that the actions

it takes are reasonable and relevant and do not increase bureaucracy or do not result in excessive growth of expenses on such actions.

2.2.2. Since the Bank works in the external environment and cannot fully control changes occurring there, the internal control system for AML/CFT/F/C applied by the Bank is being continuously improved based on development of the international practices and adaptation to new challenges and risks. The Bank in its internal regulations determines a particular list of taken internal control measures.

2.2.3. The internal control measures for mitigating compliance risks are assessed for their reasonability and effectiveness in the Bank. They are assessed as part of self-assessment, internal and/or external audit at least once a year.

2.2.4. If abnormally high Compliance Risks, which cannot be fully eliminated, including through the internal control measures taken, are identified with regard to the Counterparty, project, transaction, or the Staff, the Bank strives to suspend or stop cooperation with such Counterparty or employee in the safest way.

2.2.5. If necessary, the Bank ensures that contracts and agreements with the 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. Such agreements shall also include provisions to prevent and deter the Prohibited Practices and apply Enforcement Measures.

2.3. Risk Detection and Assessment

2.3.1. The Bank detects and assesses Compliance Risks using the risk-based approach, which implies the identification of the transaction's, project's, business line's, Staff's exposure to such risks based on the results of analyzing the key factors affecting the level of such risk. A list of these factors may include the registration country, type of business, reputation, key clients, services requested, total time in business, credit history, sanctions imposed, etc.

2.3.2. The risk-based approach uses the principle of a commensurate level of a subject risk and the extent of due diligence performed in relation to such subject: the higher the risk is, the more complete and detailed information should be available to the Bank.

2.3.3. To assess the Compliance Risks, including a risk of Money Laundering, Financing of Terrorism, Fraud and Corruption and other Compliance Risks, the Bank uses the following 3-level scale, where the following risk levels are identified:

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

2.3.4. The Bank's internal regulations define criteria for assigning risk level to a Counterparty, procedures for Counterparty Identification and monitoring their transactions, a list of documents requested from the Counterparty and procedures for detecting and assessing the risk of Politically Exposed Persons. In this case, the due diligence extent and the list of requested documents and confirmations are determined depending on the Counterparty's risk level.

2.3.5. The Bank may establish criteria or 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.

2.3.6. The Compliance Risks are detected and assessed within the framework of initial Counterparty's due diligence and subsequent monitoring in accordance with the procedure established within the Bank.

2.3.7. The risks of Misconduct of the Staff are assessed based on their exposure to respective risks. Using various preventive and verification mechanisms, the Bank executes control over employees' activities, especially the activities of those who are directly involved in dealing with the Counterparties and process their transactions.

2.3.8. The Compliance Risks are detected and assessed by the Bank with regard to all new transactions, business processes and products developed by the Bank itself or proposed to it by its Counterparties and partners.

2.4. Identification

2.4.1. The Bank shall identify all Counterparties and persons involved in its projects and transactions (Know Your Customer principle).

2.4.2. The Bank establishes 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 the Counterparties, if the volume of planned transactions with the Counterparties in question does not exceed the Limit of Non-Banking Transactions established for the purposes of AML/CFT/F/C.

2.4.3. The Bank takes all required measures to confirm that a Counterparty or a third party acting on behalf of the Counterparty is exactly the person declared in the transaction documentation. These measures are a mandatory internal control tool for AML/CFT/F/C that minimizes the risks of Prohibited Practices and protects the Bank from exposure to possible financial and/or reputational risks.

2.4.4. The Know Your Customer principle implies that:

– The Bank has collected all necessary information that supports the conclusion that a Counterparty and/or a third party (if any) acting on behalf of the Counterparty, its shareholders and beneficiaries have been fully identified and all adherent risks are detected and assessed;

– The Bank has confirmation that the Counterparty and/or a third party (if any) acting on behalf of the Counterparty do not conduct any Prohibited Practices;

– The funds used in the transaction were acquired by the Counterparty and/or a third party (if any) acting on behalf of the Counterparty not as a result of the Prohibited Practices or a violation of applicable restrictions or any other violations;

– The members, beneficiaries and top management of the Counterparty and a third party (if any) acting on behalf of the Counterparty have been cleared against specialized compliance lists of international organizations or individual countries;

– The Bank has confirmation that the Counterparty is acting in its own interests or on behalf of third parties.

2.4.5. Depending on the risk assigned to a Counterparty, the Bank may frame the Counterparty Identification process in accordance with a simplified, standard or enhanced procedure (applicable to high-risk Counterparties). In this case, the Bank may define criteria based on compliance therewith, regardless of the general Counterparty's risk level, such that the Identification process may follow simplified, standard or enhanced procedures or may ultimately be omitted.

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

2.4.7. The Bank refuses to execute transactions with the Counterparties related to financial institutions that fail to apply AML/CFT measures. The Bank establishes no relationships with financial organizations, which have no physical presence in the states of their legal address (so called "shell banks") or with the Counterparties acting on their behalf and opens no accounts in the name of any anonymous holders. In this case, the Bank does not cooperate with the organizations making the above transactions either.

2.4.8. The Bank strives to identify agents of the Counterparties and, if a Counterparty or its agents act for the benefit of third parties, the Bank also identifies the third parties.

2.5. Monitoring and Self-Assessment of the Compliance Risks

2.5.1. In order to identify and control the Compliance Risks, the Bank regularly monitors the activities of the Staff, the Counterparties and the persons involved in the Bank's project.

2.5.2. The Bank uses various monitoring procedures, where scope and frequency depend on the level (type) of risk assigned to a Counterparty and the Staff's exposure to the Counterparty's transactions. In addition, the applied monitoring procedures at the Bank depend on the availability of automated system within the Bank and particular transaction parameters or Counterparty categories.

2.5.3. The mandatory element of monitoring of the Compliance Risks of the Bank's Counterparty and projects is to trace occurring changes based on the information received from the Counterparty itself, from the mass media and the dedicated databases.

2.5.4. The Counterparties are monitored by the Bank (the first and the second lines of defense) on an ongoing basis. This information is constantly updated in the Bank's record keeping systems.

2.5.5. To identify the Prohibited Practices, the Bank develops and applies transactional and situational attributes that may serve as a basis for suspecting that the Counterparty and/or the Staff are applying the Prohibited Practices.

2.5.6. If necessary, the Bank takes internal control measures aimed at identifying gaps and deficiencies in IIB's internal procedures, which may result in realization of the Compliance Risks.

2.5.7. If deemed feasible, the Bank may conduct the integrity review of the bank products and the projects implemented with the Counterparties. The objective of such review is to identify the Compliance Risks not detected previously, to check effectiveness of the implemented internal control measures for AML/FT/F/C, to determine actual non-performance of the basic provisions of the agreements/contracts entered into, etc.

The frequency of such integrity reviews shall be established by the Bank as may be required in light of the Compliance Risks identified in relation to the Bank's products and projects.

2.5.8. In order to assess the effectiveness of the Compliance Risk management system, the Bank develops the control system that, among other things, can include assessment of training effectiveness, duty distribution effectiveness, internal control implementation effectiveness, etc. The results of such control, including within the reports of internal and external auditors, are considered by the Bank's governing bodies and used to improve the Compliance Risk management system.

2.5.9. The Bank regularly self-assesses the Compliance Risks assumed. They are self-assessed subject to the special status of the Bank as a supranational organization, subject to the applied business model and the objectives of its activities, its scale, areas and sectors of transactions as well as subject to any other factors that may influence its exposure to the Compliance Risks assumed.

2.5.10. As part of self-assessment of the Compliance Risks, the Bank determines the types and levels of internal controls applied to each identified risk and assesses their effectiveness and need for improvement.

2.6. Work with the Staff

2.6.1. When hiring the Staff, the Bank enters into employment and civil law agreements only with those persons, who confirm to comply with the requirements of this Policy.

2.6.2. When hiring the Staff, the Bank takes certain actions to obtain confirmations that their past and future activities comply with the requirements of this Policy and other IIB's documents on compliance, including based on regularly filled-in compliance questionnaires.

2.6.3. The Bank regularly trains its Staff, which, among other things, include description of the Compliance Risks and how they may cause damage to the Bank, how to identify them, what actions should be taken to mitigate the Compliance Risks, description of the ethical rules of conduct

established at the Bank, etc. The training is based on the approved procedure for the set categories of the Staff in accordance with the program developed and updated by the Bank taking into account trainees' professional activities and positions as well as the level of knowledge they should attain.

2.6.4. In order to prevent the Compliance Risks, following the trainings, the Bank determines the level of the Staff's knowledge necessary to mitigate the Compliance Risks and, if required, provides additional training.

2.6.5. To ensure integrity in its activities, the Bank may provide training, including engaging third party specialists, to staff of its Counterparties and any other persons involved in the Bank's projects.

2.6.6. The Bank takes relevant measures to protect whistleblowers, who report on the Counterparties and/or the Staff suspected of or actually performing the Prohibited Practices.

2.7. Enforcement Measures

2.7.1. In order to prevent and combat the Prohibited Practices, the Bank incorporates clauses on enforcement measures for violation of the compliance requirements in its agreements/contracts and accordingly applies sanctions to wrongdoers.

2.7.2. The Bank includes certain remedies in financing agreements for dealing with breaches that may consist of disbursement suspensions or early reimbursements, suspension or refusal to cooperate.

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

2.7.4. IIB may exclude a Counterparty or any other entities or persons from participating in IIB's activities or its projects if they are found to be involved in the Prohibited Practices or are included in lists of excluded entities that are filed with international organizations.

2.8. Investigation of the Prohibited Practices

2.8.1. The Bank reviews and checks information regarding the suspected involvement of the Counterparties and/or the Bank's Staff in the Prohibited Practices. Any material concerns related to the Prohibited Practices or Misconduct shall be promptly reported to the authorized bodies of the Bank in accordance with the requirements of the internal regulations.

2.8.2. When receiving and assessing the information received on the identified Compliance Risks, the Bank takes into account the investigation standards adopted by the international financial institutions and, based on such standards, prepares the relevant internal regulations.

2.8.3. The Bank may investigate concerns voiced by any anonymous source.

2.8.4. The Bank prohibits to apply to the Staff that in good faith reported of the identified facts or suspicions of performing the Prohibited Practices any retaliation measures, discrimination, disciplinary, or similar actions.

3. HANDLING INFORMATION AND ENSURING CONFIDENTIALITY

3.1. Handling information

3.1.1. When requesting information from its Counterparties for internal control arrangements for AML/CFT/F/C, the Bank takes appropriate measures to reduce the risk of receiving invalid or outdated information.

3.1.2. When collecting information for executing internal control for the purposes of AML/CFT/F/C, the Bank uses the data received from a Counterparty. Information from third parties and electronic data are only used by the Bank 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, information from the supervisory bodies, regulators, state registration chambers and agencies particularly formed to check data from portals of state authorities.

3.1.3. The Bank ensures that the information received during implementation of this Policy is properly stored during the storage period set forth in Rules 3.

3.2. Confidentiality

3.2.1. The Bank treats any information obtained about a Counterparty, the Staff and the transactions with them, information about the Counterparties or the Staff suspected of performing the Prohibited Practices as confidential information.

3.2.2. The Bank does not disclose information about the persons reporting the Counterparties and/or the Bank's Staff suspected of or actually performing the Prohibited Practices, except when such persons themselves request to disclose such information.

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

4. LIST OF REFERENCES

1. Code of Conduct (ОНД-32) (current edition, being updated).
2. Staff Regulations on Employment Terms of International Investment Bank Employees (ПДК-53) approved by Order No. 13 dated February 01, 2016 (as updated).
3. IIB's Rules on Document Management (ПДК-84) approved by an Order No. 45 dated May 28, 2015.
4. Procedure for Receiving and Handling Complaints at International Investment Bank (ПДК-69) approved by Order No. 50 dated May 17, 2016.

5. LIST OF REGULATORY DOCUMENTS BECOMING VOID UPON ADOPTION OF THIS DOCUMENT

With the adoption of this document, the «Policy on Anti-Money Laundering, Combating the Financing of Terrorism, Fraud and Corruption» approved by the Protocol of the 106th IIB Council Meeting dated December 9, 2016 becomes void.