Appendix to Minutes 212 of
the Meeting of the Council of
the Eurasian Development Bank
dated 16 April 2024

COMPLIANCE CONTROL FRAMEWORK OF THE EURASIAN DEVELOPMENT BANK

TABLE OF CONTENTS

ARTICLE 1. GENERAL PROVISIONS

1.1. This Compliance Control Framework of the Eurasian Development Bank has been developed in accordance with the Charter of the Eurasian Development Bank and universally recognised principles and norms of international law contained in the documents of the United Nations, based on recommendations and documents of the Financial Action Task Force, the Eurasian Group on Combating Money Laundering and Financing of Terrorism, the Basel Committee on Banking Supervision at the Bank for International Settlements, and practices applied by the World Bank and banks within its Group as well as Wolfsberg Group banks, and sets out the main goals, objectives, principles, guidelines and arrangements of the Eurasian Development Bank's ("Bank") Compliance Control system.

1.2. The Compliance Control system shall be based on the "three lines of defence" model, which ensures that all Bank divisions are involved in monitoring, evaluating and controlling risks.

1.3. The functioning and development of the Bank's compliance control system shall be based on a Compliance Culture.

1.4. This Framework shall apply to the activities of all Bank divisions and shall be read and applied by all Bank employees.

ARTICLE 2. GENERAL TERMS, DEFINITIONS AND ABBREVIATIONS

"Chief Compliance Officer" means a manager who reports to the Chairman of the Bank's Management Board and directly coordinates and supervises the activities of the Bank's division responsible for Compliance Control, as well as other Bank divisions, excluding business units.

"Prohibited Practices" means any of the following:

"Obstruction" means knowingly destroying, falsifying, substituting or concealing information material to an audit, or providing false information to persons conducting audits to substantially impede the establishment of facts of corruption, fraud, coercion or collusion, and/or threatening, harassing or intimidating any person to prevent the obtaining of information relevant to these facts, or actions aimed at creating substantial obstacles to the Bank's exercise of its rights to conduct any audits or inspections as provided by the documents regulating the Bank's activities or contracts entered into by the Bank.

"Corruption" means the abuse of official position, giving or taking a bribe, abuse of authority, commercial bribery or other illegal use by a Bank employee of their official position contrary to the interests of the Bank and/or its member states to obtain a benefit in the form of money, valuables, other property or services of a proprietary nature, other proprietary rights for themselves or for third parties, or illegal provision of such benefit to said persons by other individuals.

"Fraud" means any act or omission, including misrepresentation of facts or information, which intentionally or unintentionally misleads or results in attempts to mislead a person to obtain a financial or other benefit or evade an obligation.

"Coercion" means causing damage and/or harm or threatening to cause damage and/or harm, directly or indirectly, to any person or their property to influence their actions.

"Collusion" means an agreement between two or more persons to achieve an improper purpose, including improperly influencing the actions of another person.

"Compliance Control" means a series of measures, including rules, methods and procedures implemented by the Bank on an ongoing basis to effectively manage Compliance Risk, timely identify, prevent where possible and monitor conditions and circumstances relating to the occurrence of Compliance Risk in the course of the Bank's

ongoing activities, as well as to take corrective measures and improve controls adequate to the identified and/or potential risks.

"Compliance Culture" means a model of behaviour based on a commitment to the Bank's corporate values, respect for the Bank's interests, adherence to ethical norms and rules of conduct, avoidance of Prohibited Practices, and knowledge of and compliance with the Bank's internal regulatory documents.

"Compliance Risk" means the Bank's risk of significant financial losses or full or partial loss of its business reputation due to non-compliance with regulations, including the Bank's internal regulatory documents, the Bank's obligations under agreements and contracts, or professional standards.

"Divisions" means the structural and territorial divisions of the Bank.

"Sanctions" means any economic, financial or trade restrictions, including prohibitions on the use of funds or other property imposed or enforced by the United Nations, including the United Nations Security Council, laws, decrees, regulations, resolutions, rules or other statutes or judicial decisions of competent authorities or agencies, interstate groupings or individual nations, non-compliance with which may result in a breach by the Bank of its obligations, the imposition of Sanctions on the Bank, substantial damage to the Bank's business reputation and/or limitations on the Bank's ability to conduct its business.

"Sanctions List" means the Consolidated United Nations Security Council Sanctions List, the OFAC's Specially Designated Nationals and Blocked Persons List, the OFAC's Foreign Sanctions Evaders List, the EU Consolidated List of Sanctions, the UK Sanctions List or another list with a similar level of prohibitions established by the competent authorities of interstate grouping or individual states, in the event that the Bank becomes obliged to comply with the Sanctions imposed by that state.

ARTICLE 3. COMPLIANCE CONTROL GOALS, OBJECTIVES AND PRINCIPLES

3.1. The main goals of Compliance Control shall be to:

3.1.1. Create conditions for the Bank's sustainable development through Compliance Risk management;

3.1.2. Minimise the risk of financial loss and the total or partial loss of the Bank's business reputation; and

3.1.3. Promote a Compliance Culture.

3.2. The main objectives of Compliance Control shall be to:

3.2.1. Ensure that the Bank's activities comply with generally recognised principles and norms of international law, ethical norms of behaviour and business conduct, professional standards and laws applicable to the Bank's operations;

3.2.2. Ensure that the Bank and its employees comply with the provisions of the Bank's constituent documents and agreements on the Bank's presence with the governments of the Bank's member states, as well as agreements with central/national banks and other authorised bodies of the Bank's member states and the Bank's internal regulatory documents.

3.2.3. Safeguard the legal rights of the Bank's shareholders, investors, clients and other counterparties.

3.2.4. Prevent the Bank, its management bodies and employees from becoming intentionally or unintentionally involved in illegal activities, especially money laundering, financing of terrorism, corruption, fraud, unlawful use of insider information and market manipulation, Prohibited Practices or any other activity considered illegal in the

territories/jurisdictions where the Bank operates or recognised as such by international treaties and the Bank's internal regulatory documents.

3.2.5. Prevent the Bank from becoming involved in political activities, funding political parties or politically biased non-profit organisations, unions and foundations.

3.2.6. Organise effective interaction among Bank employees and divisions in the process of Compliance Control.

3.3. The implementation of Compliance Control shall be based on the following principles:

3.3.1. Independence: Compliance Risk management measures shall be developed by an independent division that has no business functions or other responsibilities that could lead to a conflict of interest between Compliance Risk management duties and other employee duties.

3.3.2. Continuity: Compliance Control shall be carried out on an ongoing basis, ensuring continuity in the management of Compliance Risk.

3.3.3. Comprehensiveness: Compliance Control shall cover all areas of the Bank's activities.

3.3.4. Relevance: the Compliance Control function shall be adequately resourced to manage Compliance Risk, including having employees with a high level of professional competence and resources that ensure Compliance Risk management aligns with the current level of the Bank's development.

ARTICLE 4. PARTICIPANTS IN THE COMPLIANCE CONTROL SYSTEM AND THEIR ROLES AND RESPONSIBILITIES

4.1. The participants in the Compliance Control system are the Council of the Bank, the Management Board of the Bank, the Chief Compliance Officer, the Bank's division responsible for Compliance Control, the Internal Audit Service and other Bank divisions.

4.2. The Bank's Council shall:

- ensure the establishment and operation of the Bank's Compliance Control system;

- approve this Framework and, where necessary, give instructions to amend or supplement it;

- receive and review information on the functioning of the Compliance Control system as part of the Bank's quarterly and annual reports; and

- take Compliance Risks into account when approving the Bank's investment projects within the competence of the Bank's Council.

4.3. The Bank's Management Board shall:

- ensure the implementation of this Framework;

- set priorities for the development and improvement of the Bank's Compliance Control system.

- review and approve the Bank's internal regulatory documents aimed at implementing this Framework;

- take Compliance Risks into account when approving investment projects and other Bank transactions; and

- make decisions aimed at managing Compliance Risk in cases submitted for consideration of the Bank's Management Board by the Chief Compliance Officer.

4.4. The Chief Compliance Officer shall:

- coordinate and supervise the functioning of the Compliance Control system at the Bank;

- review and decide on measures to respond to violations and complaints identified through Compliance Control activities;

- make operational decisions aimed at managing Compliance Risk; and

- submit for consideration of the Bank's Management Board any issues which, in accordance with the Bank's internal regulatory documents, fall within the competence of the Management Board.

4.5. The Bank division responsible for Compliance Control shall:

- develop internal regulatory documents aimed at managing Compliance Risk based on this Framework;

- conduct Compliance Control measures to prevent the occurrence of and minimise Compliance Risk;

- coordinate the activities of Bank divisions for the purposes of Compliance Risk management; and

- train Bank employees in Compliance Control.

4.6. The roles of Bank divisions in Compliance Risk management shall be determined by their place in the "three lines of defence" model:

4.6.1. Divisions whose activities may create Compliance Risks ("first line of defence") shall identify possible Compliance Risks when preparing transactions/operations, developing new products or services or promoting cooperation with clients or other counterparties. "First line of defence" divisions shall implement measures to minimise and manage emerging risks by, *inter alia*, ensuring that documents and information necessary to perform due diligence on clients and other counterparties are made available and that client and other counterparty information is kept up to date.

4.6.2. Divisions that support business operations in terms of risk assessment ("second line of defence") shall identify and assess risks in their area of responsibility and monitor compliance with established limits, fostering a Compliance Culture;

4.6.3. The IAS, as the "third line of defence," shall independently assess the functioning of the Compliance Control system and evaluate the quality of Compliance Procedures and Compliance Risk management processes in line with its work plan.

ARTICLE 5. CLASSIFICATION OF KEY COMPLIANCE RISKS

5.1. Risk of involvement in activities/operations related to money laundering, the financing of terrorism or the financing of the proliferation of weapons of mass destruction:

5.1.1. The Bank's member states criminalise activities aimed at money laundering and the financing of terrorism or the proliferation of weapons of mass destruction.

5.1.2. To minimise this risk, the Bank shall:

- not open or maintain accounts in the name of anonymous holders or persons using fictitious names/pseudonyms, or establish relationships with banks that open or maintain such accounts;

- not establish or maintain relationships with banks that do not have permanent governing bodies in the territories of the states in which they are registered;

- not serve persons who have not provided the necessary documents or information for identification, including their representatives or beneficial owners;

- reserve the right to refuse service to persons listed as entities and individuals associated with the financing of terrorism and extremism, as well as those suspected of using their accounts for transactions or operations related to money laundering, financing of terrorism or financing the proliferation of weapons of mass destruction;

- implement the Know Your Customer (KYC) principle to identify clients and other counterparties, their representatives, beneficiaries and beneficial owners, as well as public officials who are members of governing bodies or beneficial owners of clients or other counterparties, and shall regularly update and verify the information and data obtained for identification purposes;

- monitor and control transactions on client accounts, including those of respondent banks; and

- at least once a year, conduct training for Bank employees involved in maintaining client accounts, servicing clients and conducting transactions on financial markets, as well as other Bank employees to combat money laundering, financing of terrorism and financing the proliferation of weapons of mass destruction.

The Bank shall not establish relationships with persons incorporated or located in states/territories that do not comply with the Financial Action Task Force recommendations.

5.1.3. All documents and information obtained in the process of identifying and examining clients and other counterparties, as well as information on client transactions, shall be carefully documented and kept for at least five years from the date of termination of the relationship with them.

5.1.4. The Bank shall take all necessary measures to combat money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

5.2. Risk of breaching applicable Sanctions laws:

5.2.1. The Bank shall not enter into business relationships with persons subject to Sanctions if such relationships contravene the Bank's obligations to investors and creditors and/or may result in the imposition of Sanctions on the Bank, cause substantial damage to the Bank's business reputation or limit the Bank's ability to conduct its business.

5.2.2. The Bank shall not engage in transactions or dealings which, in the Bank's opinion, may violate and/or be aimed at circumventing applicable Sanctions laws, and thereby cause substantial damage to the Bank's business reputation and limit the Bank's ability to conduct its business. The Bank shall establish into business relationships with persons on the Sanctions Lists or subject to other Sanctions if such relationships violate applicable Sanctions laws and/or conflict with the Bank's obligations to investors and creditors.

5.2.3. The Bank shall ensure compliance with applicable Sanctions laws by:

- implementing multi-stage controls for checking all of the Bank's clients, other counterparties and other parties to transactions/dealings against the Sanctions lists;

- closely monitoring Sanctions laws, including amendments and additions thereto;

- timely updating the Sanctions lists in the Bank's systems;

- conducting detailed analyses of transactions subject to applicable Sanctions laws and the Bank's obligations to investors and creditors;

- implementing automated online checks of all transactions against the Sanctions lists.

5.3. Risk of using Prohibited Practices:

5.3.1. The Bank shall demonstrate zero tolerance towards involvement in Prohibited Practices, develop a system of corporate values based on integrity, transparency, trust, professional responsibility and intolerance of corruption and bribery, not accept any use of Prohibited Practices, and communicate this position to clients and other counterparties.

5.3.2. The implementation of the system of corporate values, principles of business communication and conduct for all Bank employees in the course of their official duties, interactions with clients and other counterparties, and the framework for dealing with violations of ethical and professional standards shall be governed by the Eurasian Development Bank's Business Ethics Regulations.

5.3.3. Bank employees shall not:

- accept any property benefits or advantages (including payment for holidays, medical treatment, foreign tourism, health trips, etc.) for themselves, their close relatives or acquaintances from the Bank's clients or other counterparties, including potential ones, and/or employees of any parties involved in a transaction with the Bank, and/or officials, international or public servants, and close relatives of said persons;

- receive gifts (including in the form of services) from clients or other counterparties and/or their employees in connection with the performance by Bank employees of their official duties unless they comply with the general rules for dealing with business gifts and their value does not exceed one hundred (100) US dollars or the equivalent in another currency;

- receive any part of disbursements on loans provided by the Bank and/or amounts under treasury transactions;

- provide undue advantages to third parties; or

- use any benefits, privileges or immunities granted by the Bank due to their official position for personal enrichment or the enrichment of their close relatives.

5.3.4. The Bank shall take reasonable and available measures under the circumstances to detect, prevent and discontinue Prohibited Practices.

5.3.5. Procurement of goods and services for the Bank's needs shall be based on the principles of equal opportunities, transparent relationships, competitiveness and the best quality standards to prevent the possibility of any corrupt practices and to obtain goods and services of the best quality at a price acceptable to the Bank, with the ability to choose suppliers.

5.3.6. The Bank shall take due care to ensure that its sponsorships and charitable donations (where such activities may be carried out by the Bank) do not serve as a cover for bribes.

5.3.7. The Bank's human resource policies shall be based on its corporate values, and all Bank employees shall be subject to the same approaches regarding recruitment, remuneration, job assignment, training and performance appraisal, excluding any corruption practices.

5.3.8. The Bank does not tolerate bribery in international commercial transactions, including investments.

5.3.9. Bank officials or other employees shall not offer, promise, provide or transfer directly and/or through intermediaries any values and/or non-property advantages to influence a client, another counterparty or a public authority to obtain or retain a commercial or other advantage in transactions.

5.3.10. Employees shall be assured that none of them will be demoted, penalised or harmed in any way for refusing to pay a bribe, even if it results in a loss of business for the Bank.

5.4. Risk of conflict of interest:

5.4.1. A conflict of interest, where the Bank fails to proactively identify, prevent and resolve situations with indications of conflicts of interest, creates grounds for financial and reputational risks.

5.4.2. The Bank shall adhere to a policy of openness in identifying, preventing and resolving conflicts of interest.

5.4.3. The methods used by the Bank to identify, assess and manage conflicts of interest shall be established by the Bank's Management Board.

5.5. Risk of misuse of insider information and market manipulation:

5.5.1. Misuse of insider information and market manipulation undermines fair pricing of financial instruments, foreign currencies and commodities, leads to unequal treatment of investors and destroys investor confidence.

5.5.2. The Bank shall take all necessary measures to combat the misuse of insider information and prevent market manipulation, including by establishing a ban on the transfer of insider information to unauthorised persons and prohibiting the distribution of knowingly false information and transactions aimed at misleading market participants regarding the price of financial instruments, foreign currencies or commodities.

5.5.3. The Bank shall take necessary measures to prevent and minimise risks associated with the possession and use of insider information received from other entities that have designated the Bank as an insider and have transferred their insider information to the Bank.

5.5.4. The Bank shall protect insider information from entities who have designated the Bank as an insider and implement measures to diversify information flows to prevent insider information leakage and misuse.

ARTICLE 6. KEY COMPLIANCE CONTROL TOOLS

6.1. To manage its Compliance Risk, the Bank shall use the following key Compliance Control tools.

6.1.1. Process regulation: the Bank's Management Board has developed and implements internal regulatory documents governing banking operations and transactions, labour relations with Bank employees and other areas of Bank activities, providing for the necessary Compliance Control measures where appropriate.

6.1.2. Communicating the Bank's zero tolerance towards Prohibited Practices to clients and other counterparties, including by incorporating relevant provisions in contracts and agreements. The Bank reserves the right to take any relevant measures, including terminating contractual relations with a client or other counterparty if any Prohibited Practices are identified in their operations, and to claim damages, including reputational damage, caused to the Bank by the use of Prohibited Practices.

6.1.3. Expertise of employees of the division responsible for Compliance Control: to effectively manage Compliance Risks, employees of the division shall be directly involved in client due diligence, project and transaction analysis, and transaction monitoring and analysis. Assessing the level of client or counterparty Compliance Risk and project risks and considering these risks in interactions with clients and other counterparties ensures the implementation of a risk-oriented business model.

6.1.4. Analysis of external and internal data, including complaints and enquiries: the Bank shall analyse information and data, including publications in the media, other

trustworthy external sources, as well as enquiries or complaints received by the Bank about instances of abuse, misconduct, wrongdoing or improper conduct by Bank employees or in connection with Bank activities, including those received through the Compliance Hotline, to which reports of violations and abuses can be directed.

6.1.5. Informing the Bank's management and supervisory bodies: information on all aspects of the functioning of the Compliance Control system shall be communicated to the Bank's management and supervisory bodies, including as part of quarterly and annual reports to the Bank's Council, which shall include information on compliance measures implemented during the reporting period.

6.2. Bank employees shall comply with this Framework and promote a Compliance Culture. Violation by a Bank employee of this Framework or internal regulatory documents of the Bank adopted in pursuance of this Framework may result in disciplinary penalties in accordance with the Human Resources Framework of the Eurasian Development Bank; in the event of a proven violation of Prohibited Practices by a Bank employee, the Bank may, in addition to disciplinary penalties, require the employee to compensate for any illegally obtained benefits and reputational damage caused to the Bank.

ARTICLE 7. FINAL PROVISIONS

7.1. This Framework shall take effect on the date the Bank's Council approves it by adopting the relevant resolution.

7.2. This Framework may be amended as necessary, in the cases and in accordance with the procedure established by the Bank's Council.