Annex 8
to Minutes 990 of the Meeting of the
Management Board
of the Eurasian Development Bank
dated 8 September 2022

APPROVED BY
the Management Board of the Eurasian
Development Bank
(Minutes 990 dated 8 September 2022)

COMPLIANCE CONTROL FRAMEWORK
OF THE EURASIAN DEVELOPMENT BANK
# TABLE OF CONTENTS

1. **Abbreviations and Definitions**
   - 1.1. Abbreviations
   - 1.2. Terms and Definitions
   - 1.3. Terms and Definitions Used Exclusively in This Framework

2. **Intended Use and Scope**
   - 2.1. Intended use
   - 2.2. Scope, owner and revisions

3. **General Provisions**
   - 3.1. Compliance control goals
   - 3.2. Compliance control objectives
   - 3.3. Compliance Control Principles

4. **Classification of Key Compliance Risks**
   - 4.1. Risk of involvement in ML/FT/FPWMD-related activities/transactions
   - 4.2. Risk of breaching applicable Sanctions laws
   - 4.3. Corruption risk
   - 4.4. Risk of conflict of interest
   - 4.5. Risk of non-compliance with applicable tax discipline laws
   - 4.6. Risk of misuse of insider information and market manipulation

5. **Compliance Control Arrangements and Key Tools**
   - 5.1. Setting up a compliance control system
   - 5.2. Key compliance control tools

6. **Roles and Responsibilities**
   - 6.1. The Bank’s Management Board
   - 6.2. Chief Compliance Controller
   - 6.3. SCCD
   - 6.4. Bank divisions
1. Abbreviations and Definitions

The definitions of terms, abbreviations, and abbreviated names of the Bank’s divisions as used in this Compliance Control Framework of the Eurasian Development Bank (“Framework”) are provided in the Bank’s Glossary.

1.1. Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML/FT/FPWMD</td>
<td>Money laundering/financing of terrorism/financing of proliferation of weapons of mass destruction</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-money laundering and countering the financing of terrorism</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
</tbody>
</table>

1.2. Terms and Definitions

The following terms and definitions are used in this Framework:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Compliance Controller</td>
<td>A senior manager who reports to the Chairman of the Bank’s Management Board and directly coordinates and supervises the activities of the Bank’s SCCD and other divisions, excluding business units.</td>
</tr>
<tr>
<td>Business Gift</td>
<td>Any tangible or intangible valuable thing for which there is no obligation to pay the usual price, received by or given to a Bank employee in connection with the performance of his or her official duties.</td>
</tr>
<tr>
<td></td>
<td>A business gift can be in the form of benefits or services resulting in financial benefits (such as work, services, payment for entertainment, recreation or travel expenses, loans, discounts, provision of property, including housing, charitable contributions, donations, etc.) or an entertainment or educational event.</td>
</tr>
<tr>
<td>Client</td>
<td>A legal or unincorporated entity that uses the Bank’s services, or persons who plan to use the Bank’s services.</td>
</tr>
<tr>
<td>Compliance control</td>
<td>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 take corrective measures and improve controls adequate to the risks identified.</td>
</tr>
<tr>
<td>Compliance culture</td>
<td>A model of behaviour based on a commitment to the EDB’s corporate values, respect for the Bank’s interests, adherence to ethical norms and rules of conduct, and knowledge of and compliance with the Bank’s internal regulatory documents.</td>
</tr>
<tr>
<td>AML/CFT officer</td>
<td>An employee in charge of arranging ML/FT risk management and monitoring compliance with the Eurasian Development Bank’s Internal Control Rules to Counter Money Laundering and the Financing of Terrorism.</td>
</tr>
</tbody>
</table>
### 1.3. Terms and Definitions Used Exclusively in This Framework

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank, EDB</td>
<td>Eurasian Development Bank, its headquarters and territorial divisions</td>
</tr>
<tr>
<td>Subsidiary (company)</td>
<td>An organisation whose decisions are or may be determined by the EDB by virtue of its predominant shareholding in the company’s share capital</td>
</tr>
<tr>
<td>EDB Group</td>
<td>EDB, Subsidiaries and their subsidiary companies</td>
</tr>
<tr>
<td>Sanctions</td>
<td>Any economic, financial or trade restrictions, including those 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 of the United States, the European Union, the United Kingdom, Switzerland, Japan or any other state, non-compliance with which may result in a breach of the Bank’s obligations or imposing sanctions on the Bank, cause substantial damage to the Bank’s business reputation and/or limit the Bank’s ability to carry out its business activities.</td>
</tr>
<tr>
<td>Sanctions List</td>
<td>Consolidated United Nations Security Council Sanctions List, the OFAC’s Specially Designated Nationals and Blocked Persons List, the OFAC’s Foreign Sanctions Evaders List, EU Consolidated List of Sanctions, the UK Sanctions List or another similar level of restrictions or prohibitions established by the competent authorities of the United Nations, the European Union and its Member States, the United States, the United Kingdom, Switzerland, Japan, the EDB member states or other states, in the event that the Bank becomes obliged to comply with the Sanctions imposed by that state.</td>
</tr>
</tbody>
</table>
2. Intended Use and Scope

2.1. Intended use
This Compliance Control Framework of the Eurasian Development Bank ("Framework") has been developed in accordance with the EDB’s constituent documents, taking into account 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 World Bank, the Wolfsberg Group and the Basel Committee on Banking Supervision at the Bank for International Settlements and sets out the main goals, objectives, principles, guidelines and arrangements of the Bank’s compliance control system.

2.2. Scope, owner and revisions
2.2.1. This Framework shall govern the Bank’s activities and relationships with EDB Group companies on compliance matters.
2.2.2. This Framework shall take effect, apply and be amended or revoked in accordance with the Regulations on the Eurasian Development Bank’s Internal Regulatory Documents.
2.2.3. The EDB’s internal regulatory documents on compliance control shall be consistent with the provisions of this Framework.
2.2.4. The owner of this Framework shall be the SCCD.
2.2.5. This Framework shall be revised if the owner of the respective internal regulatory documents is reorganised and assigns its functions relating to the administration of this Framework to other Bank divisions, or if any provisions of this Framework need to be updated and/or clarified, however not less than once every three years.


3.1. Compliance control goals
3.1.1. Compliance control shall be an integral part of the Bank’s internal control and risk management system and shall be continuously implemented at all levels within the competence of the Bank’s management bodies, officials, collegial bodies and divisions and functional responsibilities of Bank employees.
3.1.2. The main goals of compliance control shall be to:
   - create conditions for the Bank’s sustainable development through compliance risk management;
   - minimise the risk of financial loss and total or partial loss of the Bank’s business reputation; and
   - promote compliance culture.

3.2. Compliance control objectives
3.2.1. Ensuring that the Bank’s activities comply with generally recognised principles and norms of international law, ethical norms of behaviour and business conduct, professional standards of operations, integrity and lawfulness, as well as compliance with the Bank’s documents.
3.2.2. Ensuring that the Bank and its employees comply with the provisions of the Bank’s constituent documents and agreements on the Bank’s presence concluded 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, observe the legal rights

---

1 An association of major banks (ABN AMRO, Banco Santander Central Hispano, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, UBS) developing international guidelines and principles to combat corruption and money laundering through the global financial system.
of the Bank’s members, investors and Clients/Counterparties, and comply with the Bank’s internal documents.

3.2.3. Preventing the Bank, its management bodies and employees from becoming intentionally or unintentionally involved in illegal activities, especially money laundering, financing of terrorism, corruption, fraud, use of insider information, production, transportation and distribution of drugs and weapons of any kind, irreparable environmental and/or social damage to territories and communities resulting from Bank projects, or any other activity that is considered illegal in the territories/jurisdictions in which the Bank operates or that is recognised as such in international treaties and the Bank’s internal regulatory documents.

3.2.4. Ensuring ethical behaviour and business conduct, integrity and compliance with generally accepted principles, rules and standards of international financial markets and applicable law.

3.2.5. Assisting Bank divisions in preventing the disclosure of bank secrecy and confidential information.

3.2.6. Preventive identification and resolution of conflicts of interest.

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

3.2.8. Ensuring that the Bank, its management bodies and employees take action to implement this Framework and other internal regulatory documents, including through regular retraining of existing staff and training of newly hired staff on compliance risks and compliance controls, and ensuring effective interaction between Bank employees and divisions in the implementation of compliance controls.

3.2.9. Ensuring interaction with the relevant Authorised Bodies on matters related to the implementation of compliance control, in particular in respect of AML/CFT and anti-corruption.

3.2.10. Ensuring interaction with Financial Institutions as well as other market participants in the exchange of information relating to compliance control.

3.3. Compliance Control Principles

3.1. The compliance control system shall be based on the “three lines of defence” model, which ensures that all Bank divisions are involved in accepting, evaluating and controlling risks.

3.2. The implementation of compliance control shall be based on the following principles:

3.2.1. Independence. Compliance risk management measures shall be developed by an independent division, which has no business functions or other areas of work that could lead to a conflict of interest between compliance risk management duties and other employee duties.

3.2.2. Continuity. Compliance control shall be carried out on an ongoing basis, ensuring continuity in the management of compliance risk.

3.2.3. Inclusivity. Compliance control shall cover all areas of the Bank’s activities.

3.2.4. Relevance. The compliance function shall be adequately resourced to manage compliance risk, including the availability of employees with a high level of professional competence. The resources allocated shall enable compliance risk to be managed at a level corresponding to the Bank’s current level of development.

4. Classification of Key Compliance Risks

4.1. Risk of involvement in ML/FT/FPWMD-related activities/transactions

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

4.1.2. To minimise the risk of ML/FT/FPWMD, 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 Clients who have not provided the documents or information necessary to identify them, as well as their representatives or beneficial owners;
- reserve the right to refuse to service persons on the lists of entities and persons associated with the financing of terrorism and extremism, as well as persons who are suspected that the accounts they open may be used for ML/FT/FPWMD-related transactions;
- by implementing the KYC principle, identify Clients and Counterparties, their representatives, beneficiaries and beneficial owners as well as public officials who are members of governing bodies or beneficial owners of Clients/Counterparties, and shall regularly update and verify the information and data obtained for identification purposes;
- monitor and control transactions on Clients’ accounts, including those of respondent banks; and
- at least once a year, conduct AML/CFT training for Bank employees involved in maintaining Clients’ accounts, servicing Clients, conducting transactions on financial markets, etc.

4.1.3. The Bank shall have no relationships with persons incorporated/located in states/territories that do not comply with FATF recommendations.

4.1.4. All documents and information obtained in the process of identifying and examining Clients and 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 relationships with the relevant Client/Counterparty.

4.1.5. The Bank and EDB Group financial institutions shall take all necessary measures to combat money laundering and the financing of terrorism or the proliferation of weapons of mass destruction.

4.2. Risk of breaching applicable Sanctions laws

4.2.1. The Bank shall not enter into business relationships with persons subject to Sanctions if such business relationships are contrary to 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.

4.2.2. The Bank shall not engage in transactions or dealings which, in the opinion of the Bank, may violate applicable Sanctions laws 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 not enter into business relationships with persons on the Sanctions Lists or subject to other Sanctions if such business relationships violate applicable Sanctions laws and/or conflict with Bank’s obligations to investors and creditors.

4.2.3. The EDB shall ensure compliance with applicable Sanctions laws by:
- implementing multi-stage controls for checking all of the Bank’s Clients/Counterparties and other parties to transactions/dealings against the Sanctions lists;
- closely monitoring Sanctions laws and amendments and additions thereto;
- timely updating the Sanctions lists in the Bank’s systems;
- conducting a detailed analysis of transactions, subject to applicable Sanctions laws and the Bank’s obligations to investors and creditors; and
- implementing automated online checks of all transactions against the Sanctions lists.
4.3. Corruption risk

4.3.1. The Bank shall adhere to a system of corporate values based on integrity, transparency, trust, professional responsibility and intolerance of corruption and shall communicate its position of intolerance of corruption to its Clients/Counterparties.

4.3.2. 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, interaction with Clients and Counterparties, and the framework for dealing with violations of ethical and professional standards shall be governed by the Bank’s Business Ethics Regulations.

4.3.3. Bank employees shall not:
- accept/receive any property benefits or advantages (including payment for holidays, including on weekends, medical treatment, foreign tourism and health trips, etc.) for themselves, their close relatives or acquaintances from the Bank’s Clients/Counterparties, including potential ones, and/or employees of any of the parties involved in a transaction with the Bank, and/or officials, international or public servants, and close relatives of the said persons;
- receive gifts or favours from Clients/Counterparties (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 set out in the Eurasian Development Bank’s Compliance Control Regulations;
- receive any part of disbursements on loans provided by the Bank;
- provide undue advantages to third parties; or
- use any benefits, privileges or immunities granted by the Bank due to the employee’s official position for their personal enrichment or the enrichment of their close relatives.

4.3.4. Procurement of goods and services for the Bank’s needs shall be based on the principles of equal opportunities, transparent relationships 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, based on ensuring the possibility to choose suppliers.

4.3.5. 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.

4.3.6. The Bank’s human resources policy shall be based on the Bank’s corporate values and a high culture of interaction between employees at all levels.

4.3.7. All Bank employees shall be subject to the same approaches with regard to recruitment, remuneration, job assignment, training and performance appraisal.

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

4.3.9. The Bank and EDB Group financial institutions shall take all necessary measures to prevent corruption risks.

4.4. Risk of conflict of interest

4.4.1. A conflict of interest, where the Bank fails to take measures in advance to identify, prevent and resolve situations with indications of conflicts of interest, creates grounds for financial and reputational risks.

4.4.2. The Bank and EDB Group financial institutions shall adhere to a policy of openness with respect to the identification, prevention and resolution of conflicts of interest.

4.4.3. The methods used by the Bank to identify, assess and manage conflicts of interest are set out in the Eurasian Development Bank’s Regulations on the Prevention and Management of Conflicts of Interest.
4.5. Risk of non-compliance with applicable tax discipline laws

4.5.1. The Bank shall condemn tax crimes and support the member states’ efforts to improve tax discipline.

4.5.2. The Bank shall establish the tax residency of its Clients and their beneficial owners and shall be prepared to exchange the relevant information in order to implement tax discipline laws within the applicable provisions of the legislation of the Republic of Kazakhstan as the state of the Bank’s headquarters, arising from multilateral and/or inter-governmental agreements signed by the Republic of Kazakhstan.

4.5.3. EDB Group companies shall implement the provisions of their national tax discipline laws (taxation of foreign accounts) and participate in the international exchange of information on financial accounts in accordance with their national legislation.

4.6. Risk of misuse of insider information and market manipulation

4.6.1. Misuse of information and market manipulation undermine fair pricing of financial instruments, foreign exchange and commodities, lead to unequal treatment of investors and destroy investor confidence.

4.6.2. The Bank and EDB Group financial institutions shall take all necessary measures to combat the misuse of insider information and prevent market manipulation, including, but not limited to, establishing a ban on the transfer of insider information to persons who do not have access to it, as well as a ban on the distribution of knowingly false information and transactions aimed at misleading as to the price of a financial instrument, foreign currency or commodity.

5. Compliance Control Arrangements and Key Tools

5.1. Setting up a compliance control system

5.1.1. The EDB Management Board shall be responsible for establishing an effective compliance control system at the Bank.

5.1.2. The Chief Compliance Officer shall oversee the operation of the compliance control system and set priorities for its development.

5.1.3. The Bank has established a separate business unit, the SCCD, with a dedicated Compliance Control Unit, whose tasks and functions include developing key compliance controls and ensuring and participating in their practical implementation. The Bank has also appointed an AML/CFT Compliance Officer.

5.1.4. To harmonise its approach to compliance control and risk management, the Bank shall work with EDB Group companies to coordinate and monitor their compliance risk management activities. Necessary interaction may take place through the corporate governance bodies of the Subsidiaries as well as directly between authorised compliance officers of the Bank and EDB Group companies.

5.2. Key compliance control tools

5.2.1. Process regulation. The Bank has developed and implements internal regulatory documents governing banking operations and transactions, labour relations with its employees and other areas of its activities, providing for the necessary compliance control measures where appropriate. A detailed description of the compliance control processes is provided in the Eurasian Development Bank’s Compliance Control Regulations.

5.2.2. Expertise by SCCD employees. To effectively manage compliance risks, SCCD CCU employees shall be directly involved in Client due diligence, project and transaction analysis, and transaction monitoring and analysis. Assessing the level of Client/Counterparty compliance risk and project risks and considering these risks in cooperation with Clients and Counterparties ensures the implementation of a risk-oriented business model.

5.2.3. Analysis of external and internal data, including complaints and appeals. The Bank shall analyse information and data, including publications in the media, other trustworthy external sources, as well as complaints/appeals received by the Bank about
instances of abuse, misconduct, wrongdoing or improper conduct by Bank employees or in connection with Bank activities. The Bank shall operate a Compliance Hotline, to which irregularities and abuses can be reported. All reports shall be reviewed and analysed in accordance with the Eurasian Development Bank’s Compliance Control Regulations.

5.2.4. Informing the Bank’s management and governing bodies. All matters relating to the operation of the compliance control system shall be reported to the Chief Compliance Officer, including in the form of weekly monitoring reports on settlement service transactions. Quarterly and annual reports to the Council of the Bank shall include information on the compliance measures implemented in the relevant reporting period.

6. Roles and Responsibilities

6.1. The Bank’s Management Board
- ensures the establishment and operation of the Bank’s compliance control system; and
- reviews and approves the Bank’s internal regulation documents aimed at implementing this Framework.

6.2. Chief Compliance Controller
- oversees the operation of the Bank’s compliance control system;
- monitors the operation of the compliance control system at EDB Group companies;
- makes decisions aimed at managing compliance risk; and
- sets priorities for the development and improvement of the EDB’s compliance control system.

6.3. SCCD
- develops and implements compliance control measures; and
- interacts with EDB Group companies on compliance risk management.

6.4. Bank divisions
- divisions whose activities may create compliance risks (“first line of defence”) take actions to identify possible compliance risks when preparing transactions/operations and developing new products/services or promoting cooperation with Clients/Counterparties, and implement measures aimed at minimising and managing arising risks;
- divisions that support business operations in terms of risk assessment (“second line of defence”) identify and assess the risks in their area of responsibility and monitor compliance with established limits, fostering a compliance culture; and
- the IAS, as the “third line of defence,” independently assesses the functioning of the compliance control system, the quality of compliance procedures and compliance risk management processes.