DESTEKBANK

2024

PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Name of the policy	Prevention of Laundering Proceeds of Crime and Financing of Terrorism Policy
Approved by	Board of Directors
Effective Date	04.08.2021
Last Revision Date	06.12.2023
Version Number	2

1. PURPOSE AND SCOPE

This policy is aiming to ensure that Destek Yatırım Bankası AŞ complies with the obligations determined by Law No. 5549 and its' sub-regulations, within the framework of preventing money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction; determining strategies, internal controls and measures, implementation principles and responsibilities about monitoring and control rules, trainings and internal audit activities in order to reduce the risks that the Bank may exposed to, by applying a risk-based approach, considering the size, nature and volume of the business with regard to the Bank's customers, transactions and services; and to raise awareness of the Bank's employees on these issues.

This policy covers all employees of the Bank, the Head Office and related departments.

2. RISK APPROACH

The Bank's risk appetite regarding compliance risk related with money laundering and financing of terrorism regulations is zero. Therefore, The Bank shall get all the measures in order to keep the compliance risk at minimum in a permanent manner, in all its activities.

The Bank closely monitors the regulations to which it is subject, and takes the necessary measures to ensure timely compliance. Important regulatory changes that may increase the risk arising from these obligations will be reported to the Board of Directors by the Compliance Officer. In this framework, the compliance officer regularly evaluates the risk situation of the Bank in the fight against money laundering and terrorist financing, bribery and corruption every year, and makes the necessary changes in the Bank's policies and procedures on the subject and submits them to the approval of the senior management.

3. DUTIES AND RESPONSIBILITIES

Compliance within the framework of preventing money laundering and financing of terrorism is an important element of the Bank's corporate culture and is not specifically the responsibility of only one or a few departments or individuals. All bank employees, regardless of title, have a responsibility to fight money laundering and terrorist financing. Bank employees are obliged to pay due attention and care to money laundering and terrorist financing in all their activities. Otherwise, they may be faced with legal sanctions ranging from fines to imprisonment in accordance with the relevant legislation. In this context, compliance activities are considered as an inseparable element of all activities of the Bank. All employees of the Bank are obliged to

- To learn, understand and comply with the Law No. 5549 and the Law No. 6415, the legal regulations regarding these laws and all related internal regulations,
- Acting within the framework of the principles of know your customer and identification explained in this policy and the policy-related procedure, in all Bank transactions, particularly in customer identification,
- Participating in training activities to be organized on the subject,

- If, while performing banking transactions, they see a suspicious situation within the scope of money laundering crime and financing of terrorism in transactions made or attempted to be carried out at or through our Bank, notifying the Compliance Officer in writing (including e-mail) of this situation,

Apart from the duties and responsibilities applicable to all employees, the Legislation Department, Compliance Officer, Internal Control Department and Internal Audit Departments are also responsible for fulfilling specific duties and responsibilities related to the subject.

4. APPROACH TO FIGHTING LAUNDERING AND TERRORIST FINANCING

The Board of Directors considers direct or indirect use of the products and services it offers for the purpose of laundering proceeds of crime or financing terrorism as one of the most fundamental risk areas in terms of its corporate existence. For this reason, a risk management program was established by determining the rules at the policy and implementation level by the Bank; rules and procedures have been determined on the fight against bribery and corruption. The main elements of the Bank's approach to this issue are as follows:

- Determination of the corporate policy by the Board of Directors on combating money laundering and financing of terrorism and creating detailed sub-regulations on the subject within the framework of this policy.
- Carrying out risk management activities with a risk-based approach,
- Monitoring and control activities,
- Training activities,
- Internal audit activities,
- Appointment of Compliance Officer

RISK MANAGEMENT POLICY

The Bank’s risk management activities are shaped within the framework of the following principles:

- Developing methods for identification, rating, classification and assessment of the risks by taking into account at least the customer risk, service risk and country risk.
- Rating and classification of services, transactions and customers according to risks
- Ensuring the monitoring and control of risky customers, transactions or services; reporting of these in a way that warns the relevant units, developing appropriate operating and control rules for the execution of the transaction with the approval of a higher authority and auditing when necessary, reporting in a way that warns the relevant functions within the Bank,
- Questioning the consistency and effectiveness of risk identification and assessment methods, risk rating and classification methods retrospectively through case studies or realized

transactions, re-evaluating and updating them according to the results and developing conditions.

- Carrying out necessary development studies by following the recommendations, principles, standards and guides brought by national legislation and international organizations regarding the subjects within the scope of risk,
- Reporting the risk monitoring and evaluation results to the Board of Directors/Audit Committee at regular intervals.

The bank's risk management approach is shaped within the framework of factors such as customer acceptance rules, customer recognition and identification, and risk classification. Training and internal audit activities are also integral parts of this approach as activities that support the core elements of the risk management program.

CUSTOMER ACCEPTANCE RULES

The Bank does not accept the persons and institutions described below as customers.

- As a basic principle, the Bank does not provide banking services to individuals and institutions that have not passed know your customer and identification procedures.
- A business relationship cannot be established with individuals and institutions that refuse to submit information and documents that are required to be submitted in accordance with legal regulations.
- No business relationship is established with people whose real identities and addresses cannot be determined, or with people who refuse to give a physical address.
- The business relationship with the customer in question is terminated in cases where the identification and confirmation of the previously obtained customer's identity information needs to be done again but cannot be done due to doubts about the adequacy and accuracy of the customer's identity information.
- No business relationship can be established with persons and institutions named in the blacklists or sanctions lists published by the official institutions in Turkey or countries such as the United Nations, the European Union and OFAC on laundering proceeds of crime, financing terrorism or financing the proliferation of weapons of mass destruction; existing business relationships are terminated.
- Banks and institutions that do not have a physical address cannot be accepted as customers.
- Shell companies or institutions suspected of providing shell banking services are not accepted as customers. Banks that provide services to such customers are not accepted as customers.
- Persons and institutions engaged in illegal betting and gambling activities, including those operated over the Internet, cannot be accepted as customers.
- A business relationship cannot be established with those who operate in an area subject to a license, a special authorization or permit, but do not have the necessary permit/license/authorization document.
- In cases where sufficient information cannot be obtained about the purpose of the business relationship or the desired transaction pursuant to the current legal regulations and the customer refrains from meeting the information requests in this direction, a permanent business relationship cannot be established or the requested transaction cannot be performed.

- Persons and institutions that declare only hold-mail addresses as address information are not accepted as customers.
- In cases where the Bank provides correspondent services, banks that use their accounts with the Bank to provide correspondent services to other banks are not accepted as customers; the business relationship with banks determined to provide such services is terminated. Similarly, the banks to which correspondent services will be provided are not allowed to use these accounts as correspondent accounts with transfer.

On the other hand;

Utmost care and attention is paid to accept people and institutions who are suspected that their wealth and funds have been acquired through illegal means, as well as people with negative social reputations, as customers.

In joint stock companies, in cases where the shares are bearer shares, it is essential that there is no doubt about the ownership of the company. When necessary, the ownership of bearer shares is determined through the Bearer Share Registration System records kept by CRA.

Acceptance of banks established in off-shore centers as customers is subject to the approval of the board of directors.

KNOW YOUR CUSTOMER AND IDENTIFICATION

KNOW YOUR CUSTOMER

Knowing the customer; means having sufficient knowledge about customers and their activities. The principle of knowing the customer reduces and controls the money laundering risk, and also facilitates the detection of transactions related to illegal activities. The purpose of KYC is to ensure clarity in the customer's transactions and information, and to establish and maintain a relationship based on mutual trust. The Bank handles the KYC process with a risk-based approach.

Within this scope, information regarding knowing the customer is obtained from the customers who will enter into a business relationship with the Bank. The scope of information to be provided is determined by the type of customer and expected transaction activities. This information is confirmed by documents or independent sources when necessary and possible.

Enhanced due diligence rules are applied for those customers who are determined to be high risk as a result of the risk score assessment made by the Bank. During the active relationship with the customer, regular review, monitoring and control activities are performed to ensure that the transactions carried out by the customer are compatible with the information held by the Bank and the source of wealth. Within the framework of a risk-based approach, the Bank applies more frequent and enhanced customer review rules for its risky customers.

Rules triggering the review include, at a minimum, changes in control ownership or scope of business in legal entities, significant changes in senior management or operating structure, changes in beneficial owners, and significant changes in the customer transaction profile.

IDENTIFICATION

In terms of preventing laundering proceeds of crime and financing of terrorism, the most important step of KYC process is identification. In accordance with the legal regulations, a customer relationship cannot be established without fulfilling the obligations regarding identification. Identification is not only a liability limited to customers, but also includes other persons and institutions that are required to be identified in MASAK legislation, such as real beneficiaries, control holders, persons authorized to represent.

Apart from establishing a permanent business relationship, the Bank performs a duly identification before the transactions that require identification in the MASAK legislation. A business relationship cannot be entered into with persons who act on behalf of and/or in favor of a third party and fail to submit the information and documents requested by the Bank about that person.

It is essential that identification is made face-to-face by a Bank employee or the Bank's contracted representative (support service organizations) or in the form of remote identification in accordance with the relevant regulations of the BRSA and MASAK.

Bank employees are obliged to transact with valid document types determined within the scope of the relevant legislation during customer identification. In addition to the identification of the customer, it is essential to determine the customer's transaction profile and financial profile on the basis of detailed criteria such as the purpose of the customer's transaction, whether he acts on behalf of or on behalf of someone else, the planned transaction amounts and the source of the investment, and to provide it during the creation of the customer relationship.

The Bank takes the measures specified in the legal legislation in order to determine whether or not it is acted on behalf of someone else in customer acceptance and transactions that require identification at or through the Bank. In a transaction that requires identification, in the event that the customer declares that someone else's account has been acted upon or it is determined by the Bank, the identity of the person on whose account the transaction is made must also be determined in accordance with the legal regulations, in addition to the person performing the transaction. Even if the customer does not state that he has acted on behalf of someone else, in case such a situation is suspected, measures to determine the real beneficiary are implemented.

In the process of determining the real beneficiary, while accepting customers for legal entities registered in the trade registry, it is aimed to reveal the real person or persons who ultimately control the legal entity. For this purpose, the shareholding structure of the legal person is determined, and it is determined whether there are real persons who have shares in the partnership above the limits specified in the legal legislation. In cases where the real person partner does not exist or where it is suspected that the existing partner is not the real beneficiary of the partnership, an investigation is carried out to determine the final beneficiary and the identity information of the identified real persons is obtained, and documents confirming the identity are provided where possible. When the real beneficiary cannot be identified, the real person or persons with the highest executive authority registered in the trade registry are considered the real beneficiaries as senior managers. In cases where it is restarted to work with a corporate client that has ceased to be actively worked or significant changes such as change in the ownership of the company etc., a re-declaration is taken from the customer for the determination of the actual beneficial owner. Practices for determining the real beneficiary are repeated within the scope of customer review processes.

In the subsequent transactions made face to face within the scope of continuous business relationship of the customers, whose identity identification obligations have been duly fulfilled before, identification will be made in accordance with MASAK legislation.

A business relationship can be established or a transaction can be made by relying on the measures taken by another financial institution regarding the identification of customer, the person acting on behalf of the customer or the real beneficiary, and obtaining information about the purpose of the business relationship or transaction. For this, the conditions sought in the MASAK legislation must be met.

RISK CLASSIFICATION

The Bank scores and classifies its customers in terms of risks associated with money laundering and terrorist financing, within the framework of a risk scoring model.

The risk scoring model is structured to include, as a minimum, the following risk elements:

- Customer risk
- Product/service risk
- Geographical risk

The main purpose of customer risk classification, rating and evaluation is to identify customers, business relations and transactions with acceptable risk and above, to monitor them continuously, and to ensure that the information and documents of the customer are kept up-to-date.

Politically exposed persons, associations and foundations, persons and institutions residing/ operating in countries under close monitoring by FATF are evaluated in the highest risk group, regardless of risk scoring. There is no domestic or international distinction in determining politically exposed persons.

The bank classifies its customers as low, medium and high risk in the classification based on risk scoring. Tighter control processes are implemented for medium and high risk customers. Acceptance of all high-risk clients is subject to approval by the compliance officer.

The bank also scores its customers based on transactions they carry out from the accounts they keep at the bank.

Risk score calculations are repeated every month and changes in risk levels and their causes are analyzed by the relevant departments and necessary measures are taken.

MONITORING AND CONTROL

The Bank establishes an appropriate monitoring and control mechanism to confirm that its transactions and activities are carried out in accordance with the obligations related to the prevention of money laundering and terrorist financing, within the scope of legal regulations, the Bank's internal regulations, corporate policy and the procedure related to corporate policy.

Situations within the scope of monitoring and control activities are as follows:

- High risk customers and transactions
- Transactions with risky countries
- Complex and unusual transactions
- Transactions that are not compatible with the customer profile
- Transactions within the scope of identification obligation when evaluated together
- Completeness and up-to-datedness of customer information and documents
- Transactions made through technological channels
- New products and services

The Bank regularly monitors transactions in order to detect suspicious situations in customer transactions. During this monitoring process, it should be evaluated whether the customer's transactions are in accordance with the customer and transaction profile known to the Bank. In monitoring activities, a risk-based approach is followed within the framework of the transactions determined as risky transaction groups and the risk classification created by the Bank. All Bank employees are obliged to notify the Compliance Officer in writing, if they see a suspicious situation within the scope of money laundering crime and financing of terrorism in transactions made or attempted to be carried out at or through the Bank. It is the Compliance Officer's authority and responsibility to decide whether or not to report suspicious transactions to the MASAK.

TRAINING ACTIVITIES

The main purpose of the Bank's training policy is to ensure compliance with all relevant legislative obligations, to create a corporate culture by raising the awareness of the Bank's employees on corporate policy and procedure and risk-based approach.

In order to prevent laundering proceeds of crime and financing of terrorism, the Bank conducts training activities in accordance with the size of the enterprise, business volume and changing conditions. Training activities are carried out within the framework of an annual training program, under the supervision and coordination of the Compliance Officer. As a minimum, the trainings include the conceptual framework, regulatory obligations, suspicious transaction types and case studies, international regulations, and the bank's policy and implementation principles.

In principle, the Bank ensures that the training on the prevention of money laundering and financing of terrorism is given to the personnel who are determined to be directly exposed to the said risk, every year, and to the new employees within the first two months following the start of the job. The main responsibility for delivery of trainings rests with the compliance officer. The compliance officer is authorized to group employees in terms of training needs and scope, and to determine which personnel or group will receive training at what intervals and by which training method.

In order to determine the effectiveness and adequacy of training activities, evaluation is made using appropriate techniques. According to the results of this evaluation, it may be decided to organize additional trainings or to repeat the trainings outside the annual program, if necessary.

INTARNAL AUDIT

The implementation of compliance activities regarding the prevention of money laundering and financing of terrorism is regularly audited by the Bank's Internal Audit Department with a risk-based approach.

The Internal Audit Department audits at least the following issues in the process of auditing liabilities related to laundering proceeds of crime and financing of terrorism:

- Whether the Bank's policies, procedures and processes are adequate in terms of the risks identified in relation to money laundering and terrorist financing,
- The competence of the Bank's employees in the implementation of existing policies and procedures,
- The adequacy of policies and procedures in this regard, including the risk management activities established, and the effectiveness of surveillance and control activities,
- Activities carried out within the scope of knowing the customer, identification and customer acceptance policies,
- Adequacy of training activities and training given to Bank employees.

The Compliance Officer also examines the other audit reports of the Internal Audit Department, evaluates whether there is a malfunction in terms of obligations regarding the prevention of money laundering and financing of terrorism, and takes preventive/corrective measures if necessary.

APPOINTMENT OF COMPLIANCE OFFICER

As regulated in the Compliance Program Regulation, the Bank is not among the obligors to create a compliance program and is solely responsible for appointing a compliance officer at the administrative level. Compliance Officer is appointed by the Board of Directors. When the Compliance Officer cannot be on duty temporarily due to leave, illness or similar reasons, the duties and responsibilities of the Compliance Officer are fulfilled by the Deputy Compliance Officer. The decision regarding the person(s) who can represent the Compliance Officer is subject to the same procedure as for the appointment of the Compliance Officer.

OTHER OBLIGATIONS

PROVIDING INFORMATION AND DOCUMENTS

The Bank is obliged to provide all kinds of information, documents and related records in all kinds of media that may be requested by the supervision and inspection authorities authorized by the Law, all information and passwords required in order to provide access to these records and make them readable, fully and accurately, and to provide the necessary convenience.

RETENTION AND PRESENTATION

Documents in all media regarding all obligations and transactions brought by Law No. 5549, Law No. 6415 and their sub-regulations are kept for eight (8) years from the date of issue, books and records from the last registration date, and documents related to identification from the last transaction date. and submitted to the authorities upon request.

KEEPING CONFIDENTIALITY

Bank employees may not disclose or use, for the benefit of themselves or third parties, the secrets they have learned regarding the persons, transactions and account statuses, business, enterprises, wealth or profession of customers and people related to customers, or other matters that should be kept confidential, except for persons and institutions expressly authorized by law.

It cannot be disclosed to anyone, including the parties to the involved in a transaction that a suspicious transaction has been reported, except for those who carry out liability control or the courts during the trial. Real and legal persons who fulfill their obligations within the scope of Law No. 5549 and Law No. 6415 and related sub-regulations cannot be held responsible in any legal or criminal terms.

These obligations continue even if the Bank's employees leave their positions.

5. FIGHTING CORRUPTION

The Bank fights against acts of corruption and bribery with a “zero tolerance” approach. Within the scope of this struggle, it observes compliance with current national and international laws and regulations and ethical and professional principles in all its activities.

As an extension of this approach, the Bank aims to prevent its customers from using their bank accounts for bribery and corruption-related acts.

The Bank cannot give aid, donations or gifts to any government official or political party candidate at any decision stage that may benefit its activities. Compliance with ethical principles is observed regarding donations to charities, and Internal Control approval is obtained by running approval processes within the Bank.

Business partners and outsourcing companies must comply with the Bank's policies and principles. Since business relations with third parties may carry risks within the scope of acts of corruption and bribery, it is considered to work with business partners who fully comply with the laws of anti-corruption and anti-bribery in order to reduce these risks; Work with persons and institutions that violate the Bank's rules on this matter shall be terminated.

Employees of the Bank may not obtain any benefit from customers, suppliers, business partners and other third parties with whom they have a relationship within the scope of their activities, except for gifts (except for cash or cash equivalents) that can be accepted with the approval of their managers. No cash or cash-like gifts can be given or accepted. Employees must avoid situations that may create such conflicts as much as possible, considering that giving or accepting gifts may cause conflicts of interest.

Maximum attention is paid to the conditions and quality of the hospitality and invitation and how it will be performed. Before any invitation or entertainment is organized, evaluations are made on issues such as the intention of the entertainment and the invitation, the perception it will create on the part of

customers, stakeholders and society, its cost, scope, effects on the corporate image, and whether it has any privileges for public officials.

The bank also does not allow facilitation payments within the framework of country legislation; or in its relations with third parties, it does not allow the other party to offer, request or accept it.

It determines the main risk areas and takes measures to manage the risks related to these, in line with the objective of preventing its customers from using their bank accounts to commit acts related to bribery and corruption. In this context;

- Measures are taken to identify politically exposed persons and determine the source of these people's wealth
- Transaction structures that may be related to bribery and corruption are determined and measures are taken to detect them.

In this context, at least the money movements of politically exposed persons with risky countries, the amounts sent to their accounts by foreign exchange offices or money transfer institutions; unreasonable transactions on these accounts; transactions made by customers operating in sectors considered to be high risk in terms of bribery and corruption; transfers between foundations and associations that are under the control or management of politically exposed persons are monitored by the Bank.

DESTEK YARTIRIM BANKASI A.Ş.