Ziraat Katılım

ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION COMPLIANCE POLICY

2023 December

ZİRAAT KATILIM BANKASI A.Ş.

ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION POLICY

As Ziraat Katılım Bankası A.Ş. our primary goal is to fully comply with applicable national and international laws and regulations and sanction regimes in order to prevent the products and services we offer to our customers from being used in activities related to money laundering, financing of terrorism, financing the proliferation of weapons of mass destruction and other financial crimes.

1. PREAMBLE

It is the policy of all branches,subsidiaries and affiliates of Ziraat Katılım Bankası A.Ş. to combat the laundering of the proceeds of crime and activities that facilitate it, as well as the financing of terrorism/the proliferation of weapons of mass destruction or other financial crime activities, and to actively pursue the prevention of these activities.

The Bank carries out its activities in accordance with the laws in force and international standards, in particular with the Law No. 5549 on the Prevention of Laundering Proceeds of Crime, Law No. 6415 on the Prevention of the Financing of Terrorism and the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction No. 7262.

The policy is reviewed once a year and when necessary, in order to ensure and maintain compliance with legal regulations and international standards, and necessary updates are made.

1.1. Purpose

Purpose of this policy:

- Preventing the use of our products and services in laundering of the proceeds of crime and the financing of terrorism, as well as the financing of the proliferation,
- Forbidding the activities that facilitate ML/TF/PF and other financial crime activities,
- Ensuring that each personnel of the Bank is knowledgeable on the rules regulating the combat the laundering of the proceeds of crime, financing of terrorism, and other financial crimes for all branches, subsidiaries and affiliates operating within the group, and is conscious about and responsible of abiding by these rules,
- Ensuring that the customers, transactions, products and services are assessed with a risk-based approach, and that the necessary actions are taken with regards to identifying and mitigating the reputational, operational, legal, and concentration risks Ziraat Katılım Bank may face in this regard,
- Complying with international sanction regimes, and preventing Bank from intermediating in transactions that may result in any sanction,
- Protecting the interest, reputation, and customer quality of the group,
- Conducting secure banking activities,
- Identifying the operation and rules in this field and defining roles and responsibilities,
- Establishing the principles and standards that Bank must abide by.

1.2. Scope and Legal Framework

This policy covers all domestic and overseas branches, as well as domestic and local subsidiaries and agents. Law No. 5549 on Prevention of Laundering Proceeds of Crime, Law No. 6415 on Prevention of Financing of Terrorism, Law No. 7262 on Prevention of Financing of Weapons of Mass Destruction, and the regulations and communiqués published regarding these laws constitute the legal basis of our Bank's AML/CFT policy. This policy includes policies regarding risk management, monitoring and control, training, internal audit and information sharing.

1.3. Roles and Responsibilities

Principles mentioned in this policy need to be considered and applied by all units operating within group and employees at every level. They need to avoid transactions and activities that may be considered as laundering of the proceeds of crime, financing of terrorism/the proliferation, or facilitating these actions. For this purpose, duties and responsibilities must bu fulfilled with necessary attention and care.

While the Compliance Unit is responsible for the implementation of our Bank's AML/CFT policy; Board of Directors is ultimately responsible for ensuring that our Bank's obligations under the Law No. 5549 on the Prevention of Laundering Proceeds of Crime are fulfilled.

Compliance Officer conducts activities regarding risk management, suspicious transaction reporting, monitoring and control within the scope of the compliance program included in the policy, while internal audit activities are conducted by our Bank's Board of Auditors.

2. AML COMPLIANCE PROGRAM

Ziraat Katılım Bank compliance program contains the following:

- AML compliance function,
- Risk management policy,
- Monitoring and control,
- Suspicious transaction reporting,
- Training,
- Internal audit,
- Sanction policy,
- Keeping and retention of records,
- Obligation to provide information and documents,
- Effective communication and interaction with regulatory and supervisory institutions.

The AML/CFT/CFP compliance policy is reviewed annually with a risk-based approach, and in case of any change, it is approved by the Board of Directors or person(s) to whom it has delegated its authority.

2.1. AML Compliance Function

Compliance Officer has the authority to request all kinds of information and documents related to its field of duty from all units within the Bank and to access them in a timely manner, in order to make a decision with an independent will. The compliance officer and compliance unit act in accordance with the confidentiality principles stipulated in the relevant laws and regulations while carrying out their activities in accordance with the written policies and procedures. While carrying out their activities, they act in accordance with the confidentiality principles stipulated in the relevant laws and regulations.

2.2. Risk Management Policy

Our Bank's risk management policy includes activities to define, rate, monitor and mitigate the risks that the bank may be exposed to in relation to the financing of the ML/TF or proliferation of weapons of mass destruction.

The risk management policy includes, at a minimum, internal precautions and operating rules regarding know your customer principles. Activities regarding risk management include those about the identification of the customer and real beneficiary, conducting necessary controls for customer due diligence (CDD), and taking the risk-mitigating measures that are compatible with the risk levels after the risk assessment is conducted according to determined risk factors.

2.2.1. Know Your Customer Principles

The most effective way to protect Bank from those desiring to use it as an intermediary for the acts of money laundering, financing of terrorism and other financial crimes is to know our customers, to establish our policies and procedures within

the scope of “know your customer” in line with legal legislation, and fully comply with them. This process includes the steps of obtaining information about new and existing customers, identification, and verification.

2.2.1.1. Customer Acceptance Policy

Within the framework of the "Know Your Customer" principle at our Bank, it is essential to identify customers and persons acting on behalf of customers, and to implement the necessary controls and take measures to reveal the real beneficiary of the transaction.

Within this scope, a customer acceptance policy was formed in order to conduct CDD that is compatible with the customer’s risk profile, and to determine the customers that bear high risk with regards to ML/FT/PF and those who will not be provided products/services by Bank.

With regards to the customer acceptance policy, obtaining adequate information with regards to the following are important in forming an open and trust-based bank-customer relationship:

- Identification and verification of customer/beneficial owner,
- Consistency of documents and information,
- Customer’s job, main field of profession that creates revenue,
- Customer’s financial profile,
- Work or business place.

2.2.1.1.1. Persons and Entities That Cannot to Be Accepted as Customers

In order for a natural or legal person to be accepted as a customer, they must meet the criteria determined in accordance with this policy. In this context, the following are not accepted as customers and business relationships are not established with them:

- Persons and entities whose real identity and addresses cannot be determined and verified,
- Those who want to open an account under a different name,
- Those providing misleading information regarding their identities or are reluctant to provide any information,
- Those detected, as a result of detailed research, to have provided inconsistent or inaccurate information before,
- When the real beneficiary cannot be identified,
- When information about the nature and purpose of the business cannot be obtained,
- When adequate information cannot be obtained to comply with this policy,
- When there are persons whose funds are determined to be the proceeds of an illegal activity,
- Persons and entities mentioned in the sanctioned lists published by official institutions and in the lists monitored by Ziraat Finance Group,
- Shell banks and shell companies.

2.2.1.1.2. Circumstances Requiring Rejection of Transaction and Termination of the Business Relationship

In establishing a continuous business relationship, information is obtained about the purpose and nature of the business relationship. Business relationships with customers who are detected to have used their accounts for the purposes of money laundering and the financing of terrorism are terminated. Ziraat Katılım Bank does not establish business relationships and does not perform the requested transaction in cases where they cannot identify or obtain sufficient information about the purpose of the business relationship.

The business relationship is terminated if the required identification and verification cannot be made as there is a suspicion regarding the adequacy and accuracy of the previously obtained customer identification information.

Business relationships are terminated with customers who are added on the sanction lists following the establishing an account relationship. If the customers monitored through the filtering program do not provide adequate information and documents regarding the transaction they want to perform, the requested transaction is not conducted and the termination of the business relationship is taken into consideration.

Apart from these, when information about the source of the funds deposited into the customer account cannot be obtained, when individual accounts are detected to have been used for commercial purposes, when real beneficiary of the transaction and beneficial owner of the customer cannot be determined, high-risk products/services are intensely used or transactions incompatible with the customer profile are performed, the requested transaction is not conducted, and the termination of the business relationship with the customer is taken into consideration. Compliance officer also evaluate whether the issues stated above constitute suspicious transactions.

2.2.1.2. Customer Due Diligence (CDD)

CDD includes the processes below:

- Identification of the customer and, where applicable, the beneficial owner,
- Verification of the customer identity based on reliable and independent information, data or documents to the extent required by the relevant legal regulations,
- Understanding of the purpose and nature of the business relationship, and applying enhanced measures in high risk situations,
- Screening the customers for the possibility of being on the sanction lists,
- Monitoring the transactions within the scope of continuous business relationship.

2.2.1.2.1. Obligation of Identification

Regarding the obligation of identification for the transactions conducted by or through the Bank, it is essential to determine the identity of the account holder, persons those acting on behalf of the account owner, the real beneficiary of the transaction, and those authorized to represent, as well as the determination the identity of shareholders and control structure for customers with legal entity.

- Regardless of the amount in the establishment of a permanent business relationship,
- In case the transaction amount or the total of any connected transaction series is, regardless of the amount, equal to or higher than is seventy-five thousand TL,
- When the total amount of a single transaction or a series of related transactions in electronic transfers exceeds is seven thousand five hundred TL,
- Regardless of amount, in cases requiring suspicious transaction reporting,
- Regardless of amount, when there is suspicion about the adequacy and accuracy of previously obtained customer identification information the identity of the customer and those acting on behalf of them are verified by means of receiving the identity information and verifying this information. Identities are verified before the establishment of a business relationship or the completion of the transaction.

Identification of Real Persons:

In real person identification; name, surname, place and date of birth, nationality and residence status, job and occupation information, address, contact number, type and number of identity document or other uniquely identifiable information, signature sample, account type and nature of banking relationship information, for Turkish citizens, in addition to this information, mother, father's name and TR ID number, e-mail address information, if any is obtained.

Remote Identification of Real Persons:

It is possible to establish a permanent business relationship with remote customer acceptance at our Bank, the necessary organization and technical infrastructure for secure customer acceptance via electronic channels has been established, and measures have been taken to verify the identity of customers within the necessary confidentiality and security measures. Enhanced measures are implemented with a risk-based approach in the business relationship established by remote identification. Although a signature sample is not taken in customer acceptance by remote identification, if a

customer acquired in this way comes to the branch, a signature sample will be taken by identifying in accordance with the "Identification of Real Persons".

The information received from the customer in remote identification, all kinds of information and documents for confirmation and records in all kinds of media are kept in a way that allows them to be given to the competent authorities when requested.

Identification of Legal Persons:

With regards to the identification of legal persons, title, legal status, trade register number, tax identity number, field of activity, address on which the headquarters is registered, address of the place of the operation, purpose and nature of activities, phone number, e-mail address, as well as the name, surname, date and place of birth, nationality, types and numbers of IDs, and signature of the person representing the legal entity, IDs of real persons authorized to operate the account, ID of the senior executive in case there is no authorized person, IDs of beneficial owners, financial status of the business, and the expected usage of the account (amount, number, purpose of the expected transactions, source and purpose of the funds) are obtained.

In addition, the identity information of real and legal person shareholders who own more than 25% share of the legal entity or have control of 25% or more funds and/or management should be identified and preserved.

Identification of Persons Acting on Behalf of Others:

Individual application is essential and important when opening an account on behalf of a customer or commencing a business relationship. However, in some cases, persons may desire to form a business relationship through their representatives. In such cases, it is important for the real beneficiary to be detected. Bank detects whether the customer acts on their own behalf, and whether any person claiming to act on behalf of someone else is authorized to do so.

Identification of Persons Acting For the Benefit of Others:

Branches take the necessary measures to determine whether someone has acted on behalf of someone else's account. Moreover, for a permanent business relationship to be established, the declaration regarding the actions on behalf of others is added on all contracts drawn up within the scope of the permanent business relationship. When the person requesting the transaction declares that she/he has acted on someone else's account, the identity and authorization status of the person requesting the transaction and the identity of the person whose account has been acted upon are determined.

In case there is suspicion about the fact that the person acted on his/her own behalf but for someone else's account even though that person claims otherwise, the employee conducting the transaction conducts the necessary and reasonable research to reveal the real beneficiary.

Identification of Real Beneficiary (Beneficial Owner):

Before commencing a business relationship with a customer, the identity/identities of the beneficial owner should be always detected and verified. Beneficial owner is:

- The real person on whose behalf a transaction is conducted,
- Real beneficiary is defined as the real person(s) who have control over the legal entity or the institutions without a legal personality or influence over the account or transaction belonging to them.

In determining the beneficial owner, the ownership structure of legal entities is examined and in legal entities with complex ownership structures, the possibility that the structure is being used to hide the identity of the real beneficiary is taken into account if there are no reasonable grounds. The beneficial owner is an individual and can be one or more. Share ownership rate, which is taken into consideration in the detection of the beneficial owner, may differ according to the local regulations of the host countries. In cases when the beneficial owner cannot be identified, real person(s) registered on the trade register with the highest executive power is/are accepted as the beneficial owner on a senior executive status.

Identification in Subsequent Transactions:

In case of subsequent transactions of a person who has already been duly identified and with whom a permanent relationship has been established; identity information are taken and compared to those kept by the incumbent and then,

signature specimen of the real person who is executing the transaction on relevant document is taken. If any doubt arises about the authenticity of the information obtained, identity documents that are basis for verification or notarized copies of the same are presented, and then the accuracy of the information is verified through a comparison of the information contained in such documents against the information kept by the liable party. In subsequent transactions performed by systems that allow remote transactions, necessary measures shall be taken for verifying customer identity and keeping such information up-to-date.

Identification for Electronic Transfers:

In domestic and international electronic transfers to be conducted equal or more than seven thousand five hundred TL following information is required:

- Name/surname of the sender, title of the legal person, full names of other legal persons and institutions with no legal personality,
- Account number, reference number of the transaction in cases when there is no account number,
- Address or date and place of birth or either the customer number or citizenship number or passport number or tax identity number of the sender to detect the sender.

This information must be verified as well. In electronic transfer messages, information about the recipient specified in the first two articles is also included.

In domestic/international electronic transfer messages below the threshold value determined for identification in electronic transfers, the information specified in the first two articles regarding the sender and the receiver is included. Verification of this information is not mandatory.

Correspondent Relationship:

While establishing correspondent relationships:

- Reliable information is obtained from public sources on whether the relevant financial institution was subjected to an investigation regarding money laundering or terrorist financing and received punishment or warning, the nature, subject, and reputation of the business, and the audit adequacy upon it,
- System of the relevant financial institution on combating money laundering or terrorist financing is evaluated, it is made sure that the system is appropriate and effective,
- Senior executive approval is received before a new correspondent relationship is formed,
- The responsibilities of the bank and the counterpart financial institution within the scope of AML/CFT are clearly defined in a contract to meet the issues specified in the “Identification Obligation” section,
- In cases when the correspondent relationship comprises of the use of payable through accounts, the relevant financial institution is made sure to have taken the necessary measures within the framework of the principles indicated on the "Identification Obligation" section, and be able to provide the identity information of relevant customers when demanded.

The bank does not enter into a correspondent relationship with sign banks and financial institutions that it cannot be sure not to have their accounts used by sign banks.

Reliance on Third Party:

The Bank may establish a business relationship or make a transaction by relying on the measures taken by another financial institution with regards to the customer on issues regarding the identification of the customer, the person acting on behalf of the customer and the beneficial owner, and obtaining information about the purpose of the business relationship or transaction.

When a business relationship established or a transaction is carried out by relying upon the third party, information and documents regarding customer identification of the customer are immediately obtained from the third party. Under any circumstance, the approval of the compliance unit must be received before conducting such a transaction. Principle of relying on the third party is does not apply in case the third party is located in risky countries.

Ziraat Katılım

2.2.1.2.2. Identity Verification

Identity verification process includes the verification of customer identity and address. During the identity verification process, information received for identification purposes is verified, and identities and addresses of the person and persons acting on behalf of the customer are determined and verified. No business relationship is establihed or a transaction is not conducted until the identity of the customer is determined and verified.

Verification of the legal entity's title, trade registry number, field of activity and address, documents pertaining to registration in the trade registry; verification of the tax identification number is made through the documents issued by the relevant unit of the Revenue Administration.

With regards to the accuracy of the person authorized to represent the legal person, identity documents provided for the identification of real person, as well as documents regarding the registration issued or approved by the official institution authorized to keep records of the companies in the relevant country are used. Signatures are verified via the signature declaration prepared by the notary in the relevant country. In order for them to be provided when demanded by the authorities, original or notary-approved copies of the confirmed identity documents are submitted, than copied or saved as electronic image, or identity information is recorded.

In case there is suspicion regarding the authenticity of the documents used for the purpose of verifying the information obtained from the customers within the scope of identification, the authenticity of the document is verified, to the extent possible, by applying to the person or institution that issued the document or other competent authorities.

2.2.1.2.3. Transactions Requiring Special Attention

Special attention is paid on complicated and extraordinarily large transactions, as well as transactions with no apparently reasonable legal and economic purpose, necessary measures are taken to obtain adequate information regarding the purpose of the requested transaction, and the information, documents and records obtained in this context are preserved. In suspicious cases, when the information obtained from the customer is inadequate, compliance unit should be informed regardless of the fact that the transaction is made or not.

2.2.1.2.4. Measures Against Technological Risks

Ziraat Katılım Bank pays special attention on the risk of using the new and developing technologies in money laundering and financing of terrorism/the proliferation,and take appropriate measures in preventing it.

By paying special attention to transactions such as depositing money, withdrawing money from the account and electronic transfers, which are carried out using systems that enable non-face-to-face transactions, transactions that do not comply with the financial profile and activities of the customer or are not related to their activities are closely monitored and if any discrepancies are detected, the compliance unit is informed. Including the amount limit and the limit on the number of transactions, appropriate and effective measures are taken against technological risks.

2.2.1.2.5. Relationships with Risky Countries

Financial institutions within the group must pay special attention to the business relationships and transactions with real and legal persons residing in and institutions without a legal personality operating in risky countries, as well as their citizens, collect as much information as possible regarding the purpose and nature of transactions with seemingly no reasonable legal and economic purpose, and record them.

2.2.1.3. Monitoring the Customer Status and Transactions

Branches constantly monitor, within the scope of continuous business relationship, whether the transactions conducted by their customers are compatible with the information regarding their profession, commercial activities, business history, financial status, risk profile, and fund sources, and keep the information, documents, and records about their customers up to date. Moreover, with regards to customer identification, the accuracy of the phone number, fax number, and e-mail address is verified by using these tools, when necessary, to contact with the relevant person within the framework of the risk-based approach. In case a transaction incompatible with the purpose of the establishing the business relationship and customer profile, about which information is provided by the customer during the customer acceptance process, the business relationship is reevaluated. It is constantly monitored whether the opened accounts are actually used by the person under whose name the account was opened.

2.2.1.4. Simplified Due Diligence Measures

In cases when the risks of money laundering or terrorist financing are low, based on the nature of the risk, measures to be taken regarding customer acceptance can be applied in a simplified manner.

Financial institutions may take simpler measures in terms of customer acceptance for the following transactions:

- Transactions conducted by financial institutions among themselves,
- Transactions in which the customer is a public institution within the scope of general administration or professional organizations with public institution status,
- Establishing a business relationship through collective customer acceptance within the scope of salary payment aggrement,
- Transaction in proportion with the source of funds for customers receiving salary, pension or social aid from defined and appropriate sources,
- Accounts opened for legal payment transactions upon the instruction of public institutions,
- Transactions regarding pension plans and pension contracts that provide pensioner rights to employees by deducting their wages Transactions in which the customer is a publicly traded company with shares listed on the stock exchange.

Simplified measures include the following measures:

- Verification of the identities of the customer and the beneficial owner after the business relationship is established (for instance, when account transactions are above a defined monetary threshold),
- Decreasing the frequency of updates regarding customer identification,
- Decreasing the degree of monitoring and investigation processes that continue based on a reasonable monetary threshold,
- Inability to collect some information or to take specific measures in order to understand the purpose and intended quality of the business relationship, but understanding the purpose and quality from the type of the conducted transactions and formed relationship.

Ziraat Katılım Bank does not apply simplified measures where the applicant knows, suspects, or has reason to suspect that the applicant is involved in money laundering or terrorist financing, or that the transaction was carried out on behalf of someone else in contact with AML/CFT.

2.2.1.5. Enhanced Due Diligence Measures

In cases when the risk of money laundering and financing of terrorism/the proliferation of weapons of mass destruction is high, enhanced due diligence measures need to be implemented during the CDD process consistent with the identified risks. Within the scope of enhanced measures, one or more measures stated below are taken in proportion to identified risks.

- Obtaining additional information on the customer and updating the identity information of the customer and beneficial owner more often,
- Obtaining additional information on the nature of the business relationship,
- Obtaining as much information as possible on the source of the asset of the transaction and the customer's funds,
- Obtaining information of the purpose of the transaction,
- Requiring the approval of an senior officer for commencing a business relationship, maintaining a current business relationship or conducting the transaction,
- Increasing the number and frequency of controls, and strictly observing the business relationship by means of defining the types of transaction that require additional control,
- With regards to establish permanent business relationship, requiring the first financial movement be made from another financial institution to which the know your customer principles are applied,

- Obtaining detailed information about the profession and field of activity, to understand whether there is international trade among its activities,
- Investigating whether the regions in which the customer has commercial relationships and their international transfers are as expected,
- Obtaining information regarding the expected business volume, total sales, major customers and suppliers of the business operations,
- Requiring the first payment to be done via an account of the customer at a bank subject to similar CDD standards.

Our Bank implements enhanced due diligence measures for customers as bearing high risk in terms of sector, product, and geography, and when standard CDD processes are inadequate with regards to AML/CFT.

2.2.2. Risk Management Activities

Activities regarding risk management are comprised of the following at the minimum level:

- Developing the risk identification, rating, classification, and evaluation methods based on customer, product, sector and geography risk,
- Rating and classification of services, transactions, and customers according to risks,
- Ensuring that the risky clients, transactions or services are monitored and controlled, reported to the relevant units, and developing appropriate operation and control rules in order for the execution of the transaction with the approval of the higher authority and its supervision when necessary,
- Retrospectively inquiring the consistency and effectiveness of risk identification and assessment methods through case studies or realized transactions, re-evaluating and updating them according to the results and developing conditions,
- Conducting the necessary improvement works by following the national legislation, and the recommendations, principles, standards, and guides of international institutions on issues within the scope of risk,
- Reporting the risk monitoring and assessment results regularly to the Board of Directors,
- Taking additional measures for high-risk groups.

2.2.2.1. Rating of Risks and Defining the Risk Areas

ML/FT risks faced by our Bank based on many factors, such as the provided products and services, types of customers, and geographical regions.

Customer Risk: It refers to the risk that the Bank will be exposed to in case customers or persons acting on their behalf/account take part in money laundering or terrorist financing activities.

Product/Service Risk: An important element in evaluating the ML/FT risk is to investigate new and current products and services presented by the financial institution in order to determine how and through which channels to use them in money laundering or terrorist financing. Remote transactions, products/services presented by using new and developing technologies, and cash transactions create the product/service risk.

Country/Geography Risk: Customers and transactions in connection with regions with inadequate regulations with regards to the prevention of the laundering of the proceeds of crime and financing of terrorism/the proliferation of weapons of mass destruction that do not cooperate with other countries and international organizations in preventing these crimes, that are considered risky by authorized international organizations, where smuggling, corruption and bribery are widespread, are considered tax haven due to the high rates of drug trafficking in terms of country, residency and parties of transaction are considered geographically risky.

2.2.2.2. Mitigating the Risks

After the risks to be exposed to ML/TF are defined at Bank, the risk areas are determined and the customer portfolio is classified according to the determined risk levels, measures to control and reduce the risk are implemented.

In line with the measures in question, our Bank pays special attention on the business relationships and transactions with individual and legal persons residing in risky countries, institutions with no legal personality operating in and citizens of these countries, collects as much information as possible about the purpose and nature of transactions with no apparently reasonable legal and economic purpose, and records them.

2.3. Monitoring and Control

Purpose of monitoring and control is the protection of Bank from the risks related to ML/FT, and the continuous monitoring and control over whether the activities are conducted in compliance with the regulations and communiqués issued in accordance with the relevant law, as well as the institution's policies and procedures.

In this context, the required monitoring and control include the following activities:

- Monitoring and controlling of high-risk customers and transactions,
- Monitoring and controlling of transactions conducted with countries considered very high-risk and high-risk,
- Monitoring and controlling of high-risk customers who frequently conduct transactions in a substantial amount via sampling method,
- Monitoring and controlling of customers who conduct transactions within a certain time period only through alternative distribution channels via sampling method,
- Monitoring and controlling of customers and accounts that have been dormant for a long while via sampling method,
- Monitoring and controlling of complicated and extraordinary transactions,
- Controlling of customers and transactions through the black and sanctions lists monitored by the Group,
- When taken together, monitoring and controlling of connected transactions exceeding the amount requiring identification by sampling method,
- Checking the information and documents about the customers that must be kept electronically or in written form, as well as information that must be provided on electronic transfer messages via sampling method, completion of missing parts and updating them,
- Ongoing monitoring the compatibility of the transaction conducted by the customer with the information regarding the customer's business, risk profile, and fund sources throughout the business relationship,
- Controlling transactions carried out using systems enabling non face to face transactions,
- Risk-based controlling of services that may be subject to abuse due to recently introduced products and technological development,
- Monitoring and controlling of customers who make large transactions from their accounts via sampling method activities within this scope are conducted by the compliance units of institutions.

2.4. Suspicious Transaction Reporting

With regards to a transaction desired to be or conducted by our Bank or through the Bank; in case there is any proof, information, suspicion or existence of issues that will require suspicion suggesting that;

- It was obtained via illegal methods or used for illegal purposes such as laundering of the proceeds of crime and financing of terrorism,
- It was used by terrorist organizations, financiers of terrorism and the proliferation of weapons of mass destruction and for the purpose of conducting terrorist activities even though it was legally obtained,
- It is connected to ML/FT.

Financial Intelligence Unit (MASAK) is notified by the Compliance Officer about activities and transactions decided to be

suspicious after the necessary research is conducted within the framework of the time and procedures indicated on the law and regulations. Compliance Officer may request all kinds of information and documents from all units with regards to the suspicious transaction in connection with his/her field of duty, and those units provide the demanded information and documents, and make the process convenient.

Within the framework of the regulations within the scope of the confidentiality of suspicious transaction reports and the protection of those who report; personnel, who are aware in any way that a suspicious transaction report has been made, cannot give information to anyone, including the parties of the transaction, except for the information given to the supervisors assigned with the liability audit and the courts during the trial.

If there is a document or serious indication supporting the suspicion that the assets that are the subject of an attempted or ongoing transaction are related to money laundering or financing of terrorism, the request for the suspencion of the transaction is sent to the MASAK, together with the reasons, and the transaction is not conducted during the period specified in the relevant laws and regulations until a decision is made from the financial intelligence unit.

2.5. Training

The purpose of Bank's training policy regarding the prevention of laundering of the proceeds of crime and financing of terrorism is to ensure that Bank complies with the obligations imposed by the Law and other regulations enacted in accordance with the Law-related, to create a corporate culture and update the knowledge of the personnel by increasing the awareness of responsibility in the matters of corporate policy and procedures and risk-based approach.

Training activities are conducted under the supervision and coordination of the Compliance Officer. It is essential for the training activities to be conducted within the scope of the annual training program prepared in a way to include the following subjects.

All personnel in the bank are provided with training on the prevention of laundering proceeds of crime and financing of terrorism. Priority is given to the training of personnel who are in direct contact with the customer. It is essential to provide training to newly recruited personnel during the orientation process. It is ensured that the Compliance Officer/Compliance Unit personnel and training staff participate in domestic/international training, seminars and certification programs on this subject for the purpose of professional specialization. Trainings are organized using in-class, on-the-job and distance education methods. Participation in the remote training is mandatory.

Trainings to be given to employees in relation to ML/FT at the minimum level are as follows:

- Concepts of the laundering of the proceeds of crime and financing,of terrorism,
- Stages and methods of laundering the proceeds of crime, and case studies on this subject,
- Legislation on the laundering of the proceeds of crime and financing of terrorism,
- Risk areas,
- Institution policy and procedures,
- International regulations on combating money laundering and terrorist financing,
- Know your customer principles,
- Suspicious transaction reporting principals,
- Recording and retention obligation,
- Obligation of providing information and documents,
- Sanctions to be applied in case of non-compliance with obligations,
- Sanctions to be applied in case of non-compliance with obligations.

Information and statistics regarding the training activity implemented by the Bank are reported to the MASAK Presidency by the Compliance Officer until the end of March of the following year.

2.6. Internal Audit

The purpose of internal audit is to give assurance to the Board of Directors regarding the efectiveness and adequacy of the whole Compliance Program.

Within the scope of internal audit activities;

- Defects, faults and abuses that are discovered during internal audits as well as opinions and recommendations to prevent their recurrence are reported to the Board of Directors.
- Deficiencies discovered in the course of monitoring and control studies and risky customers, services and transactions are included when determining the scope of the audit.
- When determining the units and transactions to be audited, it should be ensured that the quality and quantity of the transactions performed in the Bank is represented in fullest extent

Activities falling within this scope are executed by the Board of Internal Auditors or relevant audit units. Information and statistics regarding the internal audit activity by the Bank are reported to the MASAK Presidency through the compliance officer until the end of March of the following year.

2.7. Sanction Policy

Ziraat Katılım Bank, together with financial institutions within Ziraat Finance Group, conduct their operations in compliance with national legislation and international standards which govern the Bank's international operations. Ziraat Katılım Bank follow the international sanction programs, especially those of United Nations Security Council, and takes the necessary measures to comply with them. Bank shall not provide any service to countries and activities subject to sanctions, and shall not mediate any banking services that violate the sanctions.

Bank shall not enter into business relationships with persons and organizations that are listed in the sanction lists, shall not conduct transactions requested or ordered by these persons and organizations, shall not mediate the transactions which directly or indirectly involve such persons and organizations. The Bank shall not open accounts for customers who are included in United Nations Security Council and other sanctions lists followed. Sanction lists are screenned regulary in case existing customers who were not sanctioned before may be sanctioned later. Business relationships with persons and organizations shall be terminated that are subsequently added in the sanctions lists.

Our Bank, among the transactions that are desired to be carried out in connection with the countries under sanctions; may agree to take certain actions at its discretion, such as those related to humanitarian aid or as permitted by a license from an appropriate authority. However, these transactions are evaluated on a case-by-case basis and firstly reviewed by the Compliance Unit.

2.8. Record-Keeping and Retention

Regarding the obligations and transactions brought by the Law, in any environment;

- Documents, date of issue,
- From the last recording date of the books and records,
- Documents and records related to identification, from the last transaction date.

It must be kept for eight years from the date of application and submitted to the authorities if requested. The starting date of the retention period of the documents regarding the identification of the accounts at the bank is the date the account is closed.

2.9. Obligation to Provide Information and Documentation

In accordance with the relevant laws and regulations by our Bank; all kinds of information, documents and records related to them and records in all kinds of media are provided to be requested by MASAK and Auditors, or all necessary information and passwords are provided in order to make them readable, and the necessary convenience is provided in this regard.

2.10. Effective Communication and Interaction with Regulatory and Supervisory Institutions

Institutions within the Group shall cooperate with all kinds of institutions in combating ML/FT in compliance with relevant rules and regulations and ZFG corporate policy.

In particular, by the units operating overseas, in effective communication with the regulatory and supervisory authorities in the regions where they operate, all requests that have a legal basis, such as inspection requests, freezing, blocking, reporting of accounts, are fulfilled within the specified period.

3. OTHER MATTERS

This policy enters into force on the day it is approved by the board of directors or the member or members on whom it has delegated its authority and the commitment forms regarding the Institution's policy are notified to the MASAK Presidency within 30 days from the date of approval.

All bank personnel are informed about this policy.