Ziraat Bank

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

January 2025

Ziraat Bank

Table of Contents

Ziraat Bank

ZIRAAT BANK

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

As T.C. Ziraat Bankası A.Ş., our primary goal is to ensure full compliance with applicable national and international laws, regulations, and sanctions programs, in order to prevent the use of our products and services in activities related to money laundering, terrorist financing, the proliferation of weapons of mass destruction, and other financial crimes.

DEFINITIONS AND ABBREVIATIONS

Laundering:	Subjecting the proceeds of crime to various processes in order to smuggle them out of the country or to hide their illegal source or to form an opinion on people to make them believe that they were obtained in a legal way,
Bank:	T.C. Ziraat Bankası A.Ş.,
UNSC:	The United Nations Security Council,
UNSC Resolution:	United Nations Security Council sanctions resolutions on the financing of the proliferation of weapons of mass destruction and their annexes,
Electronic Transfer:	Process of sending a certain amount of money and movable goods so as to be sent to the receiving customer of a financial institution from the sending customer of another financial institution by means of electronic devices,
FATF:	Financial Action Task Force,

Ziraat Bank

Financial Institution: Banks, institutions other than banks authorized to issue debit cards or credit cards, authorized institutions specified in the foreign exchange legislation, money lenders within the scope of the legislation on money lending, financing and factoring companies, capital market intermediary institutions and portfolio management companies, mutual funds, insurance, reinsurance and pension companies, financial leasing companies, institutions providing settlement and custody services within the framework of capital market legislation,

Fund: Money or bank loans, bank and traveler's checks, money orders, securities, stocks, guarantees, bonds, bills, policies, letters of credit and similar securities, any and all immovable or movable, tangible or intangible goods, rights, receivables and any and all documents, including those in electronic or digital media, evidencing and representing a right of ownership or an interest therein, whose value can be represented by money, regardless of the way it is obtained,

Ultimate Beneficiary: Natural person(s) that ultimately control or have ultimate influence on the natural persons who conduct banking transactions, as well as natural and legal persons or unincorporated organizations on whose behalf banking transactions are conducted,

Trust: Legal relationship leaving the control of a certain asset by its owner, who drew up the contract, to a trustee who executes the relevant contract with regards to the management, use or other actions defined on the contract regarding an asset, in order for a beneficiary or a group of beneficiaries to benefit,

Laws: The Law on Prevention of Laundering Proceeds of Crime dated 11/10/2006 and numbered 5549, the Law on Prevention of Financing of Terrorism dated 07/02/2013 and numbered 6415, the Law on Prevention of Financing of the Proliferation of Weapons of Mass Destruction dated 27/12/2020 and numbered 7262,

Financing the Proliferation of Weapons of Mass Destruction:	Financing the proliferation of weapons of mass destruction (FPWMD); partially or fully used funds or financial services provided for the production, acquisition, possession, development, export, commissioning, shipping, transfer, stocking or use of ballistic, nuclear or biological weapons and relevant materials (incl. The dual-use goods used both for technological and illegal purposes),
Assets:	An individual's or entity's, 1) Assets as encompassing the money and earnings held or owned by an individual or entity, as well as those under their direct or indirect control, including any benefits and values obtained from them or resulting from their conversion, 2) Assets as encompassing the money and earnings held or owned by an individual or entity, including any benefits and values obtained from them or resulting from their conversion,
Freezing of Assets:	Means removal or restriction of power of disposal over any assets in order to prevent dissolution, consumption, conversion, transfer, assignment and transfer of assets and other disposal transactions,
MASAK:	Republic of Turkey Ministry of Treasury and Finance Financial Crimes Investigation Board,
Risk:	Possibility of financial or reputation damage that may be faced due to reasons such as the use of products and services for the purposes of laundering proceeds of crime or terrorist financing or not fully complying with the regulations and issued obligations introduced as per the Law,
Risky Countries:	Countries without adequate regulations regarding AML and CFT that do not cooperate in combating these crimes or those considered risky by authorized international institutions,
Illicit Funds:	Value of the money or assets that are obtained as a result of crimes and not via legal methods,

Continuous/Ongoing Business Relationship:	Business relationship between the bank and the customer, established due to services such as opening accounts, giving loan or credit card, safe deposit boxes, leasing, life insurance or private pension, and has a continuous characteristic,
Branch:	Domestic branches of T.C. Ziraat Bank A.Ş.,
Suspicious Transaction:	Existence of any information, suspicion or any issue requiring suspicion concerning the asset, which is the subject of the transaction made or intended to be made at or via the bank, suggesting that it was obtained via illegal methods or used for illegal purposes, used for terrorist actions or by terrorist organizations, terrorists or terrorism financiers within this context or is relevant or connected to them,
Suspicious Transaction Reporting (STR):	Notification of customers and transactions considered suspicious,
Shell Bank:	Bank without any physical service office in any country, without any full-time staff, and that is not subject to the supervision and authorization of any official authority regarding banking transactions and records,
Financing of Terrorism:	Financing of terrorists, terrorist organizations or their activities via legal or illegal methods, mediating or helping or supporting of this financing,
International Sanctions:	Decisions and regulations issued by international authorities regarding the country, person, institution or ships that are sanctioned because of laundering the proceeds of crime, terrorist activities or anti-democratic applications,
Compliance Department:	Refers to the unit consisting of employees working under the compliance officer and responsible for the execution of the compliance program,

Compliance Officer:	The official vested with the necessary powers to ensure compliance with the obligations under the law on AML/CFT/FPWMD and the legislation issued on the basis of the law employed at TR Ziraat Bankası A.Ş. and its consolidated subsidiaries and foreign branches,
Compliance Program:	The set of measures to be taken to prevent Money Laundering and Financing of Terrorism,
Senior Executive:	General Manager and Executive Vice Presidents, managers of units within the scope of internal systems, and managers operating in units other than the advisory ones, who are equal to or higher than the Executive Vice President in rank by their authorities and duties, even though they were employed with different titles,
Senior Management:	Board of Directors and senior executives,
Overseas Branch:	Branches and representative offices running operations abroad,
Ziraat Finance Group:	A group of domestic and foreign subsidiaries under the parent company Ziraat Bankası A.Ş., which are affiliated to the same shareholder group, even if they operate under separate legal entities,

1. PREAMBLE

It is the policy of all branches, subsidiaries and affiliates of Türkiye Cumhuriyeti Ziraat 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.

This policy has been created based on the Bank's size, trading volume and quality of transactions performed. It is essential that all financial institutions within Ziraat Bankası A.Ş. adhere to this policy to the extent permitted by the legal regulations and competent authorities in the countries where they operate.

The Bank is committed to ensuring that its management and employees fully comply with the said laws and standards and prevent banking products and services from being used for the purpose of laundering proceeds of crime, and financing of terrorism/proliferation of weapons of mass destruction.

Our policy on AML/CFT 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 if required. The issues specified within the scope of the national risk assessment are also taken into account within this policy.

1.1. Purpose

This policy ensures that the Bank fights against laundering proceeds of crime and financing of terrorism / proliferation of weapons of mass destruction while conducting its activities, identifies and evaluates the risks it will be exposed to in this regard with a proactive approach, creates the necessary action plans to mitigate them, takes measures and precautions, and acts in compliance with legal regulations within the scope of principles, recommendations, standards and guidelines introduced by national and international organizations.

The purpose of this policy is to determine the strategies, internal controls and measures, operating rules and responsibilities and to raise awareness of the employees of the institution on these issues in order to ensure the compliance of the obligation with the obligations regarding the prevention of laundering proceeds of crime and financing of terrorism / proliferation of weapons of mass destruction and to mitigate the risk to which it may be exposed by evaluating its customers, transactions and services with a risk-based approach.

1.2. Scope and Legal Framework

Our AML/CFT/FPWMD policy covers all branches, representative offices and agencies of our Bank.

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 issued in relation to these laws constitute the legal basis of the Bank's AML/CFT policy. The Bank conducts its activities in accordance with the aforementioned laws and international standards.

In addition, the development of national legal systems to combat money laundering, financing of terrorism and proliferation of weapons of mass destruction and other financial crimes, and the recommendations and standards issued by the Financial Action Task Force (FATF), which sets international standards binding on member countries, aiming to prevent illegal activities and the damage they cause to society, are also taken into account.

Our AML/CFT/FPWMD policy includes policies on risk management, monitoring and control, suspicious transaction reporting, sanctions, training, internal audit and information sharing.

1.3. Roles and Responsibilities

Principles set forth in the Bank's AML/CFT/FPWMD policy must be observed and implemented by all units and all employees at any level, and transactions and actions that may be considered as laundering the proceeds of crime, financing terrorism and the proliferation of weapons of mass destruction, or that may facilitate these activities must not be undertaken. Accordingly, roles and responsibilities must be fulfilled with necessary attention and care. It should be noted that in case of violation of the policy, disciplinary actions may be applied.

The Board of Directors of our Bank is ultimately responsible for the adequate and effective implementation of the Policy and the Compliance Program as a whole. The activities related to risk management, suspicious transaction reporting, monitoring and control within the scope of the compliance program included in the AML/CFT/FPWMD policy are carried out by the Compliance Department under the supervision of Compliance Officer and internal audit activities are carried out by the Bank's Board of Internal Auditors.

2. COMPLIANCE PROGRAM

Ziraat Bank has established a risk-based compliance program in order to prevent the products and services it offers from being used unwittingly as an intermediary in activities related to laundering proceeds of crime, financing of terrorism or other financial crimes and to carry out the necessary control activities in order to comply with both national legislation and international standards and regulations. Our Bank's compliance program includes the following elements:

- Compliance Function
- Compliance Risk Management Activities
- Monitoring and Control Activities
- Suspicious Transaction Reporting
- Training Activities
- Internal Audit Activities
- Sanctions

In order to effectively manage the risks to be encountered within the scope of money laundering, financing of terrorism and proliferation, three lines of defence is applied in our Bank, which enables the determination of risk management structure and processes with strong governance. The first line includes activities related to the management of risks to be encountered during the delivery of products and services to customers, while the second line includes activities related to the management of risks, including establishing, identifying and monitoring controls related to risk management, providing necessary assistance, support and advice, testing and analyzing the results/controls related to risk management and reporting. On the third line, internal audit departmentprovide assurance on the effectiveness and adequacy of the management of these risks and make recommendations on their effective management. It is essential that all lines work in cooperation, coordination and communication.

2.1. Compliance Function

The Compliance Department, under the supervision of the Compliance Officer, is authorized to ensure the Bank's compliance with applicable laws, regulations and other legislation regarding the prevention of laundering proceeds of crime and financing of terrorism / proliferation of weapons of mass destruction. The Compliance Officer is entitled to demand and access all kinds of information and documents from all units within the Bank, regarding its own area of duties, in order to decide independently. Compliance officer, deputy compliance officers and the compliance department carry out their activities in accordance with the written policies and procedures, they act in compliance with the confidentiality principles stipulated under the relevant laws and regulations.

The Compliance Department employs a sufficient number of personnel, taking into account the volume, number of customers and legal regulations, to fulfill the tasks related to the implementation of the compliance program and to manage the risks regarding AML/CFT/FPWMD.

2.2. Compliance Risk Management Activities

Bank's compliance risk management policy includes activities to identify, assess, rate, monitor and mitigate the risks that the bank may be exposed to in relation to AML/CFT/FPWMD.

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 our Bank from those who want to launder the proceeds of crime, finance terrorism or use it as an intermediary for other financial crimes is to know our customers, to establish our policies, principles and practices in accordance with legal regulations within the scope of the "Know Your Customer" principle and to fully comply with them. This process includes information gathering about new and existing customers, identification, and verification.

2.2.1.1. Customer Acceptance Policy

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

Within this scope, a customer acceptance policy was formed in order to conduct CDD (customer due diligence) that is compatible with the customer's risk profile, and to determine the customers that bear high risk with regards to AML/CFT/FPWMD and those who will not be provided products/services by the Bank. Accordingly, before establishing a new business relationship, the Bank conducts due diligence and identification in accordance with the risk profile of the customer, obtains the necessary documents and accepts customers who can be identified accordingly.

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. Within this framework,

- Persons and entities whose real identity and addresses cannot be determined and verified,
- Those who want to open an account under a different name than their real identity,
- Those providing misleading information regarding their identities or are reluctant to provide any information,
- As a result of detailed investigations, those with inconsistencies and inaccuracies in the information previously provided,
- When ultimate beneficiary cannot be identified,
- When information about the nature and purpose of the business cannot be obtained,
- When the information and documents requested to comply with this policy cannot be provided,
- Persons and entities mentioned in the lists of prohibited persons published by official institutions on laundering proceeds of crime and terrorism and in the lists monitored by the bank

Shell banks ve shell companies,

are not accepted as customers and no business relationship will be established with them.

Rejection of the Transaction and Termination of the Business Relationship

When a continuing business relationship is established, 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 Bank does not establish business relationships and does not perform the requested transaction in cases where they cannot identify or obtain sucient information about the purpose of the business relationship.

In the event that the required customer identification and verification cannot be made due to suspicions about the adequacy and accuracy of the identity information previously obtained, the business relationship shall be terminated. 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.

In line with the obligations of our Bank within the scope of international banking legislation arising from its international activities and correspondent relations, in the presence of valid and justified reasons, restrictions may be imposed on the services provided and the business relationship may be terminated when necessary.

Anonymous accounts may not be opened at our bank. The business relationship is terminated with the customers who are added to the sanction lists after the account relationship is established. If the customers monitored through the filtering program do not provide the necessary information and documents regarding the transaction they wish to perform, the requested transaction is not carried out and the termination of the business relationship is taken into consideration. Compliance officer also evaluate whether the issues stated above constitute suspicious transactions.

2.2.1.2. Customer Due Diligence (CDD)

Customer Due Diligence includes:

- Identification of the customer and, where applicable, the ultimate beneficiary,

- Verification of the customer identity based on reliable and independent information, data or documents to the extent required by the relevant legal regulations,

- Understanding the purpose and nature of the business relationship and applying Enhanced Due Diligence measures in high-risk situations,

- Screening customers against sanctions lists,

- Monitoring transactions within the scope of continuous business relationship.

2.2.1.2.1. Identification Obligation

As for identification obligation for transactions performed at or through the Bank, it is essential to identify account owner, persons acting on behalf of the account owner, the real beneficiary of the transaction, authorized representatives as well as the determination the identity of shareholders and control structure for customers with legal entity. Regardless of the amount in case of a permanent business relationship,

- For transactions above the amount specified in the legislation,

- Irrespective of amount in cases when a suspicious transaction reporting is necessary,

- Irrespective of amount in cases where there is doubt about the adequacy and accuracy of the 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 the Ultimate Beneficial Owner

Ultimate beneficial owner is defined as the natural person(s) who ultimately controls or has ultimate influence over the account or transaction of the natural person(s) on whose behalf the transaction is made as well as legal person(s) or unincorporated organizations that carry out transactions at the Bank. Before entering into a business relationship with a customer, the identity of the ultimate beneficiary(ies) is always identified and verified.

Branches shall take the necessary measures to identify the ultimate beneficiary of the transaction. When identifying the ultimate beneficiary, questions such as who owns/holds more than 25% of the shares of the legal entity or unincorporated organization, who effectively controls the customer, and who are the persons on whose behalf transactions are made are utilized.

Correspondent Relationship

While establishing correspondent relationships,

• Whether the counterparty financial institution is under investigation for money laundering or terrorist financing and whether it has been fined or warned, the nature and subject matter of its business, its reputation and the adequacy of the supervision over it shall be obtained from publicly available sources.

• The counter money laundering and counter terrorist financing system of the counterparty financial institution is assessed and it is ensured that the system is appropriate and adequate.

• The approval of the senior manager is obtained before establishing a new correspondent relationship.

• The responsibilities of the bank and the counterparty financial institution in relation to the AML/CFT are clearly set out in a contract to meet the requirements set out in the "Identification Obligation" section.

• Where the correspondent relationship involves the use of payable through accounts, the Bank shall ensure that the counterparty financial institution has taken adequate measures in accordance with the principles set out in the "Identification Obligation" section and can provide the identity information of the relevant customers upon request.

Our Bank does not enter into a correspondent relationship with shell banks and financial institutions with which it is not sure whether or not they make their accounts available to shell banks.

Reliance on the Third Party

The Bank may establish a business relationship or carry out a transaction by relying on the measures taken by another financial institution in relation to the customer in order to determine the identity of the customer, the person acting on behalf of the customer and the ultimate beneficiary and to obtain information about the purpose of the business relationship or transaction.

Reliance on third party is possible provided that;

• It is ensured that the third party has taken other measures to ensure the requirements of the identification, retention of records and know your customer rule, and if it is located abroad, that it is also subject to regulations and supervision in accordance with international standards in the field of combating laundering proceeds of crime and financing of terrorism, and that

• Certified copies of the documents related to identification (in case a permanent business relationship is established through remote identification by the trusted organization, the digital images taken) are provided immediately from the third party upon request,

• The identification of the customer whose information is shared by the third party is not made within the scope of simplified measures,

When a business relationship is established or a transaction is performed based on reliance upon a third party, information and documents regarding customer's identification are promptly taken from the third party and, in any case, approval is received from the Compliance Department before taking such an action. The principle of relying on a third party does not apply if the third party is domiciled in a high-risk country.

2.2.1.2.2. Verification of Identity

The identity verification process involves verifying the customer's identity and address. During the identity verification process, the information received for identification is verified and the identity and address of the person or persons acting on behalf of the customer are identified and verified. No business relationship is established or any transaction is carried out until the identity of the customer has been identified and verified. Upon presentation of the original or notarized copies of the identity documents, a legible photocopy or electronic image is taken or information regarding the identity is recorded to be presented when requested by the authorities. If a document is received, its copy is kept at the Branch with other documents of the customer.

In order to verify the address declared by the customer, one of the following documents or methods can be used: a residence certificate, an invoice for a service that requires a subscription such as electricity, water, natural gas, telephone and issued within three months prior to the transaction date, a document containing address information issued by any public institution, a document that the notification has been made to the customer in case of receiving a notification by mail to the customer address.

If there is any doubt about the authenticity of the documents used to confirm the information received from the customers within the scope of the identification obligation, the authenticity of the document shall be verified by contacting the person or institution that issued the document or other competent authorities, to the extent possible.

2.2.1.2.3. Relationships with High-Risk Countries

Branches are obliged to pay special attention to business relations and transactions with individuals and legal entities, unincorporated entities and citizens of high risk countries, and to collect and record information to the extent possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose on the surface. Detailed explanations on risky countries are provided in the country/geographic risk section.

2.2.1.2.4. Ongoing Monitoring of Costumers Risk Profile and Transactions

Customer Due Diligence and Monitoring customer's transactions includes regular follow-up of the customer with whom a business relationship is established and the financial transactions it carries out, updating information and documents in a short time in case of any changes, and updating the customer risk profile in terms of the nature of the business relationship.

Branches continuously monitor whether the transactions carried out by their customers are compatible with the information on their customers' profession, commercial activities, business history, financial status, risk profile and fund sources within the scope of continuous business relationship and keep the information, documents and records about their customers up-to-date.

2.1.2.3. Simplified Measures

Where the risks of laundering the proceeds of crime or financing terrorism/proliferation of weapons of mass destruction are low, due to the nature of the low risk, customer identification measures may be simplified. Simplified measures may only relate to elements of the customer onboarding process or continuous monitoring.

Simplified measures include;

• Verifying the identity of the customer and the ultimate beneficiary after the business relationship has been established,

• Reducing the frequency of updates to customer identification,

• Reducing the degree of ongoing monitoring and examination procedures performed based on a reasonable monetary threshold,

• Not collecting certain information or take certain measures to understand the purpose and intended nature of the business relationship, but understanding its purpose and nature from the type of transactions and relationship.

Simplified measures shall not be applied in cases where there is a suspicion that the applicant, the person on whose behalf the transaction is carried out or the transaction creates or may lead to a risk of laundering or terrorist financing.

2.1.2.4. Enhanced Due Diligence Measures

Where money laundering or financing of terrorism risks are high, enhanced due diligence measures should be applied in the customer due diligence process consistent with the risks identified. Within the scope of enhanced due diligence measures, in transactions requiring special attention, transactions carried out using systems that enable non-face-to-face transactions, transactions within the scope of relations with high risk jurisdictions and high-risk situations to be determined within the framework of the risk-based approach; in proportion to the identified risk, stricter measures including obtaining additional information about the nature of the business relationship, the purpose of the transaction, obtaining information about the source and usage of the funds, the source of the wealth of the customer, etc. are applied.

Our Bank implements enhanced due diligence measures for customers deemed to be high-risk in terms of sector, product and geography, where standard customer due diligence processes are not sufficient in terms of AML/CFT.

2.2.2. Risk Management Activities

In the Bank, an appropriate risk management system has been established by taking the necessary measures to identify, rate, monitor, control and take necessary measures to mitigate the risks of the transactions and customers carried out within the scope of ongoing business relationship in terms of AML/CFT, and to monitor the transactions carried out outside the continuous business relationship with a risk-based approach.

2.2.2.2. Identification and Classification of Risk

Financial institutions may be exposed to legal risk, operational risk, reputational risk, concentration risk and sanctions risk in terms of laundering the proceeds of crime, financing terrorism/ proliferation of weapons of mass destruction.

Our Bank implements an effective customer acceptance policy and customer identification principles using a risk-based approach to mitigate and prevent potential risks. Effective controls are applied across high-risk regions, sectors, products/services, and channels, while appropriate measures are taken to address the risk of money laundering and terrorist financing through the misuse of new products, business practices, and emerging technologies.

2.2.2.2. Rating of Risks and Defining the Risk Areas

The Bank's AML/CFT/FPWMD risks depend on many factors, including the types of the products and services offered, the channel through which the products and services are offered, and geographical risk.

In order to implement an effective risk-based approach, our customers are rated as very high, high, medium and low according to the following risk areas to assess potential AML/CFT/FPWMD risks.

Customer Risk: Refers to the risk to which the bank may be exposed in the event that customers or persons acting on their behalf/account act for laundering and terrorist financing purposes. When assessing the risk of a customer, factors such as the type of customer, location, residency, nationality, duration of business relationship with the Bank, source and amount of income, political connections, sector and documentation are taken into account.

Product/Service Risk: Products/services and the distribution channels through which they are delivered pose different risks for AML/CFT/FPWMD. Non-face-to-face transactions, products/services offered through the use of new and developing technologies and cash transactions create product/service risk.

Geographic Risk: Customers and transactions that are connected in terms of country, residency, and transaction parties to countries that do not have adequate regulations on the prevention of laundering proceeds of crime and financing of terrorism/proliferation of weapons of mass destruction, that do not cooperate with other countries and international organizations to prevent these crimes, that are considered risky by competent international organizations, where smuggling, corruption and bribery are widespread, where comprehensive sanctions are applied, and regions with high rates of drug trafficking known as tax havens pose a geographical risk.

2.2.2.3. Mitigating the Risks

The first step in mitigating risks associated with money laundering and financing terrorism/proliferation of weapons of mass destruction is to identify potential risks. The second step is to identify controls for high-risk customers, products and processes by utilizing technological developments. The final step is to review the implementation process of the identified controls and implement the risk improvement and mitigation plan.

After the risks to be exposed to the Bank regarding AML/CFT/PFPWMD are defined, risk areas are identified and the customer portfolio is classified according to the determined risk levels, measures to control and mitigate the risk are implemented.

With regard to these measures, the Bank pays special attention to business relations and transactions with individuals and legal entities as well as entities without legal personality and citizens

of risky countries, and collects and records information to the extent possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose.

Customers and transactions categorized as very high risk are outside the Bank's risk appetite, the Bank does not enter into business relations with customers in this category, and the Bank does not act as an intermediary for transactions categorized as very high risk. Persons and organizations included in the sanction lists monitored and customers engaged in illegal betting and gambling are considered in this class. Enhanced due diligence measures are implemented for customers considered to be at high risk category and for their transactions.

2.3. Ongoing Monitoring and Control Measures

The purpose of monitoring and control is to protect the Bank from the risks associated with AML/CFT/FPWMD and to continuously monitor and control whether the Bank's activities are carried out in accordance with the relevant laws, regulations and communiqués issued pursuant to the law, and the policies and procedures of the organization. Activities within this scope are carried out by the Bank's Compliance Department and support is received from other units when necessary. In case of any suspicion regarding the customer and transactions, necessary actions are taken by the Compliance Officer.

The Bank takes the necessary measures to obtain sufficient information about the purpose of the requested transaction, paying special attention to complex and unusually large transactions, transactions of high-risk customers with no apparent reasonable legal and economic purpose, transactions made using systems that enable non-face-to-face transactions, and services that may become vulnerable to fraud due to newly introduced products and technological developments, and the information, documents and records obtained within this scope are kept to be submitted to the authorities upon request. Within the scope of the identification obligation as per the Law, Board of Internal Auditors is responsible for auditing whether the information and documents included in the compliance procedure have been received.

2.4. Suspicious Transaction Reporting

If it is found out or there is information, doubt or suspicion that the income obtained as a result of a transaction carried out by our Bank or intended to be carried out through our Bank has been:

- Illegally obtained or used for illegal purposes, such as laundering the proceeds of crime and financing terrorism/proliferation of weapons of mass destruction,

- Even if it has been gained through legal means, it is used by terrorist organizations, those who finance terrorism and the proliferation of weapons of mass destruction, and to carry out terrorist acts,

- Related to AML/CFT/PFPWMD;

necessary investigations are conducted and the Compliance Officer reports to MASAK the transactions and customers that are deemed to be suspicious within the framework of the time and principles specified in the law and regulation. The Compliance Officer may request all kinds of information and documents related to his field of duty from all departments regarding the suspicious transaction, and the departments from which information and documents are requested shall provide the requested information and documents and provide the necessary convenience to the Compliance Officer in this regard.

Within the framework of the regulations concerning confidentiality of suspicious transaction reports and the protection of those who report, a Bank personnel becoming aware of a suspicious transaction report shall not inform anyone, including the parties to the transaction, that a suspicious transaction has been reported or will be reported, apart from information disclosed to auditors responsible for liability audit and courts during the trial.

If there are documents or significant indications supporting the suspicion that the assets subject to the attempted or ongoing transaction are related to laundering or financing of terrorism/proliferation of weapons of mass destruction, the transaction is forwarded to the MASAK with a request to postpone the transaction together with the reasons, and the transaction is not executed for the period specified in the Law and regulations until a decision is received.

Issues and activities within the scope of the AML/CFT/PFPWMD are reported to senior management at least once a year.

2.5. Training

Training is one of the most important ways to emphasize the importance of the Bank's AML/CFT/PFPWMD prevention efforts and to educate employees on what to do if they encounter potential money laundering. Training also serves as an important control to reduce the bank's exposure to money laundering and terrorist financing risks.

The purpose of the Bank's training policy for AML/CFT/PFPWMD purposes is to ensure compliance with the obligations imposed by the Law and other regulations issued pursuant to the Law, to create a corporate culture by increasing the awareness of responsibility of the personnel on corporate policies and procedures and risk-based approach, and to update the knowledge of the personnel.

Trainings to be provided to personnel on AML/CFT include but are not limited to the following:

- The concepts of money laundering, financing terrorism and proliferation of weapons of mass destruction,
- Stages, methods of laundering of criminal proceeds, and exemplary case studies in this regard,

- Legislation on prevention of laundering of criminal proceeds and terrorism financing,
- Risk areas,
- Bank policy and procedures,
- International regulations on anti money laundering and combating financing of terrorism,
- Guidelines on know-your-customer principle,
- Principles regarding suspicious transaction reporting and confidentiality,
- Retention and submission liability,
- Obligation to provide information and documents,
- Sanctions in case of non-compliance with the obligations

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

2.6. Internal Audit

The purpose of internal audit is to provide assurance to the board on the effectiveness and adequacy of the overall compliance program. Internal audit ensures that whether or not corporate policies and procedures, monitoring and control activities as well as training activities are sufficient and efficient, whether or not risk policy is sufficient and effective, whether or not activities of Know Your Customer/Customer Onboarding and transactions are conducted in accordance with the Law, arrangements introduced as per the Law and the are reviewed and audited annually and with a risk-based approach.

Within the scope of internal audit activities;

- Any defects, faults and abuses that are discovered as a result of internal audits as well as opinions and recommendations to prevent their recurrence are reported to the Board of Directors and the relevant management authority.
- When establishing the scope of the audit, problems identified during monitoring and control activities and customers, services and transactions that involve risks are included in the scope of the audit.
- When determining the units and transactions to be audited, it is ensured that the units and transactions of a quantity and quality that can represent all of the transactions carried out at the Bank are audited.

Activities falling within this scope are executed by the Board of Internal Auditors in the Bank. Information and statistics regarding the internal audit activity implemented by the Bank shall be reported to the MASAK by the Compliance Officer until the end of March of the following year.

2.7. Sanctions Compliance Policy

Our Bank may be subject to judicial and administrative sanctions/penalties in cases such as confidentiality of Suspicious Transaction Reports, breach of information and document provision or recording and retention obligations, failure to declare that the transaction was made on behalf of another person, failure to comply with the recommendations specified in audit reports. Acting in compliance with national and international laws and regulations is very important for protecting the reputation of Ziraat Bank and providing our products and services to our customers in a safe manner.

Ziraat Bank, together with its domestic and foreign branches and subsidiaries, operates in accordance with national legislation and international standards governing the Bank's international operations. Ziraat Bank follows international sanctions programs, especially United Nations Security Council sanctions, and takes the necessary measures to comply. No services are provided for sanctioned countries and sanctioned activities, and no banking services are intermediated in violation of sanctions.

The Bank does not enter into business relations with persons and organizations that are determined to be included in the sanction lists monitored by our Bank, does not carry out transactions requested by these persons and organizations, and does not act as an intermediary in transactions to which these persons and organizations are directly or indirectly a party. No account is opened by the Bank for persons and entities included in sanction lists, notably, lists of UNSC. Existing customers are regularly screened against the sanction list in case they may subsequently become a sanctioned person even if they are not at the beginning. Any existing business relationship with persons and corporations subsequently included in the list is terminated.

The Bank may agree to perform certain transactions at its discretion, such as those related to humanitarian aid or those permitted by a license obtained from an appropriate authority, among the transactions covered by the sanctions. However, these transactions are evaluated on a case-by-case basis and are first reviewed by the Compliance Department.

2.8. Record Keeping and Retention

With regards to obligations and transactions required by the law,

- Documents in any medium, as from their issuance,
- Book and records in any medium, as from last recording dates,
- Documents and records related to identification in any medium, as from last processing dates,

must be retained for **eight years** and submitted to authorities when requested. Retention starting date of documents and records related to identification for accounts at the Bank is the date of closure of the account.

2.9. Obligation to Provide Information

Pursuant to the relevant laws and regulations, our Bank provides all kinds of information, documents and records in all kinds of media to be requested by MASAK and Auditors, and all information and passwords required to access these records or to make them readable are provided in full and accurately.

The Bank's obligation to provide the information and documents requested by MASAK, which determines the strategy for combating laundering proceeds of crime and the financing of terrorism / proliferation of weapons of mass destruction, establishes the policies and legislation to be implemented, is fulfilled by the Compliance Officer, and the Compliance Officer provides the information and documents requested from him/her in accordance with the format and method determined and notified to him.

Within the scope of on-site audits, books and documents are made available for audit; the entire IT system are made available to the auditors in accordance with the objectives of the audit and the security of the data is ensured.

2.10. Freezing of Assets Decisions

Presidential decrees on freezing and lifting asset freezes have legal consequences after they are published in the Official Gazette. Following the publication of the asset freeze decision in the Official Gazette, the necessary action is taken in accordance with the procedure specified in the relevant provisions of Article 128 of the Criminal Procedure Law No. 5271 within the scope of freezing the existing asset values of the persons, institutions and organizations that have assets in our Bank, including the accounts they jointly own.

The Bank adopts sophisticated controls to identify, assess, monitor and mitigate potential risks of breach, non-implementation and avoidance of asset freezing decisions. Within the scope of advanced controls, measures are implemented to continuously monitor customers and transactions by taking into account potential matching criteria by taking into account the sender and recipient information in both electronic transfer and crypto asset transfer messages regarding the persons or organizations whose assets are decided to be frozen. In this context, the sender and receiver information in electronic transfer and crypto asset transfer messages are also taken into consideration.

Any disposals and transactions made in violation of the asset freezing decision shall be null and void.

3. INFORMATION SHARING

Ziraat Bank, as the parent financial institution of Ziraat Finance Group, may share information within the group regarding customer identification and accounts and transactions in order to ensure that measures within the scope of the compliance program are taken at the group level. Confidentiality provisions written in special laws do not apply to intra-group information sharing.

Those who work for the Bank shall not disclose the information they learn within this scope and shall not use it for their own or third parties' benefit. Those who disclose information that should remain confidential within this scope shall be subject to sanctions under the relevant laws.

In order to protect the confidentiality of the information shared within the Group, to ensure that the information is used only for the purpose of AML/CFT/PFPWMD, to ensure that the information shared can only be accessed by the compliance units for the purpose of AML/CFT/PFPWMD and cannot be accessed for any other purpose, it is essential to establish information flow conditions, access controls and security protocols between different financial institutions affiliated to the Group and to provide assurance in this regard.

3.1. Purpose of Information Sharing

With intra-group information sharing at Ziraat Finance:

- Effective identification and management of AML/CFT risks and mitigation of risks within the group,
- Effective group-wide implementation of the compliance program,
- Determining the nature and level of the AML/CFT risk of the organizations within the Group and thus the risk level of the Group,
- A consistent approach within the group against the misuse of new or existing products/services,
- Ongoing monitoring of customers and transactions identified as high risk by an organization within the group by other group members

is aimed.

3.2. Principles of Information Sharing

Necessary information regarding the customer, transaction, account and ultimate beneficial owner is shared within the group when necessary for the supervision and management of the risks to be exposed to money laundering, financing of terrorism and proliferation of weapons of mass destruction at the Ziraat Finance Group level and for the implementation of an effective compliance program on a group basis. Necessary measures are taken to ensure the confidentiality of the information received and its use only for its intended purpose.

Within the scope of information sharing within Ziraat Finance Group, customer, account, ultimate beneficiary and transaction information can be shared. Within the framework of information sharing, although information can be shared regarding the existence of a extraordinary situation/transaction, information cannot be shared regarding the notification of a suspicious transaction.

The Board of Directors of the parent financial institution, together with the financial group compliance officer, is responsible for taking the necessary measures to share information securely within the group.

3.3. Protection and Processing of Personal Data

The processing of personal data takes place at account opening for customer due diligence purposes and subsequently for risk mitigation purposes in relation to the transactions carried out by the customers, including the risk of AML/CFT/PFPWMD prevention.

Personal data are collected for the following purposes within the scope of AML/CFT/PFPWMD legislation:

- Conducting customer due diligence,
- Ongoing monitoring,
- Investigation and reporting of unusual and suspicious transactions,
- Identification or legal arrangement of the ultimate beneficial owner of the legal entity,
- Information sharing by the competent authorities,
- Information sharing with credit institutions, financial institutions and other obligated entities.

The personal data collected includes the following information:

• Identification information of customers and third parties (e.g. name, surname, date of birth (including place of birth for non-Turkish nationals), address, identification number, identity of the actual beneficiary),

• Financial and economic data (e.g. assets, income, number of accounts, country location of accounts, frequency of money transfers, destination, etc.),

• The purpose and nature of the business relationship or intended transaction,

• The regularity or duration of the employment relationship,

• Transactions carried out in the course of the business relationship (e.g. size of transactions, origin of funds, whether these transactions are consistent with the intended purpose, unusual transactions that may reveal suspicious transactions...),

• Individual AML/CFT risk assessment (through scoring, segmentation and profiling).

Obtaining personal data during customer due diligence (CDD) is limited to what is necessary for the purpose of AML/CFT/PFPWMD and for the conduct of the customer's business.

The personal data obtained will be processed by the Bank for the purpose of preventing the laundering of proceeds of crime and the financing of terrorism / proliferation of weapons of mass destruction and will not be further processed in a manner outside of these purposes. Personal data will not be processed for any other purpose, such as commercial purposes.

4. MISCELLANEOUS

This policy enters into force on the date it is approved by the Bank's Board of Directors or by the member(s) to whom the Board has delegated its authority and the commitment forms regarding the Institution's policy are submitted to the MASAK Presidency within 30 days from the date of approval.

All personnel of the Bank are duly informed of this policy.