TÜRKİYE İŞ BANKASI A.Ş.

POLICY FOR COMBATING FINANCIAL CRIMES AND SANCTIONS

SECTION 1

GENERAL PRINCIPLES

1. INTRODUCTION

In parallel with increasing sensitivity expressed by the international community regarding combating Financial Crimes, legal adjustments aiming to strengthen the existing applications are also being realized in our country and significant importance is being attached to the subject.

Türkiye İş Bankası A.Ş. ("the Bank"), as it attaches great importance to it, adopts combating Financial Crimes as a social responsibility beyond a mere matter of complying with laws and regulations. The Bank, having a reputable and reliable status on international ground, attaches special importance to complying with international system in its operations from the time of it being founded till today.

2. DEFINITIONS

Basel Committee on Banking Supervision: The institution which is founded by the managers of central banks of G-10 countries to promote solid inspection standards throughout the world.
Beneficial Owner: Natural person(s) who ultimately control(s) or own(s) natural person who carry out a transaction within the Bank, or the natural persons, legal persons or unincorporated organizations on whose behalf a transaction is being conducted within the Bank.
Compliance Officer: Division Manager who shall be authorized and assigned by the Bank to make sure that the Bank shall act in compliance with its obligations arising from the applicable legislation pursuant to the Code on the Prevention of Laundering of Criminal Proceeds as well as the legislation put into force on the basis of that code.
Compliance Program: The integral package of the measures built in the Bank on the basis of the applicable Legislation and the Bank Policy to combat Financial Crimes.
Compliance Risk: Risk that the Bank may suffer sanctions, financial losses and/ or loss of reputation in the event that the Bank's operations and the attitudes and acts of the Bank's staff members are not appropriate and in compliance with the applicable legislation, regulations and standards.
Continuous Business Relationship: Business relationship that is established between the Bank and its customers through services such as opening an account, lending loan, issuing credit cards, safe-deposit boxes, financing, factoring or financial leasing, life insurance and individual pension, and that is permanent due to its characteristics.
Country Risk: Risk that the Bank may be exposed to due to the banking relations, or any transaction on the basis of those relations, that may be engaged with the individuals, corporations or financial institutors of a country, which is announced by the Ministry of Treasury and Finance, or lacks satisfactory regulations to combat Financial Crimes, or fails to

display a satisfactory performance of collaboration in order to prevent such crimes or is considered by the international institutions to be risky.

Customer Risk: Risk whereby the Bank may be abused on the grounds that the customer's business field requires the use of large amounts of cash; allow the trading of high-value assets or international fund transfers; or the customer or any person who acts on behalf of him acts for the purpose of Laundering of Proceeds of Crime and Financing of Terrorism.

Deputy Compliance Officer: Bank's personnel who shall fulfill the conditions and qualifications required for the Compliance Officer for the conduct of the Compliance Program and shall work under the Compliance Officer to conduct the duties mentioned in the relevant Legislation.

FATF: Financial Action Task Force

FCIB: Financial Crimes Investigation Board

Financial Crime: Activities with the content of Laundering of Proceeds of Crime, Financing of Terrorism, Insider Trading, or Manipulation.

Financial Group: The group consisting of branches, agencies, representatives, commercial agents and similar affiliated units of financial institutions that are resident in Turkey and are affiliated to or controlled by a parent institution whose head office is in Turkey or abroad.

Financial Group Policy: Türkiye İş Bankası A.Ş. Financial Group Policy for Combating Financial Crimes.

Financing of Terrorism: Providing or collecting funds for a terrorist or for terrorist organizations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime by the law.

Insider Trading: To give purchase or sale orders for capital market instruments or change the orders that are given or cancel them and thus to provide a benefit to oneself or someone else based on information concerning directly or indirectly capital market instruments or issuers which can affect the prices of the related capital market instruments, their values or the decisions of investors and which have not been declared to the public yet.

Laundering of Proceeds of Crime (Laundering): Transactions whereby those earnings raised from unlawful means are injected into the financial system so as to convert them into non-cash form in particular to create the impression that they are derived from legal means, and to make them pass through a process in the financial system so as to conceal the illegal origins of the funds.

Legislation: The applicable law, regulations and communiqués as well as the decisions and orders by the FCIB to prevent Laundering of Proceeds of Crime and Financing of Terrorism.

Manipulation: To make purchases and sales, give orders, cancel orders, change orders or realize account activities with the purpose of creating a wrong or deceptive impression on the prices of capital market instruments, their price changes, their supplies and demands.

Payable Through Account: Type of account that is opened in a financial institution located in Turkey within the scope of correspondent relationship by a financial institution located abroad, and that enables customers of the foreign financial institution to draw cheques.

Policy: Bank Policy for Combating Financial Crimes and Sanctions.

Politically Exposed Person: State or government president having top level public responsibilities, top level politicians, government officials, judicial or military personnel, representatives of political parties attaining an important status, people who are managers of public institutions, and family members and close associate.

Risk: The financial losses or loss of reputation that the Bank or the Bank employees may suffer due to the fact that the services offered by the Bank are used to Laundering of Proceeds of Crime and Financing of Terrorism, or due to the failure to completely comply with the

obligations imposed by the Code on the Prevention of Laundering of Criminal Proceeds, or any other regulations or communiqué enacted on the basis of that code.
Senior Management: Chief Executive Officer and Deputy Chief Executive Officers of the Bank and managers of divisions within the scope of Internal Systems.
Service Risk: Risk that the Bank may be exposed in relation to new products that may be offered by using ever developing technologies or to certain services such as transactions not carried out on a vis-à-vis basis, private banking or correspondent banking.
Shell Bank: A bank which does not have any physical office in any country, does not employ full time staff and is not subject to control and authorization of an official authority in terms of banking transactions and registrations.
Suspicious Transaction: The case where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the Bank, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.
Wolfsberg Group: Organization which is established by 13 global banks and which is aiming to develop standards for banks to combat Financial Crimes and Sanctions.
Sanctions: Regulations aimed at comprehensively or non-comprehensively restricting or blocking the economic activities of the countries, individuals or entities to achieve economic and political goals.
Comprehensive Sanctions Target Countries/Regions: Countries or regions which are subject to country/region-wide sanctions by The Republic of Turkey, United Nations Security Council, United States of America, European Union or United Kingdom.

3. PURPOSE AND SCOPE

The Policy basically intends to ensure;

- Implementation of Bank Compliance Program which is established with a risk based approach to ensure Bank's compliance with the obligations imposed by the Legislation, taking into account the international recommendations, standards, and best practices published by the FATF, Basel Committee of Banking Supervision and Wolfsberg Group.
- the Bank's compliance with domestic and international sanctions,
- Determining the strategies, controls and measures, processing rules, and responsibilities by evaluating the customers, transactions, and the services being provided with a risk based approach aiming to reduce and control the risks which the Bank can be exposed to, including the risk of losing reputation.
- Strengthening the corporate culture of the Bank's employees with regards to fight against Financial Crimes and Sanctions.

Financial subsidiaries that are within the Türkiye İş Bankası A.Ş. Financial Group shall comply with the Financial Group Policy.

It is expected from foreign financial subsidiaries, branches and representative offices of Türkiye İş Bankası A.Ş., to take all necessary measures and to realize the necessary actions in order to comply with the Policy related with their activities. The provisions in the Policy comprise the minimum measures to be complied with and if it is required to implement more strict measures according to the regulations of countries where the foreign financial subsidiaries, branches and representative offices of Türkiye İş Bankası A.Ş. are operating, the

relevant measures that are more strict shall be applied. If the legislation of the relevant country does not permit the measures included in the Compliance Program to be applied, this is reported to FCIB and additional measures are taken.

4. MISSIONS, DUTIES AND RESPONSIBILITIES

The Bank's Board of Directors is the ultimate body responsible for the conduct of the Policy and the Compliance Program as a whole in an adequate and effective way.

Within the scope of Compliance Program, Board of Directors is authorized and responsible for;

- Ensuring the Bank's compliance with provisions regarding combating Financial Crimes,
- Approving the Policy, annual training programs and amendments to be made to these as per the developments,
- Assigning the Compliance Officer and Deputy Compliance Officer,
- Approving the charter for the Corporate Compliance Division governing the duties, powers and responsibilities of the Compliance Officer and Corporate Compliance Division,
- Evaluating the results of risk management, monitoring, control, and internal audit activities and ensuring that the necessary measures have been taken,
- Ensuring that all activities are carried out in a coordinated and effective way.

Senior Management of the Bank is responsible to Board of Directors for;

- Establishing the workflows and assignment regulations within the frame of principles of corporate management for banks as to comply with the Policy,
- Implementation of the processes by all employees in line with the purpose and in an effective way,
- Taking the required measures in a timely manner to ensure that the Bank mitigates the risks relating with Financial Crimes and Sanctions.

Compliance Officer who reports to the Board of Directors is assigned, authorized and responsible for;

- Undertaking those efforts in order to make sure that the Policy and Compliance Program is applied and pursue the necessary communication and coordination with the FCIB ,
- Establishing the Policy and submitting it to the Board of Directors for approval,
- Developing, updating, publishing and monitoring the Bank procedures in relation to the implementation of the Policy and the Compliance Program within the Bank, and to monitor and coordinate how those procedures are implemented in practice,
- Carrying out the monitoring and control activities as well as risk management activities,
- Submitting the works relating with training program to the Board of Directors for approval and enabling the implementation of approved training program in an effective way,
- Evaluating the information and findings obtained from Suspicious Transactions and reporting the transactions that were deemed to be suspicious to FCIB,

- Keeping records of information and statistics relating with internal audit and training activities and reporting them to FCIB within the set deadlines.

Compliance Officer may transfer some or all of its duties and authorities to the Deputy Compliance Officer in a clear and written way.

All the employees of the Bank working at all levels, are obliged to perform all their tasks and carry out their responsibilities in a correct and careful way, by adhering the Policy, relevant processes and Compliance Program in the Head Office and branches of the Bank with the aim to prevent the Bank from being faced with risks relating to Financial Crimes and Sanctions. In cases of noncompliance with the Policy or the Policy is violated in some way, disciplinary penalties can be enforced.

Effectiveness and efficiency in implementing the Policy and Compliance Program will be regularly subject to inspection and evaluation within the scope of internal audit. The findings that are stated on the reports being issued are primarily handled by the responsible divisions by considering Compliance Risk. Findings of audit relating to Compliance Risk are submitted to Corporate Compliance Division and to the Board of Directors through the Audit Committee.

SECTION 2

KNOW YOUR CUSTOMER

5. KNOW YOUR CUSTOMER PRINCIPLE AND RULES FOR ACCEPTANCE OF CUSTOMERS

The "Know Your Customer" principle is the foundation of customer acceptance process of the Bank regarding combating Financial Crimes.

The Bank attaches great importance on the "Know Your Customer" principle in order to be protected from persons and actions relating to Financial Crimes and Sanctions and carries out an implementation that complies with the international standards, recommendations, and applicable regulations.

Within the scope of "Know Your Customer" principle, the Bank performs the following,

- Identifying the customer,
- Identifying the Beneficial Owners,
- Obtaining sufficient information about the purpose and nature of requested process,
- Performing risk assessment of customer during customer acceptance process and updating the risk assessment during the business relationship in a dynamic way,
- Evaluating the customers and transactions in terms of the principals in Section 3 – Sanctions,
- Monitoring the transactions of the customer during the business relationship,
- Taking the necessary measures relating with customers, activities and transactions requiring special attention,

The said measures are performed by the responsible divisions within the frame of Legislation and Policy and the processes are established under the responsibility of Senior Management.

The Bank takes the necessary measures to avoid business relationships to be established with sanctioned persons, institutions and organizations listed in resolutions published by United Nations Security Council under the Law on the Prevention of the Financing of Terrorism and the Law on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction. All kinds of accounts, rights, assets of the persons, institutions and organizations that are not included in the aforementioned lists at the stage of establishing Continuous Business Relationship, but later amended to those lists, are frozen and reported to FCIB within the period specified in the law.

The Bank performs monitoring and control activities in relation to Politically Exposed Persons within the frame of country Legislation.

In the customer acceptance process, in line with the risk parameters defined by the Bank, risk scores of customers are determined in a systematic way and the appropriate customer acceptance processes are implemented. Furthermore, during the Continuous Business Relationship, all customers are subject to dynamic risk scoring.

In cases where identification cannot be done or sufficient information about the purpose of business relationship cannot be obtained, the Bank does not establish a business relationship

or carry out the transactions of the related parties until the suspicion and deficiencies are overcome.

In accordance with the obligations of the Bank within the scope of international banking regulation and practices and its correspondent relationships, in case of justified reasons, business relationships can be terminated or the services provided can be restricted.

The Bank;

- Does not establish Continuous Business Relationship with anonymous or with fictitious names, with real persons and legal entities that are dealing with gambling/illegal betting and with real persons and legal entities that are subject to the restrictions stated in Section 3 - Sanctions.
- Closes the accounts and terminates the business relationship with customers who are determined as dealing with fraud or gambling/illegal betting, who does not provide the information and documents requested from them about themselves and their transactions, for whom termination of business relationship decision is made within the context of the monitoring, control and risk management activities or who become subject to the restrictions stated in Section 3 – Sanctions after the customer record has been made. As an exception to this article, accounts of the persons, institutions and organizations, that become subject to United Nations Security Council resolutions under the Law on the Prevention of the Financing of Terrorism and the Law on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction after the customer record has been made, are not closed but all kinds of accounts, rights, assets are frozen and reported to FCIB within the period specified in the law.
- Does not establish correspondent relationships with Shell Banks and with banks that allow their accounts to be used by the Shell Banks. The Bank does not allow the accounts, that are established for the correspondent banks, to be used as Payable Through Accounts and closes the accounts that are used for such transactions.
- Although it is essential to prevent other banks holding accounts with the Bank from accessing accounts with other financial institutions through their foreign currency accounts in connection with customer transactions, the actions to be taken in this regard are determined by considering international good practices and the limitations determined by correspondent banks.

6. IDENTIFICATION

At the establishment of the Continuous Business Relationship and before any transaction is realized, first of all the Bank identifies the customer within the frame of applicable regulations, Policy and procedures on a timely and correct manner.

Identification is performed,

- irrespective of the amount where a Continuous Business Relationship is established,
- irrespective of the amount whenever there is a suspicion as to the sufficiency and correctness of the customer identity obtained before;
- irrespective of any amount in circumstances where a Suspicious Transaction should be reported;

- whenever the transaction amount, or the aggregate amount of more than one transaction linked to each other exceed the threshold defined in the applicable Legislation

by obtaining identity information of customers and those acting on behalf of the customers and by verification of this information.

The Bank can establish business relationships or carry out transactions by relying on measures taken related to the customer by another financial institution on identification of the customer, the person acting on behalf of customer and the Beneficial Owner, and on obtaining of information on the purpose of business relationship or transaction.

Reliance on third parties is possible only if it is ensured that;

- the third parties have taken other measures which will meet the requirements of customer identification, record keeping and the principles of "customer due diligence", and are also subject to regulations and supervision in combating Money Laundering and Financing of Terrorism in accordance with international standards if the third parties are resident abroad,
- the certified copies of documents relating to customer identification shall immediately be provided from the third party when requested.

In case of the establishment of business relationship by relying on a third party, the customer's identification information shall be immediately received from the third party. In such instances, the ultimate responsibility shall remain with the Bank.

The principle of "reliance on third parties" may not be applied to the cases where the third party is resident in a risky country.

Regarding foreign correspondent relationships;

- In order to evaluate the system of correspondent financial institution for the purposes of the prevention of Laundering and Financing of Terrorism and to ensure that the system is proper and effective, the policy and questionnaire documents of the relevant institution are obtained and investigated.
- Questionnaires and sources that are open to public are used in order to determine whether the correspondent financial institution has been investigated and fined or warned regarding Laundering and Financing of Terrorism, their business activities, reputation and sufficiency of audit.
- Establishment of new correspondent relationship or termination of existing correspondent relationship with the initiative of the Bank is executed with the approval of Deputy Chief Executive Officer to whom the activities relating with correspondent banking is reported.
- When the policy and questionnaire documents that are obtained from the correspondent bank are updated, the risk category under which the correspondent bank is evaluated is also considered.
- When account relationship is established, responsibilities of the Bank and the correspondent financial institutions are specified in a contract.

- Foreign branches and foreign subsidiaries of the Bank get opinion of Financial Institutions Division of the Bank at the stage of establishing correspondent relationship.

In accordance with the procedures established in line with the Policy, for the purpose of establishing a Continuous Business Relationship and undertaking the requested transactions, necessary measures are duly adopted and diligently applied to identify and know the Beneficial Owner.

Special attention is paid to complex and large-amount transactions and to those which do not have a reasonable legal or economic purpose and the necessary measures are taken to obtain sufficient information about the purpose and nature of transaction that is requested.

SECTION 3

7. SANCTIONS

In addition to national legislation, as a minimum, the Bank shall ensure full compliance with the sanctions as announced by,

- United Nations Security Council (UNSC),
- European Union,
- United States of America,
- United Kingdom

and which are applicable to its activities. Exceptionally and subject to the approval of the Corporate Compliance Division, the Head Office may adhere to other sanction regimes in addition to the aforementioned. In that case, the sanctions lists to be considered are to be determined by the Corporate Compliance Division.

The Bank shall maintain and implement a compliance program to assess and address the sanction risks exposed by. The Bank does not get involved intentionally in any transaction designed to circumvent the sanctions.

The Bank oversees sanction risks at the customer onboarding, customer information update and executing customer transactions. In this regard,

- Customers and their shareholders, power of attorney holders and beneficial owners are screened against sanctions lists.
- Customer transactions to be carried with or through the Bank are screened to ensure they do not directly or indirectly involve Comprehensive Sanctions Target Countries/Regions and/or individuals or entities subject to sanctions.
- Until the review of the screening results is completed by the authorized personnel, customer onboarding and/or transactions are not concluded.
- Customers are periodically screened against the aforementioned sanction lists.

The Bank does not establish business relationships within the scope listed below, without prejudice to the legal requirements, terminates existing business relationships with the customers that are:

- Subject to United Nations Security Council sanctions
- Designated as Specially Designated Nationals (SDN) by the U.S. Treasury Department The Office of Foreign Assets Control
- Owned directly or indirectly 50% or more by the individuals or entities designated as SDN
- Domiciled / registered in Comprehensive Sanctions Target Countries/Regions

The transactions of these the individuals and entities within the scope of licenses and similar documents issued by the competent authorities can be performed exceptionally and with the approval of the Corporate Compliance Department. Except for those mentioned in the above paragraph, in case the relevant sanction program permits to maintain the customer relationship or to execute the transaction, the final decision rests with the Corporate Compliance Division.

The extend of the relationship with the customers who pose risk in terms of sanctions for the Bank shall be determined by the Corporate Compliance Division with a risk-based approach.

In this regard,

- Corporate Compliance Division may terminate customer relationships categorically or a case basis.
- Access to services and products might be restricted for some customers.

Türkiye İş Bankası A.Ş.'s financial subsidiaries, foreign branches and representative offices are expected to take and fulfill all necessary measures to comply with the Sanctions related provisions of the Policy to the extent that they are related to their field of activity. These provisions in the Policy include the minimum measures to be implemented; if the Bank's financial subsidiaries, foreign branches and representative offices are required to implement more stringent measures than the aforementioned provisions in the Policy in accordance with the legislation of the countries in which they operate, the relevant strict measures are applied.

It is essential that financial subsidiaries should act in line with the guidance and limitations shared by the Bank regarding the implementation of the provisions related with Sanctions.

SECTION 4

RISK MANAGEMENT

8. PURPOSE AND SCOPE OF RISK MANAGEMENT

The main purpose is to define, grade, assess, and minimize the risks related to Financial Crimes and Sanctions which the Bank can be exposed to.

For this purpose, the Bank grades the customers, services, products, and countries within the frame of customer, service, and country risks that could be exposed to. The Bank manages these risks by establishing the processes that define, rate and assess those starting with the customer acceptance process. In this regard, the results of national risk evaluation are also taken into account.

9. RISK MANAGEMENT ACTIVITIES

Risk management activities are designed by the Compliance Officer within the frame of relevant regulation and Policy provisions and carried out by Corporate Compliance Division.

The activities relating with risk management covers;

- Developing risk defining, rating, classifying and assessing methods based on Customer Risk, Service Risk and Country Risk,
- Rating and classifying services, transactions and customers depending on risks,
- Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; taking necessary measures to mitigate the risks; reporting in a way that warns related units; carrying out the transactions with the approval of Senior Management and controlling those when necessary,
- Questioning retrospectively the coherency and effectiveness of risk defining and assessing methods and risk rating and classifying methods depending upon sample events or previous transactions, reassessing and updating them according to achieved results and new conditions,
- Carrying out required development work through pursuing principles, standards and guidelines established by national Legislation and international organizations related to issues under the scope of risk,
- Reporting risk monitoring and assessing results to the Board of Directors.

Countries, customer groups, products and services that are within the high risk category are specified by the Corporate Compliance Division utilizing a risk based approach within the frame of Legislation and Policy and those are subject to effective monitoring and controls in accordance with their qualities.

In assessing the Customer Risk relating with Financial Crimes and Sanctions, basically the below criteria are considered:

- Occupation and activity of customer,
- Establishment type of customers which are legal entities,

- Level of suitability and sufficiency of implementations for regulating and inspections with regards to combating Financial Crimes of the activity of the customer and/or the country and/or region, of which the customer is a citizen of and/or is residing and/or operating in,
- Duration of current banking relationship of customer with the Bank,
- The activity period of customers which are legal entities,
- The type and nature of banking products and services being used by the customer,
- News about the customer being published in media with negative content (if any).

At the beginning of banking relationship and during the continuation of relationship, the customers are placed in appropriate risk categories with respect to their activities and the nature and scope of their transactions and relations with the Bank, taking into account above stated fundamental criteria and other specific information and criteria about the customer.

Information and documents that are obtained from the customers within the scope of the "Know Your Customer" principle are updated once a year for customers within high risk category, once in two years for customers in medium risk category, and once in four years for customers in low risk category.

Customers in high risk category and their transactions are monitored closely with monitoring and control methods that are appropriate for the purpose. Enhanced due diligence is implemented for the customers who are in high risk category with regards to customer, service, and country risks. Within this frame, the central monitoring and control activities that are designed and carried out with a risk based approach within Corporate Compliance Division, are mainly focused on customers and transactions within high risk category.

In order to reduce the risks undertaken relating with the groups which are specified as being high risk as a result of risk assessment, one, more than one or all of below stated additional measures, at least, are taken:

- Developing procedures for ongoing monitoring of transactions and customers,
- Requiring approval of the next level personnel for establishing business relationship, sustaining current business relationships or carrying out transactions,
- Gathering as much information as possible on the intended nature of the business relationship, purpose of the transaction and source of assets that are subject to transaction,
- Obtaining additional information and documents under the scope of customer due diligence, and taking additional measures for verifying and certifying the information submitted, updating more frequently the identification data of customer and Beneficial Owner,
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that need further examination,
- Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution which applies customer due diligence principles,
- Developing processes for specifying the type of customers with whom business relationships will not be established or who will not be allowed to use certain products and services.

The risk categories of the customers are determined according to the identification information, business activities and the other customer information compliant with the current Legislation and international standards.

In this regard, the individuals and companies that are;

- Specified as to be applied special attention as per FATF recommendations,
- Required to be monitored closely if they are resident of or associated with risky countries or regions,
- Engaged in high risk activities in terms of Laundering of Proceeds of Crime and Financing of Terrorism due to the international standards (activities including intensive use or transfer of cash/foreign currency, activities dealing in high-value items etc.),
- Required to be monitored closely with special attention as being accepted to be risky and unfavorable by the authorized legal bodies due to the connection with Laundering of Proceeds of Crime and Financing of Terrorism and other Financial Crimes,
- Frequently using banking products and services in high risk category

and other customers that are required to be monitored closely since their current profiles, activities or banking relationship and transactions are deemed as risky in the concept of the risk management, monitoring and control activities included in the Compliance Program that is being carried out in compliance with the international standards, domestic Legislation and this Policy.

In terms of Service Risk;

- Electronic transfers,
- Private banking products and services,
- Systems that allow non-face-to-face transactions,
- Products and services based on new and advancing technologies,
- Correspondent banking transactions,
- Businesses and transactions, the ultimate beneficiaries of which are not clearly and completely defined,
- Other products, services and types of transactions that are required to be given special attention in the concept of the risk management, monitoring and control activities included in the Compliance Program that is being carried out compliant with the international standards, domestic Legislation and this Policy,

are monitored within high risk category.

Within the scope of Country Risk, the countries that are designated as being high risk in accordance with the criteria specified below are closely monitored:

- Evaluations whether they have got sufficient regulations and implementations with regards to combating Financial Crimes, being realized within the scope of recommendations issued by FATF,
- The report being prepared by United Nations Narcotic Drugs and Crime Office and reflecting the situation of countries with regards to narcotic drugs,

- The report being prepared by United Nations Narcotic Drugs and Crime Office and reflecting the situation of countries with regards to human trafficking,
- Corruption perception index being issued by international institution named "Transparency International" and reflecting the indices of countries relating with corruption,
- International Narcotic Control Strategy Report (INSCR),
- Countries being specified on the list of "Risky Countries" announced by the Ministry of Treasury and Finance,
- Countries to which sanctions are implemented at an international level within the frame of decisions of United Nations Security Council due to the policy and implementations relating with Laundering of Proceeds of Crime or Financing of Terrorism,
- Countries being announced by European Union or OFAC (Office of Foreign Assets Control) and being specified as bearing high risks,
- Offshore centers, free zones, and finance centers,
- Tax havens.

SECTION 5

MONITORING AND CONTROL

10. PURPOSE AND SCOPE OF MONITORING AND CONTROL

The main purpose of the monitoring and control procedures is to protect the Bank against the risks and to ensure that its operations are constantly monitored and controlled subject to the applicable Legislation and the Policy and procedures.

Monitoring and control activities are established and applied on a risk-based approach. In this respect, certain monitoring and control methods that suit the nature and level of risks associated with the Bank customers, transactions and services shall be developed and effectively implemented.

11. MONITORING AND CONTROL ACTIVITIES

Monitoring and control activities are designed and conducted using a risk-based approach under the coordination and supervision of the Compliance Officer subject to the applicable Legislation and the present Policy. In this respect, in addition to standard controls applicable to all operations of the Bank, certain appropriate and effective control processes, systems and methods are identified and implemented in order to monitor more closely those customers, transactions and operations that are deemed to be of high risk and require special diligence and attention.

Monitoring and control activities basically cover the following:

- Monitoring and control of high-risk customers and transactions,
- Monitoring and control of transactions executed with risky countries,
- Monitoring and control of complex and unusual transactions and transactions that don't have any reasonable legal and economic purpose,
- Controlling those transactions above a specific amount threshold through sampling in order to check its consistency with the customer profile,
- Monitoring and control of transactions that are linked to each other and exceed the amount which requires the identity verification,
- Controlling the veracity, up-to-dateness and adequacy of customer data and documents, and ensuring that missing ones are remediated,
- Continuous monitoring of the compliance of a customer transaction with the information compiled about his scope of business, risk profile and sources of funds throughout the transaction,
- Controlling the transactions carried out through systems that allow the execution of transactions without a vis-a-vis relation,
- Risk-focused control of those services that may remain exposed to abuse and risks in respect of Financial Crimes and Sanctions on the grounds of new products and technological developments and
- Other monitoring and controls that may be necessary in this respect.

Central monitoring and control activities are carried out by the Corporate Compliance Division. To effectively implement the Compliance Program in accordance with the applicable Legislation and the Policy and procedures at the Bank's Head Office and its

branches, on-the-spot audit and control of the compliance of the transactions, are provided through internal audit and internal control activities. Results of the central monitoring and control activities as well as the data and information reported as a result of the internal audit and internal control activities are monitored and evaluated as a whole by the Corporate Compliance Division under the supervision of the Compliance Officer.

SECTION 6

TRAINING

12. PURPOSE AND SCOPE OF TRAINING

Purpose of the training provided to all the related employees of the Bank, is to improve corporate culture and awareness in regards to the risks relating with Financial Crimes and Sanctions and in regards to the legal obligations, Policy, procedures, and practices of the Bank within this scope and to provide the up to date information to the employees. Training program is established by considering the risks of country, region, and the Bank and it is managed in a dynamic way.

13. TRAINING ACTIVITIES

Training activities of the Bank are designed and carried out under the supervision and coordination of the Compliance Officer, within the frame of provisions of the relevant regulations and Policy and shall extend to the entire personnel related thereto. Training program is prepared by the Compliance Officer, with the participation of relevant divisions of Head Office on an annual basis and it is approved by the Board of Directors. Implementation of the training program in an effective way is monitored by the Compliance Officer.

In order to ensure that the training activities are applied throughout the Bank, in-class training, e-training, other training methods, visual and audial training materials, communication channels such as internet or intranet are utilized in an effective way.

Special importance is given to selecting the lecturers who will give the trainings and in providing them the necessary trainings for this purpose.

Content of trainings are differentiated in accordance with the purpose by considering the assignment period, title, and duties of Bank's employees, and it is enabled for each related employee to get the trainings within this scope at least once in a year. The timely completion of the trainings that are assigned to the employees is the responsibility of the related Division/Region/Branch managers as well. Within the frame of amendments in the Legislation relating with the subject and per other developments, certain updates can be made in the content of trainings on a timely manner.

It is followed up and evaluated closely to ensure that the trainings are suitable and sufficient for meeting the requirements. Training activities are reviewed as per the measurement and evaluation results, with the participation of relevant divisions and they are repeated at regular intervals in accordance with the needs.

The necessary information and statistics regarding the training activities carried out within the framework of regulations are kept regularly and they are reported by the Compliance Officer to FCIB within the specified durations and principles.

14. TRAINING SUBJECTS

The trainings shall at least cover the following subjects;

- Laundering of Proceeds of Crime and Financing of Terrorism terms,
- The stages, methods of Laundering of Proceeds of Crime and case studies on this subject,
- Legislation regarding prevention of Laundering of Proceeds of Crime and Financing of Terrorism,
- Risk areas,
- Institutional Policy and procedures,
- Within the framework of Law and related Legislation;
    - Principles relating to customer identification,
    - Principles relating to Suspicious Transaction reporting,
    - Obligation of keeping and presentation of documents,
    - Obligation of providing information and documents,
    - Sanctions to be implemented in case of violation of obligations,
- The international regulations on combating Laundering and Financing of Terrorism.

SECTION 7

INTERNAL AUDIT

15. PURPOSE AND SCOPE OF INTERNAL AUDIT

Purpose of internal audit is to provide assurance to the Board of Directors in regards to the effectiveness and sufficiency of integrity of this Policy and Compliance Program.

Within the scope of internal audit,

- Establishment and execution of business processes of the Bank in accordance with the Policy,
- Efficiency and effectiveness of Policy, processes, risk management, monitoring, control, and training activities and compliance of Bank activities with the applicable regulations, Policy, and procedures

are investigated and evaluated with a risk-based approach within the frame of regulations on an annual basis and the deficiencies, mistakes, and abuses that are determined are reported to the Board of Directors together with the opinions and proposals aiming to avoid them to reoccur.

16. INTERNAL AUDIT ACTIVITIES

Principles and methods relating with implementation and reporting about the internal audit activities are arranged and implemented within the frame of Policy by Board of Inspectors.

While determining the scope of internal audit, findings identified during the monitoring and control works and risky customers, services, and transactions are included within the scope of audit.

While the divisions/branches and operations that will be audited are determined, organization structure, business and transaction volume of the Bank are also considered. Within this scope, it is ensured that the divisions/branches and transactions, that can represent all of the transactions that are realized within the Bank, are audited.

The information and statistics required within the frame of regulations in relation with the internal audit activities are kept on a regular basis and they are reported by the Compliance Officer to FCIB as per the specified periods and principles.

SECTION 8

OTHER PROVISIONS

17. SUSPICIOUS TRANSACTION REPORTS

In case there are information or matters creating suspicion that a transaction that is realized or attempted to be realized within the Bank or with the mediation of Bank, is related or connected with the Laundering of Proceeds of Crime and Financing of Terrorism, by conducting necessary researches within reasonable limits, reporting of transaction being deemed as suspicious is made to FCIB within the frame of specified periods and principles.

If there are documents supporting the suspicion that a transaction being attempted or continued is related with Financial Crimes or if there are serious indications in that regard, Suspicious Transaction reporting is made to FCIB by submitting the justifications and requesting for the transaction to be delayed and during the period determined by the Legislation, it is avoided for the transaction to be realized.

Necessary communication and cooperation required by the applicable Legislation are established between the parties involved in the process of identification, examination and consideration and reporting of the Suspicious Transaction to the FCIB.

For ensuring the confidentiality and safety of Suspicious Transaction Reports and internal reports being produced by the Bank in this regard, and for protecting the parties involved in these reports, the maximum care required within the frame of Legislation is exhibited by those who are involved in this matter.

18. MAINTENANCE AND CONFIDENTIALITY OF INFORMATION, DOCUMENTS, AND RECORDS

All information, documents, and records that are required to be obtained and preserved in relations to the customers and transactions in accordance with the regulations, are kept within the frame of periods and principles specified by Legislation, in a way to be available whenever they may be required.

Necessary measures are the confidentiality of the relevant data, documents and records. Reporting activities for the purposes of continuous information disclosure as well as requests from those authorities authorized to seek information and documents under the applicable Legislation are fulfilled with utmost diligence, subject to the applicable Legislation.

In order for the measures regarding the Compliance Program to be taken groupwide, the Bank may share the information about knowing the customer, their accounts and transactions with the institutions in the Financial Group on the basis specified in the Financial Group Policy.

19. EFFECTIVENESS AND REVIEW

The Policy becomes effective on the date it is approved by the Board of Directors. The Policy is reviewed at least once in a year with the aim to ensure compliance with the regulations and international standards and updates, whenever required, are submitted for the approval of

Board of Directors. Any amendments or updates that may be realized in relation to the Policy later on are also enforced with the approval of the Board of Directors.