

Anti Money Laundering Policy



ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM COMPLIANCE POLICY

Within the scope of Anti-Money Laundering & Countering the Financing of Terrorism (AML/CFT), Weapons of Mass Destruction (WMD) and Bribing Foreign Public Officials as well as Sanctions Programs; taking into account the damage these cause in social life, Türkiye Halk Bankası A.Ş approaches the compliance with legal and international regulations within the framework of social responsibility and attaches great importance to this effort.

DEFINITIONS AND ABBREVIATIONS

- ◆ **Asset:** The fund, all kinds of proceeds, benefits and values derived from conversion of them into one another, jointly or wholly owned or possessed or directly or indirectly controlled by a natural or legal person.
- ◆ **BCBS - Basel Committee on Banking Supervision:** A committee formed by the central banks of the developed countries and senior officials from the banking supervisory authorities, responsible for ensuring that banks work in line with international standards set by the Bank of International Settlements (BIS).
- ◆ **Bribery:** An offer, promise, grant, request or acceptance of an advantage in promoting an action that is illegal, unethical or in violation of confidence.
- ◆ **BRSA - Banking Regulation and Supervision Agency:** A public institution with a public legal personality that has administrative and financial autonomy. The agency reports to the Prime Ministry. The purpose of its establishment is to independently carry out the duties and authorities conferred by Law and other relevant legislation under its own responsibility.
- ◆ **Compliance Officer:** Refers to a person employed and assigned by the appropriate authority within Türkiye Halk Bankası A.S. and its subsidiaries subject to consolidation to ensure compliance with the obligations imposed by legislation enacted on the basis of the Law on AML/CFT and the Law.
- ◆ **Compliance Program:** The overall measures to be taken to prevent ML/FT.
- ◆ **Compliance Unit:** The unit which is composed of employees working attached to the compliance officer and charged with the conduct of the compliance program.
- ◆ **Crime Revenue - Black Money:** In general terms, a monetary asset or property that is not obtained through legal means and/or of which the relevant tax has not been paid.
- ◆ **EU - European Union:** A political and economic organization established by Member States based mainly in Europe, and named "the European Union" for the first time with the entry into force of the "Maastricht Treaty" on February 7, 1992. As part of the regulations established by the European Council, restrictive measures or arms embargoes applicable to commercial, financial or individual persons can be applied by the EU member states.
- ◆ **Executive (Top-level) Management:** The general manager and assistant general managers of a bank, the managers of the units included within the scope of the internal systems, and those managers of the non-advisory

units who serve in positions equivalent or superior to the position of assistant general manager in terms of their powers and duties even if they are employed with other titles.

- ◆ **FATF - Financial Action Task Force:** Established in 1989 by the G-7 countries within the OECD, the FATF takes measures to improve national legal systems, to harmonize legislation and strengthen the role of the financial system, and to ensure continuous cooperation among the member states in the fight against the laundering of crime revenues and the financing of terrorism.
- ◆ **FINCEN - Financial Crimes Enforcement Network:** Working under the US Treasury Department, FINCEN is a provider of intelligence and analytical networks to the State, monitoring and implementing policies to prevent and detect ML activities, identifying and investigating national and international laundering activities and other financial crimes, and supporting their investigation and prosecution.
- ◆ **Freezing of Asset:** Removal or restriction of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset.
- ◆ **Fund:** Money or property, right, claims of every kind whether movable or immovable, tangible or intangible which could be represented by money and all kinds of documents representing them.
- ◆ **FT - Financing of Terrorism:** The financing, mediating, helping or supporting the transfer of such financial activities through legal or illegal means to terrorists, terrorist organizations or their activities. (Providing or collecting funds with the intention of use or knowingly and willingly use, even without being linked to a specific act, in full or in part, for a terrorist or terrorist organizations)
- ◆ **Gatekeepers:** Referring to accountants, lawyers or other similar professional groups that open an account in a financial institution and act on the account of their respective customers.
- ◆ **Group:** Regardless of whether they operate under a different legal personality, this is the community consisting of the main partnerships established either at home or abroad under the main partnership of Halkbank of Turkey, depending on the same investor group.
- ◆ **Group Compliance Policy:** A common compliance policy aimed at the implementation of global standards to combat ML/FT in every country operating in the group.
- ◆ **HM Treasury (UK Department of Economics and Finance):** The Ministry responsible for improving and enforcing the UK government's public finance and economic policy by controlling public expenditures. The Office of Financial Sanctions Implementation (OFSI) working under HM Treasury, directs the public to properly understand and enforce sanctions imposed in the United Kingdom.
- ◆ **International Sanctions:** Decisions and regulations published by international authorities regarding money laundering, terrorist activities or countries, persons, legal entities or vessels subject to sanctions due to anti-democratic practices.
- ◆ **ML - Money Laundering:** Money laundering is any action taken to transfer the values of property originating from illegal activities abroad, or to hide their illegitimate source so as to convince that they have been obtained in a legitimate way. Laundering is carried out in a three- stage process:
 - In the first stage, revenues from a crime are converted into a form other than cash and entered into the financial system - **Placement**

- In the second stage, the money in a form other than cash is separated from its original illegal source as much as possible - **Decomposition**
- In the third stage, the laundered crime revenue is entered into the financial system after any links to the illegal source have been cut - **Integration**

- ◆ **Nested Account' Activities:** An account allowing a foreign institution accesses the domestic financial system (in effect anonymously) by operating through the correspondent banking account belonging to another foreign financial institution.

- ◆ **OECD - Organization for Economic Cooperation and Development:** The organization in which member states, with a democratic structure and market economy, work together to solve economic, social and governance problems related to globalization, and to take advantage of the opportunities offered in this process.

- ◆ **OFAC - The Office of Foreign Assets Control of the US Department of Treasury:** A section within the US Treasury Department that implements economic and commercial sanctions based on US foreign policy and national security objectives against individuals, groups and institutions linked to countries, regimes, terrorist-related groups, international drug traffickers, persons engaged in the dissemination of weapons of mass destruction, and other threatening activities.

- ◆ **Parent Bank:** Halkbank of Turkey, established in Turkey, where the financial statements of its subsidiaries and/or partnerships are controlled and consolidated.

- ◆ **Partnership in the form of Subsidiary-Consolidation:** A partnership operating under the control of the parent company.

- ◆ **Payable-Through Accounts (PTA):** 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.

- ◆ **PEPs - Politically Exposed Persons:** Including persons with significant public duties and positions, such as heads of state and government, senior judicial and government officials, military officials, senior executives of public organizations and leading political party officials.

- ◆ **Permanent Business Relationship:** A business relationship that is established with 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.

- ◆ **Risk:** The possibility that may expose to a Financial Institution or its employees of financial loss or loss of dignity due to use of its services for the purpose of money laundering or terrorist financing or not complying completely with the obligations established through the Law or Regulations and Communiqués issued in accordance with the Law.

- ◆ **Risky Countries:** The countries that are announced by the ministry out of those which do not have sufficient laws and regulations on prevention of money laundering and financing of terrorism, which do not cooperate on combating these offences or are considered risky countries by competent international organizations.

- ◆ **Senior Management:** The board of directors and top-level management of a bank.

- ◆ **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.
- ◆ **Shell Company:** A shell company is a non-trading organization that does not engage in any activity but exists only as a paper company usually located in offshore centers.
- ◆ **Suspicious Activity/Transaction Report (SAR/STR):** Reporting activities and transactions deemed suspicious to the authorities.
- ◆ **UN - United Nations:** Established in 1945, the United Nations is an international organization. As part of the regulations established by the United Nations Security Council, restrictive measures or arms embargoes applicable to commercial, financial or individual persons can be applied by the member states.
- ◆ **Wire Transfer:** The transaction carried out to transfer a certain amount of money and securities from a financial institution on behalf of the originator to the beneficiary persons in another financial institution by using electronic means.
- ◆ **Wolfsberg Group:** An association for banks created by some global banks, aiming to develop standards on combating money laundering and financing of terrorism.

PURPOSE

Determining strategies, internal controls and measures, operational rules and responsibilities of our Bank, aimed at provision of compliance of our Bank to its obligations relating to AML/CFT, Proliferation of Weapons of Mass Destruction (WMD) and Bribing Foreign Public Officials, to protect its national and international reputation; by evaluating customers, transactions and services with a risk based approach to reduce risk that our Bank might be exposed to; and increasing awareness of our employees on these issues.

Standards specified in this policy comprise the minimum requirements created by the legislation in force and aim to protect our Bank, our employees and our customers from exploitation on Money Laundering and the Financing of Terrorism Crime.

Our **Board of Directors is ultimately responsible** in ensuring the fulfilment of the Bank's "AML/CTF Prevention" obligations under the 5549 Law on the Prevention of Money Laundering.

SCOPE

Our policy relating to AML/CTF applies to all domestic and, to all foreign branches, representative offices provided that the legislation of the relevant country is applicable, offices and other service units and, Head Office departments and other similar units such as agencies and commercial representatives.

LEGAL BASIS

The Law on Prevention of Laundering Proceeds of Crime (No. 5549) and **the Law on the Prevention of the Financing of Terrorism (No. 6415)** and the Regulations and Communiqués published relating to this Laws constitute the legal basis of our Bank's policy on prevention of ML/FT. Also the recommendations, principles, standards and guidelines provided by national and international regulatory institutions and organizations, are taken into consideration.

The Financial Crimes Investigation Board (MASAK) directly reports to the Minister of Finance; and the duties and powers of MASAK are to develop policies and strategies, to prepare law, by-law and regulation drafts in accordance with the policies determined, to exchange views and information in order to prevent laundering proceeds of crime.

Financial Action Task Force (**FATF**), which was established in 1989 within the body of OECD, aims to devise the internal legal systems on preventing Money Laundering and reconcile regulations, strengthen the role of financial system and build the cooperation between the members. Since 1991, Turkey is member of FATF, of which the recommendations are obligatory for the member countries.

According to the 5237 TCK 282, the **Proceeds of Crime** is defined as any form of money/wealth/assets/interest acquired from the crimes that require punishment of minimum 6 months of imprisonment. **Laundering offence** means a person who transfers abroad the proceeds obtained from an offence requiring a minimum penalty of six months or more imprisonment, or processes such proceeds in various ways in order to conceal the illicit source of such proceeds or to give the impression that they have been legitimately acquired.

Through “The Law No.6415 on the Prevention of the Financing of Terrorism” within the scope of effective fight against terrorism and financing of terrorism; the principles and procedures have been determined for implementing the “International Convention for the Suppression of Financing of Terrorism” dated 1999 and the United Nations Security Council Resolutions related to combating terrorism and the financing of terrorism, for establishing financing of terrorism offence, and for freezing of asset with the aim of preventing financing of terrorism.

COMPLIANCE PROGRAM

Halkbank has established Compliance Program, including measures aimed at preventing Laundering and Terrorism, in order to comply with national legislation and international standards and fulfil control activities in this scope.

The compliance program shall cover the following measures:

- Developing AML/CTF policy and procedures
- Carrying out risk management activities within scope of preventing laundering proceeds of crime and financing of terrorism to define, grade, monitor, assess and reduce the risks the Bank may be exposed to
- Carrying out monitoring and controlling activities, within the scope of the Bank’s size of business enterprise, business volume and the nature of the transactions it conducts
- Assigning compliance officer and establishing the compliance unit
- Carrying out training activities within the scope of AML/CTF legislation
- Carrying out internal audit activities within the scope of the Bank’s AML/CTF policy and procedures

Risk management, monitoring and controlling activities shall be carried out by the Compliance Officer/the Compliance Unit.

Training activities are conducted under supervision and coordination of Compliance Officer.

Internal audit activities shall be carried out by the Board of Inspectors.

Within the scope of Compliance Program, risk management and control processes are conducted by paying regard to three lines of defense system and coordinating duties and responsibilities. The three lines of defense system consists of three stages which are playing very efficient role in risk management. At the first line of defense, the units (Branches and the relevant Head Office Units), which are decision makers undertaking the risk, take place.

The units at this stage are responsible for forming the proper system in line with the Policies and Procedures constituted by the Compliance Department as well as management and implementation of the processes. Understanding, evaluating and control of the business activities of our customers and the scope of business relationship with our Bank are among the duty fields of the units placed at this stage as per our “Know Your Customer (KYC)” Policy. The Compliance Department placed at the second line of defense is responsible for constituting the policies and procedures, managing the ML/FT risks which our Bank may be exposed to, conducting of monitoring and control activities and coordination of training activities. In order to be fulfilled this functions by the Compliance Department, sufficient human sources and technological opportunities are provided by taking into consideration the number of customers, the number of employees, size of business and range of products and services. The Internal Audit activities form the third line of defense which supervise whether the first and the second lines of defense reach the risk management and control targets.

The procedures and principles regarding risk management, monitoring and control, internal audit and training activities mentioned in the Policy and all measures and operating rules determined with this scope are arranged within the Implementation Directive on AML/CFT of our Bank.

Within the scope of Bank Policy the matters related to rules and procedures are specified in the AML/CTF Directive.

In defining the AML/CTF procedures, the assignment and authorisation shall be made in such a manner that the staff responsible for monitoring, controlling and supervising the transactions and workflow within the Bank according to risks is not the same staff as those responsible for carrying out the transaction.

It is compulsory that the Bank notify the AML/CTF policy to the related staff by taking their signatures.

The risk monitoring and evaluation results are regularly reported to the Board of Directors and the designated members of Board or a Committee who have the authorization delegated by the Board of Directors.

Our Bank’s Compliance Policy and Procedures, within the scope of regulation updates or from the risk-based approached perspective, are reviewed at least once a year and presented to the Board of Directors.

RISK MANAGEMENT

Risk management includes in-house measures and operational rules. In line with the AML/CTF legislations and international standards relating to “**Know Your Customer**”, customer acceptance policy was created to ensure compliance with the principles.

Customer Identification and Verification: Bank takes all precautions in order to know its real person and legal entity customers in terms of social, financial and identity information, and for that purpose, to obtain all kinds of documents, particularly those relating to identification, and to confirm the authenticity of such documents. Obtaining essential documents from the customers who has a permanent business relationship with our Bank is not considered as sufficient. Customers are monitored depending on their risk degrees, their transactions are controlled and the alterations in their information are followed up.

- If identification or obtaining of sufficient information about the purpose of the business relation is not possible, the customer cannot be accepted and required transaction cannot be performed.
- In case of having suspicion about the sufficiency and accuracy of customers’ personal identity information and inability to make essential verification and confirmation, the customer relation shall be terminated.
- Customer accounts are opened for the real name-surname or title of the legal persons. Accounts cannot be opened by using other names, anonymous names or nicknames.
- Within the scope of the necessity that customer relationships should be based on mutual information exchange, trust and full disclosure, persons and legal entities, who avoid or are unwilling about filling in the customer

information forms or who provide deceptive, unconfirmable information, are not accepted as customers.

- The persons and legal entities listed in Sanctions Lists published by authorities accepted by the international community Such as Consolidated United Nations Security Council Sanctions List, SDN and Non-SDN Lists of The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury, The consolidated list of persons, groups and entities subject to EU financial sanctions, HM Treasury’s Consolidated List of Financial Sanctions Targets in the UK and/or Bank’s internal black list are not accepted as a customer and business relationship is not established.
- Customer name and surname (title for legal entities) titles are screened against the globally accepted PEPs Lists. In case a true match is identified, the necessary measures are taken against PEP customers.
- Unless clearly authorized with a valid documentation and purpose and nature of opening account is not understood, Third parties’ requests about opening accounts on behalf of one or more person cannot be accepted. (Excluding the accounts to be opened on behalf of persons or minors under guardianship or custody)
- If there is a strong suspicion that the persons or legal persons, with whom a business or customer relationship will be established did not gather their assets through legal means, or if there are information or documents certifying such a case, banking relationship with such natural or legal persons is not initiated, their guarantees or warranties are not accepted.
- The Bank cannot establish correspondent relationship with shell banks and financial institutions working with shell banks.
- The Bank cannot establish customer relationship with shell companies.
- The Bank should ensure that the correspondent relationship does not cover the use of payable-through account and nested-account activities.

Identifying of Beneficial Owner: Beneficial owner is defined as having ultimate control over the natural persons who conduct the transactions, or natural persons, legal person or unincorporated firms on whose behalf transactions are conducted. Bank is required to take necessary measures to disclose whether customer is acting on behalf of or on account of another person and to ascertain and identify the beneficial owner of the transaction accordingly.

With respect to customer acceptance process with legal entities, the Bank identifies the natural persons holding 10% or more of the shares of a legal entity for the purpose of the identification of beneficial owner requirements on legal entities.

In case any suspicion occurs that the identified person is not the beneficial owner of the legal entity holding 10% or more of the shares or there is no such beneficial owner holding 10% or more of shares, the necessary measures are taken to disclose the ultimate controlling person/s of the legal entity. In such case, identified person/s is/are accepted as the beneficial owner and, if any person cannot be identified, the highest level authorized person/s registered in the commercial registry is/are accepted as acting senior manager/s and the beneficial owner/s.

The necessary measures are taken in order to disclose natural person/s who ultimately control/s an unincorporated organization. In case a beneficial owner cannot be identified, the highest level authorized person/s registered in the commercial registry is/are accepted as acting senior manager/s and the beneficial owner/s.

Transactions require to be paid particular attention: The Bank pays particular attention to complex and extra ordinary transactions as well as transactions not having reasonable legal and economic grounds. The Bank also takes necessary measures to collect sufficient information about the reason of transaction requested and keep all information, data, documents and records regarding the transactions.

Taking appropriate measures against technological risks: The Bank pays particular attention to the risks arising from use of emerging technologies for ML/TF purposes and takes appropriate measures to avoid such risks. The Bank also pays special attention for use of systems enabling customers to conduct non face-to-face

transactions, monitors transactions which are not in accordance with customers' profile and their business activities and, takes appropriate and efficient measures including set specific thresholds and transaction limits.

Wire Transfers: The necessary measures are taken to mitigate the risks arising from electronic wire transfers which may enable risky funds relevant to ML/TF to be used in domestic or international payments.

In outgoing domestic and international wire transfers messages, the following information of originator is provided:

- Full name of originator
- Originator's account number or transactions reference
- At least one of the following information which helps to identify the originator: Address or place of birth or date of birth or customer number, national ID number or passport number or tax number etc.
- Full name of beneficiary and/or account number

In Cross-border wire transfers related to risky countries and customers, all essential information with details and supporting documents regarding nature and purpose of transaction are collected from the relevant parties.

Monitoring the Customer Profile and the Transactions: The Bank should follow up continuously the transactions conducted by their customers whether they are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds within the scope of permanent business relationships and keep up-to-date information, documents and records regarding the customer. If the purpose of establishing business relation with our Bank declared during the evaluation of customer acceptance period is not parallel with the transactions and activities of the customer, the customer relationship should be evaluated again.

The business relationship of existing customers is terminated if customer is listed in Sanctions Lists published by authorities accepted by the international community Such as Consolidated United Nations Security Council Sanctions List, SDN and Non-SDN Lists of The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury, The consolidated list of persons, groups and entities subject to EU financial sanctions, HM Treasury's Consolidated List of Financial Sanctions Targets in the UK and/or there is a suspicion, knowledge or document that the funds/assets of customers have not been obtained in legal way.

Whether the accounts are actually utilized by the account owner is monitored continuously.

Risk Areas and Grading: The objective of the risk management policy is, within scope of preventing laundering proceeds of crime and financing of terrorism, to define, grade, monitor, assess and reduce the possible risks the Bank may be exposed to.

In line with risk-based approach, four risk areas have been designated; customer, product/service, sector and country/region risk. On the basis of designated risk areas, our Bank classifies the customers, products, sectors and countries into below mentioned groups.

- Low Risk
- Medium Risk
- High Risk
- Very High Risk

The **customer risk** means that our bank is abused by the customer or the person acting on behalf of customer who is active in money laundering process or financing terrorism.

High risk customers:

- Charity corporations
- PEPs
- Non-resident persons and legal entities

Non-face to face products and services, cash transactions that is difficult to follow up, new products served with developing technologies involves **product and service risk** because these products have AML/CTF risk.

The products and services rated as high risk are listed below:

- (a) High-Value Cash Transactions
- (b) Wire Transfers
- (c) Correspondent Banking Transactions
- (d) Drawing of Tangible Checks from Foreign Banks
- (e) Alternative Distribution Channels
- (f) Safe Deposit Boxes
- (g) Risky Credit Transactions
- (h) Complex and Unusually Large Transactions

The **industry risk** that our Bank would be abused as a consequence of the fact that the customers working in business lines or sectors which conduct intense cash usage, purchase of high-value goods or international fund transfers.

The industries and business lines rated as high risk are listed below:

- (a) Fuel Stations
- (b) Antique Shops and Art Galleries
- (c) Brokers, Brokerage Service Provider Companies
- (d) Foreign Exchange Offices
- (e) Factoring Companies
- (f) Casinos/Nightclubs
- (g) Jewelers, Gold and Diamond Gemstone and Precious Mineral Traders
- (h) Parking Lot Companies
- (i) Payment and Electronic Money Companies
- (j) Travel Agencies, Passenger and Freight Carriers
- (k) Firms that Manufacture and Trade Weapons or Military Ammunition
- (l) Sports Clubs
- (m) Operators of Lottery Gaming Halls/Lottery Franchisees
- (n) Asset Management Companies
- (o) Companies Making Leveraged Trading (Fx/Forex)
- (p) Portfolio Management Companies (PMC)

Transactions realized on accounts managed as an agent by PMC in the scope of the portfolio management contract they enter into with retail/corporate customers do also bear additional risk.

In addition, those involved in the trade of dual-use items that carry the risk of being used in terrorist activities constitute an additional risk. Within the framework of the risk-based approach, additional measures are taken in order for customer acceptance, monitoring of activities and transactions.

The Bank may be exposed to **country risk** as a consequence of the customers or transactions in relation to residents or nationals of countries which do not implement FATF recommendations or which implement them

incompletely and which are located on illegal drug production–distribution routes, or where rates of crime, such as smuggling and terror, are high and fraud and bribery are common, which are anti-democratic, cross-border centres that constitute a centre of attraction for the needs of storage of funds which are obtained through organized crimes as a result of banking secrecy provided by local banks and other financial institutions, tax advantage and judicial immunity.

Countries/regions considered high risk:

- (a) Countries that do not implement or incompetently implement FATF recommendations, and so are not listed on the FATF Cooperation Countries List,
- (b) Countries subjected to sanctions/embargoes, etc. by the UN and other international authorities (such as EU, OFAC, HM Treasury).
- (c) Countries and regions in which smuggling, terrorism, crime, corruption and bribery are prevalent and those on drug production-distribution routes are called grey areas,
- (d) Tax havens/off-shore and free zones.

Simplified Measures: The customers/products/transactions specified in the MASAK General Communiqué no. 5, published in the Official Gazette, are considered as low risk customers/products/transactions after determining that they do not bear AML/CTF risk and can be taken simplified measures in terms of customer due diligence.

Enhanced Measures: Enhanced measures are applied to the customers/products/transactions which are considered as high risk customers/products/transactions in our Implementation Directive.

MONITORING AND CONTROL

Our main goals are protecting the Bank against AML/CTF risk and controlling whether the transactions comply with laws and applicable regulations as well as the Bank's policies and procedures.

Compliance Unit is responsible for monitoring and keeping the risk assessment up to date. Compliance Unit establishes a central monitoring and control system in order to detect the AML/CTF risks and suspicious transactions. The banking transactions, particularly the ones in the high risk category, are monitored as per the set criterias and scenarios.

Monitoring and controlling activities include, but are not limited to, the following topics:

- Monitoring and controlling customers and transactions in the high risk category
- Monitoring and controlling transactions conducted with risky countries
- Monitoring and controlling complex and extraordinary transactions
- Controlling, through sampling method, whether the transactions exceeding a pre-determined limit are in accordance with the customer profile
- Monitoring and controlling related transactions exceeding the limit that requires customer identification when handled together
- Controlling, completing and updating the information and documents about the customer which have to be kept in electronic or written form and the compulsory information which have to be included in electronic transfer messages
- Monitoring whether a transaction conducted by the customer is consistent with the information about the customer's business, risk profile and source of funds on a permanent basis throughout the term of the business relationship
- Controlling transactions conducted by using systems which enable non face-to-face transactions
- Risk-based control of newly introduced products and services which may be exposed to abuse due to

- technological developments
- Checking customers and transactions against sanctions lists

Compliance Department may claim all kinds of information and documents related to its field of duty from Bank's all units in the course of its evaluation process. The units claimed information and documents by Compliance Department are required to present the requested information and documents and provide convenience to Compliance Officer and Compliance Department.

In case of existence of any information, suspicion or an issue arousing suspicion regarding money and other assets that can be represented with money being involved in transactions executed or being attempted to be executed at our Bank or through our Bank, are obtained through illegal means or used for illegal purposes, or even though they are obtained through legal means, used by terrorist organizations and sponsors of terrorism or for terrorist activities or is related with terrorism by any means, **suspicious transaction report** about the person(s) who executed the transaction must be made to MASAK.

Information about the executed suspicious transaction reports is not to be disclosed to anybody (even the parties) except authorized inspection personnel and courts in case of a legal proceeding.

Our Bank and its staff fulfilling their liability to report suspicious transactions in accordance with Law No. 5549 shall not be held responsible legally and penally.

INTERNAL AUDIT

The purpose of internal audit is to give assurance to the Board of Directors on efficiency and adequacy of the whole Compliance Program. The Bank ensures that corporate policies and procedures are reviewed and inspected on annual basis by applying a risk-based approach in order to determine whether risk management, monitoring and control activities as well as training activities are adequate and effective, whether the risk policy is adequate and effective, and whether transactions are conducted in accordance with laws and applicable regulations, Bank policies and procedures.

The following activities are within the scope of internal audit activities:

- Defects, mistakes and abuses that are detected as a result of internal audit activities as well as opinions and recommendations to prevent their re-occurrence are reported to the Board of Directors
- Deficiencies detected in the course of monitoring and control studies, risky customers, services and transactions are included in the scope of the audit when determining it.
- While determining the units and transactions to be controlled, the business size and business volumes of the Bank shall be taken into consideration.

The activities within this context are executed by the Board of Inspectors. Internal audit results and the statistics are reported to MASAK on annual basis.

TRAINING

The purpose of the Bank's training policy regarding AML/CTF is to ensure compliance with the laws and applicable regulations based on laws, establishment of a corporate culture by elevating the consciousness of responsibility of the personnel with respect to the Bank's policies, procedures and risk-based approaches and updating the employees' knowledge.

The training activities related to the prevention of money laundering and financing of terrorism will be carried out

in accordance with the size, business volume and variable conditions of the Bank.

Training programs aimed at AML/CTF are prepared by the Compliance Officer in co-operation with the Training Department. The training program is conducted efficiently under supervision and coordination of the Compliance Officer.

All newly hired staff receive AML/CTF training by the specialized personnel on compliance of the institution within a maximum of 6 months of the date of their entry into employment. Training is repeated at certain intervals to include changes in legislation and updates of information. Training activities are repeated on regular basis depending on the size of the institution and the size of business. Training activities are compatible with changing conditions and contain updates and changes of regulations and standards. The period of training activities also depends on the results of assessment and evaluation in AML/CTF trainings. Some trainings methods like the distance trainings are used besides organizing seminars and panels for conducting training activities and, the training result are recorded.

The Compliance Department and the Training Department determine a sufficient number of trainers on this issue and ensure that they attain required knowledge and proficiency. Trainers are chosen among the trainers who attended MASAK education programs. The training process is repeated at certain intervals so as to include the legislation changes.

Compliance Officer, staff of Compliance Department and members of training team are ensured participation to national and international trainings and seminars on the purpose of professional specializing of Compliance Officer, staff of Compliance Department and members of training team.

Information and statistics related to training programs are reported to MASAK on annual basis.

Training programs to be provided by the Bank to its personnel include, but is not limited to, the following subjects:

- Concepts of money laundering and terrorist financing
- Steps and methods of money laundering and case studies about the subject
- Legislation on AML/CTF
- Risk areas
- Corporate policy and procedures
- International regulations on AML/CTF
- Know your customer procedures
- Suspicious transaction reporting procedures
- Liabilities regarding maintaining and submitting records
- Liabilities regarding submitting information and documents
- Penalties to be applied in case of violation

MISCELLANEOUS

In accordance with Law No. 5549 article no.6 (periodical reporting); the transactions which our Bank participates in or mediates, exceeding the specified amount shall be reported to MASAK.

In accordance with Law No. 5549 article no.7 (providing information and documents); in case MASAK or authorised inspection personnel request, these documents and, in cases when necessary, the passwords, allowing for access to the information on our Bank's system, are provided.

Relating to AML/CTF, the documents received and prepared, starting from the preparation date, books and records, starting from the last record date, documents relating to identification, starting from the last transaction date, documents relating to accounts, starting from the closing date of the account, are preserved for 10 years.

CORPORATE LEGAL COMPLIANCE

“Compliance Controls” mentioned in Article 18 of the Regulation on the Internal Systems of Banks issued by BRSA are performed by the Compliance Department.

In terms of the above referred Regulation, the provisions are cited as follows:

“...Compliance Controls,

Compliance controls are intended to ensure that all activities which the bank carries out or plans to carry out, and new transactions and products, are in compliance with the Law and other applicable legislation, with the internal policies and rules of the bank, and with banking practices. It shall be ensured that bank personnel are promptly informed of any changes to the Law and other applicable legislation or to the internal policies and rules of the bank.

Uninterrupted compliance control shall be performed by the internal control unit or by a unit to be assigned the duty of compliance control which shall operate under the same internal systems officer as the internal control unit and which shall be organized independently of the other activities of the bank.

Before authorization is sought from the board of directors for new products and transactions or activities planned to be carried out, an opinion shall be received from the unit assigned under the second paragraph above.

In foreign branches of the bank and in its partnerships subject to consolidation, at least one member of personnel each shall be assigned to control compliance under the regulations abroad and to make reporting to the unit assigned the duty of compliance control under the second paragraph above.”

Within the scope of Internal Systems Regulations, the Activity Report is presented to our Bank by the responsible personnel in charge of legal compliance in our domestic and foreign subsidiaries as well as foreign branches and, the coordination regarding this reporting line between the branches and subsidiaries and our Bank is organized.

The activities related to Corporate Legal Compliance are; to follow-up the national regulations, to inform the relevant departments and personnel regarding national regulations update, to control the new activities, transactions and products offered or planned to offer by the Bank, whether they are complied with national regulations, Bank’s internal policies and procedures, and banking conventions based on the Internal Systems legislation.

COMPLIANCE PROCESS AND RESPONSIBILITIES

Turkiye Halk Bankasi A.S. and all its domestic and foreign branches,

- constitute the necessary policies and procedures covering requirements with respect to AML/CFT by taking into consideration the Group Compliance Policy.
- conduct all business and transactions in line with the regulations.
- conduct their internal policies and procedures in line with the international requirements, the national legislations subject to, the Group Compliance Policy and Bank's Compliance Policy.

Turkiye Halk Bankasi A.S set the confidential reporting line to enable its employees to notify deviant issues required to be reported in line with "Ethic Principles" and "Anti-Corruption Policy" accepted by the Board of Directors. Furthermore, Bank takes necessary measures to protect the employees making this notifications and regarding the confidentiality of the whistleblower.

The reports regarding the issues within the scope of the Group Compliance Policy and Bank's Compliance Policy, are escalated to the Audit Committee in quarterly basis to and to the Board of Directors at least annually.

H. ENFORCEMENT

Bank Compliance Policy Directive, Halkbank of Turkey Accepted by Resolution No. 32 of the Board of Directors dated 02/05/2018, and entering into force on the date of approval by the Board of Directors.

The provision of Bank Compliance Policy Directive are conducted by the Compliance Department on behalf of the Board of Directors.

As the entry into force of this Bank Compliance Policy Directive, the previous one Accepted by Resolution No. 7 of the Board of Directors dated 26/12/2017 has been repealed.