



# **TURKIYE HALK BANKASI A.S.**

**GROUP COMPLIANCE POLICY DIRECTIVE ON  
ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM**

## TABLE OF CONTENTS

<b>A. DEFINITIONS AND ABBREVIATIONS.....</b>	<b>3</b>
<b>B. GOAL.....</b>	<b>5</b>
<b>C. SCOPE.....</b>	<b>6</b>
<b>D. LEGAL FRAMEWORK.....</b>	<b>6</b>
<b>E. GROUP COMPLIANCE PROCESS AND RESPONSIBILITIES .....</b>	<b>7</b>
<b>F. COMPLIANCE PROGRAM.....</b>	<b>8</b>
<i>a. Risk Management and Risk Based Approach.....</i>	<i>8</i>
<i>b. Know Your Customer, Customer Acceptance Policy and Customer Due Diligence (CDD-/Enhanced Due Diligence-EDD) Processes.....</i>	<i>13</i>
<i>c. Monitoring and Control .....</i>	<i>15</i>
<i>d. Notification of Suspicious Transactions and Reporting .....</i>	<i>16</i>
<i>e. Keeping Records.....</i>	<i>17</i>
<i>f. Internal Audit .....</i>	<i>17</i>
<i>g. Training .....</i>	<i>17</i>
<i>h. Compliance with Economic and Financial Sanctions .....</i>	<i>18</i>
<i>i. Correspondent Banking .....</i>	<i>18</i>
<b>G. LEGISLATION COMPLIANCE.....</b>	<b>19</b>
<b>H. ENFORCEMENT .....</b>	<b>20</b>

## TURKIYE HALK BANKASI A.S.

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

Turkiye Halk Bankasi A.S. (Head Office Units of the Parent Bank, domestic and foreign branches, other service units) and all domestic and foreign Subsidiaries (hereinafter referred to as "the Group") attach great importance to the fight against Money Laundering (ML), Financing of Terrorism (FT), Proliferation of Weapons of Mass Destruction (WMD) and Bribing Foreign Officials, and aim to ensure full compliance with all national and international laws and other legal regulations within the scope of Sanctions Programs.

#### A. 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 Turkiye 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 AML/CFT.
- ◆ **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.
  - ◆ **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)
  - ◆ **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.
  - ◆ **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 application of global standards to combat AML/CFT 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.

## B. GOAL

The Group Compliance Policy directs the activities of Halkbank of Turkey and its subsidiaries subject to consolidation in accordance with legal regulations. It ensures the establishment of a Group-wide policy within the scope of the Compliance with AML/CTF, WMD and Sanctions on the Prevention of Bribery of Foreign Public Officials.

The standards set out in this policy include the minimum obligations stipulated in the applicable legislation of the country to which affiliated partnerships in the Group are subject, and aims to protect the Group, and its employees and customers from the risks associated with AML/CFT and bribery/fraud.

The Group Compliance Policy aims:

- To protect Group's national and international reputation by ensuring compliance with legal obligations relating to AML/CFT,
- To ensure that strategies are developed to reduce exposure to risks by evaluating customers, transactions and services with a risk-based approach,

- To identify the controls and measures, working rules and responsibilities within the Group and to raise awareness accordingly.

### **C. SCOPE**

The Group Compliance Policy on AML/CTF covers Halkbank of Turkey (Headquarter Units, all domestic and international branches and other service units) and all domestic and foreign Subsidiaries. All activities of foreign subsidiaries and branches are carried out in accordance with the legislation of the resident country. The Group Compliance Policy sets a common standard for the policies, procedures and control criteria that are to be specified in writing by the Bank and its subsidiaries in accordance with compliance legislation. Subsidiaries are responsible for the enforcement of this policy in the context of the legal obligations in their operational area.

The Department of Compliance of Halkbank Turkey is responsible for the control and monitoring of the implementation of the Group Compliance Policy in the Main Partnership Bank and in its affiliated partnerships subject to consolidation.

### **D. LEGAL FRAMEWORK**

The recommendations published by the FATF support of the development of national legal systems ensure legislative alignment, strengthen the role of the financial system and establish a continuous line of cooperation among the member states in the fight against ML/FT, and are binding within the member states.

The legal basis of the Group Compliance Policy on AML/CFT, established based on the FATF recommendations, constitutes the laws and regulations on AML/CFT of the country of operation. Along with the FATF recommendations and national regulations on AML/CFT, the group also considers the recommendations, principles, standards and regulations adopted by international regulatory bodies and national authorities (such as the UN, BCBS, Wolfsberg Group, EU, OFAC, HM Treasury), unless they are in conflict with national regulations.

The Group also takes steps to comply with:

- Rules and procedures established for the implementation of decisions on combating terrorism and the financing of terrorism of the International Agreement on the Prevention of Financing of Terrorism, dated 1999, and by the United Nations Security Council, freezing assets so that the financing of terrorism is prevented and regulate the offense of the financing of terrorism.
- The provisions of the "United Nations Convention Against Corruption, the Council of Europe "Criminal Law Convention on Corruption" and the OECD "Convention on Combating Bribery of Foreign Public Officials in International Business Transactions" in terms of bribing the Foreign Public Officials.

### **E. GROUP COMPLIANCE PROCESS AND RESPONSIBILITIES**

Halkbank of Turkey and all its domestic and foreign Subsidiaries:

- Develop policies and procedures that take into account national and international regulations on AML/CFT, considering also the Group Compliance Policy.
- Perform all activities and transactions in compliance with the Group Compliance Policy, provided that they are not contrary to the legislation of the country of operation.
- Apply their internal policies and procedures according to the legislation of the country of operation, international obligations, all relevant legal legislation and the provisions of the Group Compliance Policy.
- In the event of a partial or complete contravention of the legislation of the country of operation in implementation of the Group Compliance Policy, Halkbank of Turkey takes the required measures in line with the common opinion after evaluation with the Compliance Department.

All employees within the Group are responsible for the implementation of the Group Compliance Policy, as well as all internal policies and procedures. Group Compliance Policy is notified to all employees by taking signatures. Managers and officials responsible for compliance with the Group Compliance Policy are obliged to take the necessary measures in this regard.

All Subsidiaries are to establish procedures that are in compliance with the "Ethical Principles" and "Policy on Combating with Corruption" adopted by the Board of Directors of Halkbank of Turkey, and to establish proper channels for the reporting of controversial situations. In addition, it is also ensured that measures are

taken to protect employees who report wrong-doing and to ensure privacy of their reporting (whistle-blowing).

Subsidiaries report regularly to the Compliance Department of Halkbank of Turkey on compliance processes, as much as the legislation of the country of operation allows.

Those responsible for implementing the Group Compliance Policy in the institutions in the Group, have the authority to make decision and making evaluations and have the authority to make decisions as per their responsibilities. Communication and information sharing activities carried out with the Compliance Department of the Halkbank of Turkey is not preventing this decision making process in terms of the implementation of the Group Compliance Policy.

Regarding compliance with legal legislation, all Subsidiaries within the Group monitor regularly the legislation of the country of operation and the procedures published by regulatory agencies, and take steps to ensure compliance with these regulations. Reports are made to the Compliance Department of Halkbank of Turkey in a timely manner in the event of problems that may arise related to compliance with the legal regulations.

Information and documents requested by domestic and foreign legal authorities/regulatory agencies for the purpose of auditing and control within the Group are provided in coordination with the related units within the time limit.

The Compliance Department of Halkbank of Turkey reports to the Audit Committee of Halkbank of Turkey on matters within the scope of the Group Compliance Policy. In addition, the Compliance Officers of Subsidiaries inform the Board Member/committee to which they report on matters related to compliance with the Group Compliance Policy.

Responsible for the control and monitoring of the Group Compliance Policy, the Compliance Department of Halkbank of Turkey evaluates the efficiency of works carried out under the Group Compliance procedures. In line with a plan to be determined on an annual basis for control and consultation, the Compliance Department performs joint works/on-site visits with the units responsible for the compliance activities when necessary.

## **F. COMPLIANCE PROGRAM**

The Principles of the Group Compliance Policy include measures related to AML/CFT for the purpose of ensuring compliance with national legislation and international standards, and are the basis of both Halkbank of Turkey and its Subsidiaries.

The Group-wide Compliance Program includes the following basic measures.

- In the framework of AML/CFT legislation of the country of operation, the assignment of a compliance officer, the establishment of written policies and procedures according to the Group Compliance Policy, and the announcement of such policies and procedures to the staff,
- The carrying out of risk management activities to identify, grade, monitor, evaluate and lower the risk of exposure as part of AML/CFT activities,
- Depending on the size, volume of business and the scope of the services of the organization within the group, performing risk-based monitoring and control activities, and establishing a compliance unit,
- Training staff within the scope of the legislation on AML/CFT,
- Carrying out of internal audits into the implementation of the policies and procedures related to AML/CFT established under the compliance program.

The elements related to the basic framework of the Compliance Program are stated below.

### **a. Risk Management and Risk Based Approach**

Risk management aims to identify, grade, evaluate and mitigate the risks associated with AML/CFT to which the Group may be exposed within the framework of the risk-based approach. The Group-wide risk-based approach is used to ensure that measures to prevent or mitigate AML/CFT are proportional to the identified risks.

Risk-based monitoring and control activities are carried out considering the size, business volume and services of the organization within the group.

Risk management, monitoring and control activities are carried out by the Compliance Officer/Compliance Unit. Training activities are conducted under supervision and coordination of Compliance Officer.

The written procedures and documents of the organization within the Group include all rules identified within the scope of the Group Policy, provided that they are not in contradiction with the legislation of the country of operation.

Risk management includes internal rules and procedures for knowing the customer. In this context, all organizations within the Group form the necessary control points for the identification and determination of the real beneficiary, the monitoring of the status and transactions of the customers, the identification of areas of risk and risk grading, and the implementation the proper measures in such risk areas.

**Risk Areas and Grading:** The basic objective of the risk management policy within the scope of AML/CFT, is to identify, grade, evaluate and mitigate against risks associated with AML/CFT to which the Group may be exposed to.

The Group retrospectively examine the consistency and efficiency of risk identification, evaluation, rating and classification methods upon case studies or actual transactions executed and, re-evaluate and update the methods according to conclusion and improving conditions; and besides, regularly report the results of risk monitoring and assessment to the Board of Directors.

Four risk areas have been identified within the framework of the risk-based approach:

- Customer Risk
- Product/Service Risk
- Sector Risk
- Country/Geography Risk

The Group assesses customers, products, sectors and countries within the scope of its activities based on risk areas, assesses them with risk perception and classifies them as follows:

- Low-Level Risk
- Medium-Level Risk,
- High-Level Risk
- Very High-Level Risk

**Customer Risk:** It refers to the risk of abuse by the customer of the institutions of the Group due to the AML/CFT activities of the customer and those acting on behalf of the customer.

The customer types rated as high risk include, but are not limited to, the following:

- (a) Customers who conduct business relationships or transactions in an unusual way,
- (b) Legal person customers, where it is difficult to determine who owns or whose income he or she controls,
- (c) Charities and other non-profit organizations.

*(It is stressed in FATF recommendations that voluntary relief and charitable organizations [nonprofit-relief organizations] are vulnerable to abuse, especially in terms of the financing of terrorism. They constitute an AML/CFT risk as "they are able to benefit from the public resources, have access to large financial resources, control dense cash flow, allow global structuring, and are easy to establish").*

- (d) Gatekeepers
- (e) Mediators that are not subject to adequate AML/CFT controls, and that are not adequately audited.
- (f) Trusts, payment organizations, electronic money institutions, exchange offices and other persons or organizations providing money or asset transfer services,
- (g) Politically exposed persons (PEPs)

*It is assumed that politically exposed persons constitute an AML/CFT risk (support for illegal activities, corruption, bribery, improper use of public resources, etc.) due to their ability to access and/or control public resources. In addition to implementing the usual measures for the recognition of the customer, as detailed in the FATF recommendations on politically exposed persons (whether customer or real beneficiary), strengthened procedures should be applied to determine whether the customer or the beneficiary is a politically exposed person, to determine the source of funds and assets of foreign politically exposed persons and to constantly monitor the business relationship in a strict manner.*

- (h) Non-resident foreign persons and legal entities.



**Product/Service Risk:** Non-face-to-face transactions involve risks related to new products, products and services to be presented using cash-based, difficult-to-follow transactions and evolving technologies.

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

- (a) Services identified as potentially high risk by the authorities or by reliable sources
- (b) Banknote and precious metal trading and distribution services
- (c) High-Value Cash Transactions
- (d) Wire Transfers
- (e) Correspondent Banking Transactions
- (f) Drawing of Tangible Checks from Foreign Banks
- (g) Alternative Distribution Channels
- (h) Safe Deposit Boxes
- (i) Risky Credit Transactions
- (j) Complex and Unusually Large Transactions

Policies and procedures are established for non-face-to-face transactions, and these are implemented while a new relationship is being established, and for those still continuing Group-wide. In this context, **transactions through alternative distribution channels (ATM, Internet, dialog, mobile banking, etc.)** are classified as high risk, and so restrictions on services/transaction channels and special measures shall be implemented.

The awareness is raised regarding the abuse of such services provided by the institution within the group in terms of AML/CFT activities.

The Group pays attention to ML/FT risk enabling hiding of the identity details and measures arising from new and emerging technologies and takes necessary measures to prevent these technologies from being used for ML/FT purposes.

**Industry Risk:** Some industries and business lines include high AML/CFT risk arising from the high levels of cash usage, the ease of hiding financial sources and the difficulty in following the real objective of the activity and, customers engaged in such type of high-risk industries and business lines constitute the industry risk.

The sectors 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 and the product lists (EU, UK, US, etc.) created by international authorities are taken as references when determining risks involving transactions.

**Country/Geographical Risk:** Country risk refers to customer and transactions (who/which are by means of nationality, country of birth, jurisdiction of establishment, shareholder structure, authorized persons, transaction parties, etc.) linked to:

- Jurisdictions which do not have adequate regulation on the prevention of laundering and terrorism financing,
- Jurisdictions which do not cooperate adequately and which are considered as risky jurisdictions by the competent international organizations,
- Jurisdictions on drug production-distribution routes,
- Jurisdictions in which the crimes such as smuggling, terrorism, corruption and bribery are common,
- Jurisdictions accepted as tax-havens and offshore centers

Countries/regions considered high risk:

- (a) Countries that do not implement or incompetently implement FATF recommendations, and so do not appear 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 common and those on drug production-distribution routes are called gray areas,
- (d) Tax havens/off-shore and free zones.

#### **b. Know Your Customer, Customer Acceptance Policy and Customer Due Diligence (CDD-/Enhanced Due Diligence-EDD) Processes**

A customer acceptance policy has been established in order to comply with the "**Know your Customer**" principle included in national and international regulations, as part of AML/CFT efforts within the Group. The customer acceptance policy includes standard and enhanced customer acceptance and evaluation processes, including customer identification and verification (identification and verification, as stated in legislation, applying also to legal representatives and/or real beneficiaries), Know Your Customer principles and a re-evaluation of existing customers.

This principle is applied to protect the national and international reputation of the Group.

**Identification and Verification:** In terms of social, financial and personal information, the group takes all necessary measures to know real and legal person customers for which the group conducts transactions, to obtain all kinds of documents, especially regarding identity information, and to confirm their accuracy. Obtaining the relevant documents from the customers once is not considered enough even if a continuous business relationship is established. Customers are monitored based on their level of risk, during which their operations are checked and prospective changes are tracked.

Turkiye Halk Bankası A.S. and all domestic and foreign subsidiaries apply the identification and verification requirements by national legislation at minimum in line with the Group Compliance Policy.

Along with confirmation of identification, getting to know the customer involves obtaining information on the purpose of establishing a business relationship, identifying who is the real beneficiary and whether the transactions carried out by the customer are consistent with the financial and professional information provided the customer.

- In situations in which identity cannot be established or insufficient information about the purpose of the business relationship can be obtained, customer acceptance cannot be achieved and the requested operation cannot be carried out.
- The customer relationship is terminated in the event of doubt regarding the adequacy and authenticity of the previously obtained customer credentials, and in cases where the necessary identification and verification cannot be made.
- Customer accounts are opened under the real name-surname or title of the customer. Customer acceptance cannot be made using another name, an anonymous name or a nickname.
- Customers and organizations that refrain from filling out introductory information forms or who provide misleading or unverifiable information are not considered as customers, based on the need in a customer relationship to rely on mutual information exchange, trust and openness.
- The names of our individual/legal entity customers are screened against PEPs lists accepted by international community. In case a true match occurs the necessary measures are taken for the customer flagged as a PEP.
- Customers and transactions are checked against United Nations (UN), European Union (EU), United Kingdom (HMT), US (OFAC) and local sanction lists. It is not possible to establish a customer relationship with individuals or organizations that are registered on internal risk alert lists, or objectionable persons/organizations lists published by international authorities.

- Requests to open accounts cannot be carried out on behalf of one or more third parties (except for those to be opened in custodial and guardianship situations or for minors), unless the customer is clearly certified as legally authorized and the purpose and need to open an account is explained.
- If there is a strong suspicion, information or documentation that the assets of the persons or organizations initiating a business or customer relationship have not been obtained via legal means, they are not accepted as a customer, and no guarantees or warrants will be accepted.
- Banking relationships are not established with shell banks, or to other banks offering services to shell banks.
- No customer relationship is established with shell companies.
- It is ensured that correspondent banking services for the banks within the Group do not cover use of payable-through account and nested-account activities.

**Identifying the Beneficial Owner:** Actual persons performing transactions with the Group and natural persons or legal entities whose ultimate influence over the accounts or transactions that have ultimate control over non- natural persons, legal entities or non-legal entities that are traded on behalf of the group are defined as real beneficiaries. The group takes the necessary steps to determine whether someone else is acting on behalf of (in the name of) others, and to reveal and identify the actual beneficiary of the transaction.

With respect to customer acceptance process with legal entities, the Group identifies beneficial owners holding 10% or more of the shares of a legal entity for identification 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 Group pays particular attention to complex and extra ordinary transactions as well as transactions not having reasonable legal and economic grounds. The Group 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 Group 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 Group 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.

**Simplified Measures (Reduced Customer Due Diligence - CDD):** As a general rule, all customers are subject to the Group's Know Your Customer policies and customer acceptance procedures (CDD) including beneficial owner identifying responsibilities. There are also cases in which the AML/CFT risk is rather lower, and where information about the identity of the customer and the beneficiaries is clearly available, and cases in which adequate controls and inspections can be carried out through national/international systems. In such

cases, simplified or reduced customer acceptance procedures (CDD) may be allowed across the group to identify and verify the identity of the customer and the actual beneficiary.

The Group can also apply related simplified measures only to customers in its own country, or those in other countries that have effectively implemented the FATF Recommendations and which are regarded as having adequately fulfilled terms of the compliance with such recommendations. Simplified customer acceptance procedures (CDD) do not apply in AML/CFT or high-risk situations.

According to documents included in the FATF guide to the risk-based approach, simplified measures may include the following:

- With respect to identification, establishing a more simple process for the obtaining of such information as the customer's profession and address, and/or creating a more basic verification process with the purpose of establishing a business relationship through identity verification
- Suspending the verification of customer identification

**Enhanced Due Diligence (EDD):** The group implements strengthened customer acceptance procedures to mitigate risk in areas identified as high risk following a risk assessment. As defined in the FATF guide to the risk-based approach, strengthened measures may include the following:

- Acquiring additional information from various reliable sources for identification, and using this information in customer risk assessments
- Additional researches, such as a verifiable media survey, in terms of knowing the customer during customer risk assessment
- Compiling a review/evaluation report to allow a better understanding of the risks of being linked to ML/FT of customers and real beneficiaries.
- Confirmation of the source of funds and assets in the form of satisfactory evidence that funds and assets related to the business are not sourced through illegal activities
- Receiving high-level approval in order to initiate or to maintain a relationship

### **c. Monitoring and Control**

In order to ensure that the Group is protected from AML/CFT risks, it is essential that transactions and activities are monitored continuously in accordance with domestic and foreign legal regulations, policies and procedures.

It is the responsibility of the Compliance Officer/Compliance Unit of each organization within the Group to monitor this and to ensure that the risk assessment procedures are up-to-date. The central monitoring and control system established to detect AML/CFT risks and suspicious transactions allows the monitoring of establishment activities, and especially high-risk customers and transactions, in line with the determined criteria/scenarios.

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

- 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

**Monitoring the Customer Profile and Transactions:** Transactions carried out by customers within the scope of a continuous business relationship are subject to constant control to ensure that they are in

compliance with the profession, business activities, business history, financial situation and funding sources of the customer. Information, documents and records related to customers are kept up to date.

The customer relationship is reconsidered if anything realized that is not convenient with; the declared purpose of business relationship on the customer acceptance process and transactions that are not convenient with the profile of the customer.

The customer relationship is re-evaluated when the purpose of establishing the declared business relationship at the time of customer acceptance changes, and transactions that are not in accordance with the customer profile are made.

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.

Opened accounts are monitored constantly to control whether they are used by the actual account holder. The necessary measures are also taken to monitor transactions conducted by non-account holders with risk based approach and appropriate risk management system is constituted.

In addition, taking into account the levels of risk set out by the customers in relation to the profession/sector, nationality and the countries in which they operate, their transaction profiles and the persons/organizations with which they do business, and the products and services they use, monitoring and control activities are carried out with the intention of minimizing the risks to which the Group is exposed.

When the process of AML/CFT has been determined, duties and authorizations are assigned, ensuring that the personnel employed in the monitoring, control and supervision of the transactions and work flows in line with the risks are not the personnel performing the same operations at the same time.

#### **d. Notification of Suspicious Transactions and Reporting**

A suspicious transaction notification is made if values that can be represented by money, and money used in transactions made or attempted to be made through the group entities, are found to be:

- Obtained from illegal means or used for illegal purposes,
- Even if obtained from legal sources, if there is a suspicion that it is being used for terrorist organizations or by terrorist financiers, or for terrorist acts, or in any way connected to terrorism, the issuer of the transaction (Bank) shall make a suspicious transaction report to the relevant authorities.

Within the framework of the regulations safeguarding the confidentiality of suspicious transaction notifications made by Group employees and protecting the notifying party, information cannot be given to any person except the relevant legal authorities in the event of a suspicious transaction notification. In the framework of these regulations, the organization and personnel who made the suspicious transaction notification cannot be held responsible in legal and criminal terms.

The issues and activities covered by AML/CFT are reported to the Board of Directors t at least once a year.

#### **e. Keeping Records**

All obtained records (related to customers and transactions) are stored in a manner that is consistent with the regulations of the country subject to the legislation, and in accordance with the Know Your Customer measures and FATF Recommendation 11 , in order to any information requests from the competent authorities.

#### **f. Internal Audit**

An Internal Audit is an examination and audit of AML/CFT policy, and the Know Your Customer and acceptance procedures, taking a risk-based approach that is in compliance with regulatory requirements. The aim of an internal audit is to assure the Group management of the effectiveness and competence of the Compliance Program as a whole.

An annual risk-based approach is taken to the examination and auditing of whether the internal audit activity and Group-wide policies and procedures, risk management, training activities, monitoring and control activities are adequate and efficient, as well as the adequacy and effectiveness of the risk policy; and whether transactions are carried out in accordance with the policies and procedures established by the Law, as well as other regulations issued pursuant to the Law.

As part 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.

Activities in this context are carried out by the relevant auditing units.

#### **g. Training**

The objective of the training program on Group AML/CFT Compliance Policy is to ensure compliance with legal obligations, to create a corporate culture, to keep personnel updated, to increase the awareness of personnel across the Group, and to ensure the development of organization-specific policies, procedures and risk-based approaches.

Training activities aimed at disseminating the necessary knowledge for AML/CTF according to the requirements of the task, where all personnel are responsible for the Group, shall be carried out in accordance with the size, volume and changing conditions of the organization within the group.

Training programs for AML/CTF are prepared under the monitoring and coordination of the Compliance Officer/Compliance Unit.

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 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.

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.

The training to be given to the staff includes, but is not limited to:

- 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

#### **h. Compliance with Economic and Financial Sanctions**

The implementations on economic and financial sanctions include the following measures.

- Measures taken by countries or international organizations to prohibit or restrict financial transactions or relationships - **Financial Sanctions**
- Measures taken by States or international organizations in order to prohibit the export or import of goods or products - **Economic Sanctions**

The Group follows the globally implemented regulations and stipulated local sanctions applied by the United Nations (UN), the European Union (EU), the United Kingdom (HMT), the US (OFAC) and the country of operation, and takes the necessary steps to comply with such regulations.

#### **i. Correspondent Banking**

Correspondent Banking is a service offered by a bank (correspondent bank) to another bank (addressee) (international money transfer, check collection, etc.). Strengthened procedures are implemented in overseas correspondent banking and in similar banking relationships in order to mitigate such risks as the concealment of the real beneficiary, particularly in transactions within the group, as also stated in the FATF recommendations.

In the process of establishing correspondent banking business relations, the following measures are taken at minimum:

- Sufficient information and documents are obtained for the identification/verification of the financial institution.
- The information about the financial institution's prevention of money laundering and the Know Your Customer policies are gathered.
- Required controls are applied within the scope of the rule "no banking relationship is established with the shell banks or other banks offering services to shell banks".
- It is ensured that the correspondent relationship of the financial institution does not cover the use of Nested Account' Activities.

#### **G. LEGISLATION COMPLIANCE**

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.”

In this way, compliance with the laws and banking legislation of the country in which the banking operations are carried out abroad is paid regard. Any legal developments and correspondences published/sent by legal authorities and auditing firms are monitored regularly, and the Department of Compliance of Halkbank of Turkey reports at regular intervals on the compliance status and any actions to be taken for compliance. Legal developments for which compliance cannot be achieved within the stipulated period are reported as a non-compliance by the Department of Compliance of Halkbank of Turkey.

Relations with domestic and foreign legal authorities shall be conducted in accordance with the relevant legislation. Workflows and checkpoints are created to support due diligence so as to ensure the accurate, complete and timely communication of the required information, documentation and records by the legal authority for auditing and control purposes. Within this framework, the fulfilling of

information/documentation requests from legal authorities is the responsibility of the relevant units within the scope of the Group Compliance Policy.

## **H. ENFORCEMENT**

Group 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 entry into force, revision and enforcement of the Group Compliance Policy Directive is subject to the approval of the Board of Directors of Halkbank of Turkey.

In the partnerships subject to consolidation, the required approval process is carried out by the units responsible for the compliance when the implementation of the principles specified herein requires the approval of the Board of Directors of the affiliated partnership.