YAPI VE KREDİ BANKASI A.Ş.

CORPORATE POLICY ON PREVENTION OF LAUNDERING PROCEEDS OF CRIME AND FINANCING OF TERRORISM

YapıKredi

INDEX

1. INTRODUCTION

As known, this subject is regulated by Financial Action Task Force – FATF, established with the purpose of prevention of money laundering and financing of terrorism in the international arena and requirement for member countries to comply with the regulations and principles set out by FATF has been turned into an obligation. Our country is also a member of FATF and, in this context, compliance with international legal arrangements, preparation of regulations and performance of regulatory activities is entrusted to the Financial Crimes Investigation Board (MASAK), established as a board attached to the Ministry of Finance.

Yapı ve Kredi Bankası A.Ş., a pioneer in the banking sector in Turkey and acting with the sense of responsibility assumed by it due to its being the foremost private bank established in Turkey, displays sensitivity at highest level for full compliance with provisions of Law on Prevention of Money Laundering (hereinafter "Law") and related regulations regarding the implementation of that Law issued on 11.10.2006 by the Financial Crimes Investigation Board, taking into consideration at the same time financial repercussions of the matter and its effects on the community.

2. DEFINITIONS

Proceeds of Crime:
Proceeds of crime means assets originating from criminal activity.

Money Laundering Offence:
Money laundering offence means the offence defined in article 282 of the Turkish Criminal Code No. 5237 dated 26/09/2004.

Article 282 of the Turkish Criminal Code No.5237:
- Any person who takes away the assets acquired as a result of an offense which requires minimum six months or more punishment of imprisonment, or carries the same to a foreign country to be subject to various suspicious transaction in order to hide illegal source of these assets and to give the impression that they are acquired in the lawful manner, is punished with imprisonment from three years to seven years, and also imposed punitive fine up to twenty thousand days.

- A person who, without participating in the commitment of the offence mentioned in first paragraph, purchases, acquires, possesses or uses the proceeds which is the subject of that offence knowing the nature of the proceeds shall be sentenced to imprisonment from two years up to five years.

- Where this offence is committed by a public officer or professional person in the course of his duty then the penalty to be imposed shall be iincreased one half.

- Where this offence is conducted in the course of the activities of an organization established for the purpose of committing an offence, the penalty to be imposed shall be doubled.

- Where a legal entity is involved in the commission of this offence it shall be subject to security measures.

- In relation to the offences defined in this article, no penalty shall be imposed upon a person who directly enables the securing of financial assets, or who facilitates the securing of such assets, by informing the relevant authorities of the location of such before the commencement of a prosecution.

Financial Crimes Investigation Board (MASAK):
It is commissioned and authorized to combat laundering of proceeds of crime. It is directly attached to the Ministry of Finance.
Suspicious

Suspicious Transaction:
Suspicious transaction means presence of any findings, suspicions or grounds for suspicion in undertaken or attempted transactions with or through designated persons that the assets involved in the transaction were acquired illicitly or used for illicit purposes or were used for terrorist activities or terrrorist organizations or by terrorists or by persons financing terrorist activities or were associated with or related to the foregoing.

Designated Parties:
Designated parties mean those institutions designated as responsible for discharging the obligations (such as identification, suspicious transaction reporting etc.) set out as preventive measures to be taken for combating laundering proceeds of crime.

Compliance Officer:
It is the officer who is employed and given the necessary authority to ensure compliance with obligations set out in the Law and regulations that come into force in accordance with the Law.

Continuing Business Relationship:
It is the business relationship of a continuing nature between the Designated Parties and the customers established for providing services such as account opening, sanctioning credit facilities, issuing credit cards, allocating safe deposit boxes, financing, factoring, financial leasing services.

FATF:
Financial Action Task Force is an international organization established to combat money laundering and financing of terrorism. Turkey is also a member of this organization.

Compliance Program:
It is the entire body of measures referred to in article 5 of Regulation about Compliance Program Regarding Obligations Under Prevention of Laundering of Proceeds of Crime and Financing of terrorism.

Enhanced Approval Mechanism:
It is the higher echelon or Compliance Office approval.

Politically Exposed Person:
is a person who performs or has performed a prominent or senior public position, or a close family member of such a person or a close associate of such a person.

Beneficial Owner:
natural person(s) who ultimately control(s) or own(s) natural person who carry out a transaction within an obliged party, or the natural persons, legal persons or unincorporated organizations on whose behalf a transaction is being conducted within an obliged party.

Asset:
Asset means fund, proceeds, benefit and value derived from inter-conversion of them, owned or possessed or directly or indirectly controlled by a natural or legal person,

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.

Law no. 6415 on the Prevention of Financing of Terrorism
This Law herein, has been prepared within the scope of effective fight against terrorism and financing of terrorism for the purpose of determining the principles and procedures on 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 within the context of this Law, on establishing financing of terrorism offence, and on freezing of asset with the aim of preventing financing of terrorism.

Acts for which Providing or Collecting Funds are Forbidden
Article 3 – It is forbidden to provide or collect funds for perpetration of the following acts:

a) Acts intended to cause death or serious bodily injury for the purpose of intimidating or suppressing a population or compelling a government or an international organisation to do or to abstain from doing any act,
b) Acts set forth as terrorist offences within the scope of the Anti Terror Law No.3713 dated 12/04/1991,
c) Acts that are forbidden and stipulated as offence in;
1) Convention for the Suppression of Unlawful Seizure of Aircraft,
2) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
3) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents,
4) International Convention against the Taking of Hostages,
5) Convention on the Physical Protection of Nuclear Material,
6) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,

7) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
8) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf,
9) International Convention for the Suppression of Terrorist Bombings to which Turkey is a party.

The Offence of the Financing of Terrorism

Article 4 – (1) Any person who provides or collects funds for a terrorist or terrorist organisations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime within the scope of Article 3 shall be punished by imprisonment for a term of five to ten years, provided that his/her act does not constitute another offence requiring a heavier punishment.
(2) To impose a penalty in accordance with the provision of paragraph one, it shall not be necessary that the funds have actually been used to commit an offence.
(3) In cases where the offences that fall within the scope of this article are committed through undue influence in the public service, punishment to be imposed shall be increased by half.
(4) In cases where the offence is committed within the framework of a legal person's activity, security measures peculiar to legal persons shall be applied.
(5) In cases where the offence is committed against a foreign state or an international organization, investigation or prosecution shall be initiated upon the request of Ministry of Justice.
(6) Provisions of Law No.3713 regarding investigation, prosecution and enforcement shall also apply to this offence.

3. PURPOSE AND SCOPE

According to Regulations on Prevention of Laundering of Proceeds of Crime; the board of directors is ultimately responsible for implementation of the whole compliance program in an adequate and effective manner consistent with the extent and features of the activities of the Designated Party.

Within this scope, the Board of Directors is authorized and responsible for appointing a compliance officer, determining the duties and responsibilities of Compliance Officer and compliance department explicitly and in writing, approving the corporate policy, annual training program and amendments to them according to the developments, evaluating results of risk management, follow up and control and evaluation of results of internal audit activities, taking necessary preventive action for elimination on time of detected errors / deficiencies and ensuring the performance in an efficient and coordinated manner of all activities in the scope of compliance program.

The purpose of this corporate Policy is compliance with obligations relating to Prevention of Laundering of Proceeds of Crime and Financing of terrorism, determination of strategies to reduce contingent risk by evaluation of customers, transactions and services on a risk sensitive basis, determination of intra company controls and measures, operational rules and responsibilities as well as educating the employees of the company on these matters.

This Policy is implemented in the bank and its subsidiaries and in cases where legislation of the country where they operate permits, in its overseas branches and subsidiaries.

The bank also provides its subsidiaries and overseas branches, conducting policies and procedures within this context and proper execution of the conducted policies.

All activities to be performed and measures to be taken within the bank in the frame of this policy are determined by related procedures. Preparation of mentioned procedures, their amendment consistent with circumstances and their implementation are within the powers and responsibility of Compliance Officer. All Employees are responsible for complying with this Policy and procedures and all applicable laws and regulations in the performance of their duties. Failure to comply with or any breach of this Policy may give rise to disciplinary action against the relevant Employee in addition to the sanctions contained in the local laws and regulations. This Policy is notified to Bank employees against their signatures or other methods declared by MASAK. The updates in the Policy will be published in Bank's Intranet Portal and considered as notified.

4. RISK MANAGEMENT

The Bank and/or Bank employees face financial and/or reputational risk due to failure to fully comply with Law and regulations related to this Law or due to reasons such as benefiting from available services with the purpose of laundering proceeds of crime or financing of terrorism.

Taking into consideration the size of the Bank, business volume and nature of transactions performed, a risk management policy should be in place as part of the Corporate Policy, covering definition of contingent risks, their grading, monitoring, evaluation and reduction.

Consistency and effectiveness of risk identification, classification and grading methods are evaluated by considering the past transactions and incidents. Concluded results are reevaluated and updated according to developing conditions. In addition to this, results of risk monitoring and evaluation are regularly reported to Audit Committee and Board of Directors.

Risk management consists of customer risk, service risk and country risk.

4.1. Customer Risk

It includes the risk for obliged parties to be abused due to the business field of the customer allowing intensive cash flow, purchasing of valuable goods or international fund transfers to be carried out easily; and due to the acts of customer or those acting on behalf or for the benefit of the customer for money laundering or financing of terrorism purposes.

For the purpose of grading and reducing the aforementioned risks, individuals or entities with which continuing business relations should not be established as well as additional measures required to be taken are determined by adopting know your customer principles and customer risk profile within the frame of know your customer principle.

4.2. Know Your Customer Principles

Compliance with know your customer rules that have a very important place in FATF recommendations which are also adopted by our national legislation are of extreme importance for the bank.

Following matters are taken into consideration within that context.

4.2.1. Identification

Identification of customers and verification of the customer's identity within the scope of identification is made within the frame of the law and other regulations thereunder.

Related practice details and their amendments are determined by procedures, internal regulations and circulars published/will be published by Compliance and Internal Control Management/AML Department.

4.2.1.1. Profession, Industry and Business Line From which Income is Derived

Information is obtained both on the profession, operated industry and business line from which income is derived within the scope of know your customer principle.

4.2.1.2. Purpose of the Transaction and Source of the Funds

Sufficient information and documents should be provided and reasonably investigated in order to confirm sources of funds regarding the customer's transaction.

4.2.1.3. Business History

Information is obtained regarding the duration of the customer's activity in the stated business line.

4.2.1.4. Identifying the Beneficial Owner and Attaching Special Attention to Legal Persons

Necessary measures are adopted to determine whether the customer acts for account of others and to determine the identity of the real beneficiary of transaction. Necessary notices are displayed in branches where service is rendered to remind persons who act in their own name but for account of other people of their responsibilities in such a manner that customers may see the contents easily. In addition, at establishment of a continuing business relationship a statement in writing is taken from the customer wherein the customer declares if he is acting for account of other people. In case there are doubts that the customer acts in his/her own name but for account of another person despite the person declaring that he/she does not act for account of others, the bank makes a reasonable investigation to detect the real beneficiary.

In establishing permanent business relationship with legal persons registered to traderegistry, the natural person partners holding more than twenty-five percent of the legal person's shares as the beneficial owner have been identified. In cases where there is a suspicion that the natural person partner holding more than twenty-five percent of the legal person's shares is not the beneficial

owner or where there is no natural person holding a share at this rate, necessary measures shall be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. And natural person(s) detected shall be considered as beneficial owner. In cases where the beneficial owner is not detected, the natural person(s) holding the position of senior managing official, whose authorization to represent the legal person is/are registered to trade registry, has been considered as beneficial owner.

4.2.1.5. Information on Purpose and Intended Nature of a Continuing Business Relationship

Information is obtained on the purpose and intended nature of request, which products and services are planned to use and activity volume for the establishment of a continuing business relationship with the bank.

4.2.1.6. Location Where Activity is Performed

Information is obtained about the geographical location of the place where the activity for the stated business line is performed.

4.2.1.7. Customer Reputation

Customers and benificial owners are checked in the lists which are provided by reputable commercial organizations (such as Dow Jones or WorldCheck) in order to question involvement in known, alleged or suspected financial crime.

4.2.1.8. Reliance on Third Parties

Financial institutions may rely on measures taken by another financial institution relating to the customer for identification of the customer, of the person who acts on behalf of the customer or of real beneficiary and obtaining information for the purpose of establishing business relations or conducting transactions. In this case, the ultimate responsibility under the Law and regulations relating to the Law rests with the financial institution that conducts transactions by relying on the third party.
This principle is only applicable if the financial institution relying on the third party is satisfied that the third party has measures in place which shall ensure compliance with requirements of identification, maintenance of records and knowing the customer and in case third party is located in a foreign country, it is effectively regulated and supervised in the field of combating laundering and financing of terrorism, and certified copies of documents for identification will be made available by the third party without delay when requested.

The financial institution which establishes a business relationship or conducts a transaction by relying on a third party, shall immediately obtain the identity information of the customer from the third party.
The transactions performed between financial institutions on behalf of their customers, relationships between agents/similar units of financial institutions and third parties behave like the extension of main service unit of financial institutions are not within the scope of the principle of “reliance on third parties”. This principle could not be applied to the cases where the third party is resident in a high risk country.

4.2.2. Individuals and Entities for which Enhanced Measures should be Taken at Establishment of Business Relationship

4.2.2.1. Customer Transactions at Geographical Areas with High Risk Level or Areas Related Thereto;

Enhanced measures are taken to accept as customers individuals/entities that carry out activities in countries that do not cooperate with Financial Action Task Force (of which our country is also a member) or do not have adequate audit mechanisms or individuals/entities that have business relationship with individuals/entities carrying out activities in these countries and continuing business relationship is only established according to enhanced approval mechanism depending on information obtained as a result of reasonable investigation made from sources outside the bank.

4.2.2.2. Correspondent Banks at Geographical Areas with High Risk Level or Areas Related Thereto;

Enhanced measures are taken to accept as customers individuals/entities that carry out activities in countries outside the EU and countries that do not cooperate with Financial Action Task Force (of which our country is also a member) or do not have adequate audit mechanisms or individuals/entities that have business relationship with individuals/entities carrying out activities in these countries and continuing business relationship is only established according to enhanced approval mechanism depending on information obtained as a result of reasonable investigation made from sources outside the bank.

4.2.2.3. Free Zones and Finance Centers

Due care and diligence is exercised with respect to transactions with, free zones and other finance centres that have minimum or no regulatory or audit functions or with respect to customers that have relations with them, and business relationship is established according to enhanced approval mechanism

4.2.2.4. Politically Exposed Persons and/or PEP is a Relevant Beneficial Owner of a Client

It is determined whether the customer or beneficial owner is a politically exposed person, a reasonable investigation is made

to establish source of funds and wealth and decision to establish business relationship is made according to enhanced approval mechanism.

4.2.2.5. Sensitive Sector and Business Groups

Reasonable investigation is conducted about individuals or entities which deal in cash transactions intensely or who produce high amounts of cash on specific transactions despite cash disposals not being intense. Decision whether to have a business relation with these individuals or entities or not is made according to enhanced approval mechanism.

4.2.3. Individuals, Entities and Countries with Which Business Relationship shall not be Established

4.2.3.1. Individuals and Entities Included in Blacklists Issued by Competent Authorities Within the Scope of Prevention of Laundering of Proceeds of Crime and Financing of Terrorism Regulations

Business relationship is not established with individuals and entities appearing in blacklists issued by competent authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism regulations and none of their transactions are effected. In case it is determined that individuals or entities with which business relationship is established have connections with individuals or entities appearing in blacklists, related authorities should be notified.
Furthermore, termination of business relationship is also evaluated by Compliance and Internal Control Management/AML Department.

4.2.3.2. Countries Included in Blacklists Issued by Competent Authorities within the Scope of Prevention of Laundering of Proceeds of Crime and Financing of Terrorism Regulations

Transactions related with sanctioned countries which are given in the blacklists of the competent authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism regulations are not performed.

4.2.3.3. Shell Banks

Direct and indirect transactions and establishing business relationship with shell banks that have no physical presence, are not subjected to any audit and do not have in place adequate regulations on Prevention of Laundering of Proceeds of Crime and Financing of terrorism shall not be permitted.

4.2.3.4. Offshore Banks

Due care and diligence is exercised with respect to transactions with, offshore banks that have minimum or no regulatory or audit functions or with respect to customers that have relations with them, and business relationship is established according to enhanced approval mechanism

4.2.3.5. Anonymous Relationships

The Bank will not establish anonymous relationships nor establish relationships where the identity of the beneficial owner(s) of the customer, where relevant, cannot be established.

4.2.3.6. Individuals and Entities Declining to Provide Information or Documents

Transactions are not to be permitted of individuals or entities that decline to provide information and documents demanded during establishment of continuing business relationship and want to conduct transaction without providing the information and documents required for identification purposes.

4.2.3.7 Other Individuals and Entities with Which Business Relationship shall not be Established nor shall not be Intermediated Transactions

- Unregulated money remittance businesses
- Unregulated providers of digital/virtual currencies
- Individuals or entities where it is known that they are actively involved in criminal, corrupt or terrorist activities

4.3. Service Risk

4.3.1. Non – Face to Face Transactions

Contemporary technology allows non-face to face banking transactions to be realized. Transactions that are not face to face to be realized by the customer and third parties are allowed after submitting information and documents within the scope of identification requirements stated in the law and related regulations.

4.3.2. Correspondent Banking

During establishment of correspondent banking relation, publicly available information is gathered to determine whether the financial institution with which relation is to be established was subjected by competent authorities to a money laundering or financing of terrorism investigation, whether it was fined or not and whether supervision in its country is adequate or not. For this purpose, banks introduce specific customer acceptance rules, including but not limited to requesting from other financial institutions applying to open correspondent account in the bank, a survey form containing the above given information in writing, and implement specific work flows for which top executive's approval is required.

Sound information is obtained on whether regulatory environment in the country of financial institution with which correspondent banking relation is to be established is at adequate level and investigation is made to determine whether its system related to prevention of money laundering is adequate. An agreement where responsibilities and obligations are set out is made between the bank and the respondent financial institution.

Related practice details and their amendments are determined by procedures, internal regulations and circulars published/will be published by Compliance and Internal Control Management/AML Department.

4.3.3. New Products and Current Products that are Restructured as a Result of Developing Technologies

Whether new services to be rendered and current products that are restructured as a result of continuously developing technologies are in compliance with the law or not is controlled and application is monitored and stopped when necessary.

4.4. Country Risk

Countries that do not have adequate regulations for prevention of money laundering and financing of terrorism, do not adequately cooperate for the fight against these crimes or countries that are accepted as risky by authorized international organizations constitute country risk. Special attention is paid to transactions of individuals/entities conducting activities in these countries and individuals/entities having business relationship with these individuals/entities.

4.5. Customer Risk Classification and On Going Due Dilligence

Customer risk profiles should be determined by considering occupation, country of residence, sectors and countries in which the customer operated, , frequency of cash disposals, individuals/entities with which they have business relationship, business volume with the bank, banking services used. The purpose of customer risk profile is providing monitoring and control activities in order to minimize possible risks.

Customer risk classification methodology includes at least the following three risk categories:
- high risk;
- medium risk; and
- low risk.

Customer's risk classification is reviewed on a periodic basis and, at a minimum, in accordance with the following frequency:

- for high risk clients or those with a higher risk classification – every two years;
- for medium risk clients – every three years; and
- for low risk clients – every five years.

Implementation details and changes related to this issue are identified via internal procedures published/to be published by AML Department/Compliance and Internal Control Management, circulars and/or procedures.

4.6. Screening Of Clients And Payments

All new customers and, where relevant, the directors, beneficial owners and other connected persons are screened against a database that contains:

- the European Union Financial Sanctions List;
- the OFAC SDN List;
- United Nations Security Council List (UNSC)
- any locally-issued sanctions lists applicable to the Legal Entity;
- a list of PEPs provided by a reputable commercial organization (such as Dow Jones or WorldCheck)

Furthermore, existing customers are screened against the above sanctions lists whenever the lists are updated and to periodically screen their entire customer database against the lists.

Implementation details and changes related to this issue are identified via internal procedures published/to be published by AML Department/Compliance and Internal Control Management, circulars and/or procedures.

5. MONITORING AND CONTROL

It is fundamental that the bank should be protected against risks and should be monitored and controlled without interruption to ensure its activities are conducted in compliance with the Law, related regulations, corporate policies and procedures .

Monitoring and Control activities are held by AML section in daily basis which directly reports to Compliance Officer. Results of monitoring and control actions are reported to Compliance Officer for evaluation in terms of suspicious transaction.

Monitoring and control activities are conducted by making necessary systemic arrangements and taking into consideration the following:

- Monitoring and control of customers and transactions in high risk groups,
- Monitoring and control of transactions with risky countries,
- Monitoring and control of complex and unusual transactions,
- Monitoring and control of connected transactions when taken together that exceed the amount requiring identification,
- Controlling information and documents about customers to be maintained on electronic media or to be maintained in writing and information that is mandatory to be included in electronic transfer messages, rectification of deficiencies and their updating
- Continuous monitoring throughout the lifetime of the business relation the consistency of the transaction conducted by the customer with information about the business, risk profile and sources of funds of the customer,
- Controlling of transactions conducted by using systems that allow non- face to face transactions,
- Risk-focused controlling of newly presented products and services that may become open to misuse due to developing technologies,
- Controlling whether business relationship is established with individuals/institutions/ entities in blacklists of Competent Authorities within the scope of Prevention of Laundering of Proceeds of Crime and Financing of terrorism.
- Customer transactions are controlled in comparison to customer profile within the scenarios of monitoring and control activities.

6. SUSPICIOUS TRANSACTIONS

In case there are any findings, suspicions or grounds for suspicion derived during monitoring and control activities during the performance of non-face to face activities, that the assets involved in the transaction were acquired illicitly or are used for illicit purposes or were used for terrrorist activities or terrorist organizations or by terrorists or by persons financing terrorist activities or are associated with or related to the foregoing, that the customer is conducting transactions inconsistent with its profile, declining to provide information or documents, suspicious transaction reporting is made, regardless of a threshold in amount

Any kind of support regarding supply of information to Compliance Officer to perform his duties in a due and timely manner should be provided by the Head Office sections and branches and the information requested by him should be conveyed in the form and by the time set out in the request.

Branches and Head Office units do not report suspicious transaction to MASAK directly. Suspicious transactions should first be notified to Compliance Officer.

Financial Crimes Prevention Department shall evaluate the notifications regarding suspicious transactions and Compliance Officer is authorized to decide whether the transaction should be reported to Financial Crimes Investigation Board (MASAK) as a suspicious transaction.

Suspicious transaction reports to MASAK within this scope and internal notifications to be made to Compliance Officer cannot be shared with anyone, except related authorities determined by law.
Notification period of a suspicious transaction to Compliance Officer is at most three working days following the date of detecting the transaction. The period between the date of detecting the suspicious transaction and date of reporting this transaction by Compliance Officer to MASAK is at most 10 working days, including evaluation of Compliance Officer.

7. INTERNAL AUDIT

The internal audit management is responsible to audit annually on a risk sensitive basis whether the activities of the bank related to anti-money laundering law, regulations and communiques thereunder are conducted in compliance with the aforementioned

legislation and policies and procedures of the bank. The findings of the internal audit are channelled to Financial Crimes Prevention Department and necessary measures are taken by the related department for rectification of deficiencies.

The deficiencies, errors and frauds detected as a result of internal audit and counter measures to avoid them are reported to Board of Directors by Compliance Officer.

8. TRAINING

The Bank organizes training programs consistent with its size, business volume and other changing circumstances regarding Prevention of Laundering of Proceeds of Crime and Financing of terrorism with the purpose creating an institution culture by increasing the sense of responsibility of staff on policy and procedures of institution and on risk-based approach and updating of staff information.

Training activities are conducted under surveillance and coordination of Compliance Officer. Topics for the aforementioned training activities, the employees to participate in the training, the instructors and the training schedule are determined jointly by Compliance Officer and Training and Development Group.

The Bank training programs are conducted in two ways- in-class and remote teaching according to experience and job definition of employees to receive training that is prepared by Turkish Banks Association, The Financial Crime Investigation Group. Bank must implement and maintain procedures that ensure that training on AML is provided to new joiners within 90 days of their joining the Bank. The Bank shall review the awareness of its employees with periodic surveys or assessments and ensure that employees failing to successfully finish the surveys repeat the training.

Training covers all of the bank employees and the instructors must have attended The Financial Crime Investigation training.

The training is repeated periodicaly considering also amendments of the regulations and other requirements. The training facilities are controlled by surveys and evaluation processes in terms of the Employees' sufficiency in order to take necessary actions about the results.

9. REGULATORY TRACKING

Mitigating the Bank's potential risk and constantly monitoring and control is important to ensure that activities are conducted in compliance with laws and regulations related to this Law, Corporate Policy and procedures.

Within this scope;
- Bank changes to relevant laws, regulations and guidance are identified and analyzed for their impact upon the rules; and
- It is ensured that related rules and controls are modified to deal with any material impact of those changes.

10. OBLIGATION TO SUBMIT INFORMATION AND DOCUMENTS

Information and documents required to be provided regularly as well as information and documents requested by authorized institutions and officers are provided within the frame of the law and regulations thereunder.

11. MAINTENANCE OF RECORDS

The bank saves and maintains all information and documents provided to it in accordance with the law on prevention of laundering of proceeds of crime and regulations thereunder in an easily accessible form to be submitted when required and for the duration set out in the legislation.

Documents and records of suspicious transactions reports made to MASAK or internal reports made to the compliance officer, documents attached to reports, the written reasons relating to suspicious transactions decided not to be reported by compliance officers are all in the scope of obligation of retaining and submitting.

12. MANAGEMENT INFORMATION AND REPORTING

Compliance Officer ensure that they have appropriate internal management information sufficient to allow them to assess and monitor the effectiveness of controls and that regular reports about the AML programme are made to Senior Management, Audit Committee and Board of Directors. Additionally, in case there is any urgent/important issue, necessary reporting is made.

13. OTHER OBLIGATIONS WITHIN THE SCOPE of PREVENTION of FINANCING OF TERRORISM REGULATIONS

Bank acts in a risk based approach for preventing financing of terrorism as well as preventing of laundering and proceeds of crime in order not to be abused in financing of terrorism and not to face risks.

13.1. Freezing of Asset

The Bank, shall assure the management of the frozen assets on its records in the framework of the Law No. 6415 on the Prevention of the Financing of Terrorism dated 07.02.2013 and related regulations in accordance with permission of MASAK. In case of notification and announcement, Banks shall inform MASAK of whether they have any asset records, and if they have, of the information on the duly frozen asset within seven days following the date of notification using the same method of notification. The banks also inform MASAK of the application of unfreezing decisions in accordance with the abovementionned methods of notification. (In seven days following the notification)

13.2. Bank's Obligations

13.2.1. Reporting to MASAK

For freezing any account, Bank makes reporting to MASAK the type of business relationship, customer/account number, right and claim.

13.2.2. Blocking Non-Face-to-Face Systems

All credit and bank card of persons, institutions or organizations whose assets are frozen shall be blocked and their access to online banking or all other non-face-to-face systems shall be thwarted by the Bank.

13.2.3. Freezing Joint Accounts

All of the accounts owned jointly by the third parties and the designated persons, institutions or organizations shall be frozen as a whole. Other shareholders of frozen accounts shall notify MASAK of their rights on such accounts and the information and documents regarding their basis. The designated persons, institutions or organizations shall pay their debts to other shareholders of joint accounts through the bank account only if MASAK permits so.

13.2.4. Increase in the Amount of the Asset

If there is an increase in the amount of assets frozen, such increase shall also be subject to provisions of the freezing of assets. Therefore, it shall not be possible to access the interest, profit share, dividend and any other revenue to be obtained from the frozen assets except in the cases permitted by MASAK.

13.2.5. Access to Frozen Assets

The power of disposition on frozen assets shall only be exercised upon the permission of MASAK.

Except for the cases permitted by MASAK, those whose assets are frozen may not engage in actions for obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset. Liable parties shall not allow or facilitate the execution of such actions.

14. MONITORING OF CONTROLS

The activities conducted by Bank are controlled by AML Department whether these activities are conducted in compliance with laws and regulations related to this Law, Corporate Policy and procedures via 2nd Level Controls. This control program is constructed in accordance with the Bank's structure.