

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Introduction and Scope

QNB Finansbank (hereinafter referred to as “the Bank”) as the main financial institution and its subsidiaries (QNB Finans Leasing, QNB Finans Factoring, QNB Finans Invest and QNB Finans Asset Management) (hereinafter collectively referred to as “Companies of the Group”) collectively form Financial Group.

Group Compliance Policy on Anti-Money Laundering and Combating Financing of Terrorism (hereinafter referred to as “Group Compliance Policy”) was prepared to determine Financial Group’s principles and implementation procedures regarding anti-money laundering and counter financing of terrorism (AML/CFT) to be valid at Financial Group level.

Adequacy and effectiveness of Group Compliance Policy are assessed on an annual basis at least or whenever necessary. This policy was prepared in accordance with local regulations and obligations of QNB Group regarding AML/CFT. In case of a discrepancy, strict measures will be applied.

Purpose

The purpose of the Policy is to establish a joint standard regarding AML/CFT at Financial Group level in order to:

- Protect Financial Group from being exploited for money laundering and financing of terrorism as well as any other illegal activities,
- Ensure compliance with applicable laws and regulations, avoid legal sanctions that may be imposed on Financial Group and ensure, enhance and protect the credibility, integrity and reputation of Financial Group,
- Ensure that appropriate strategies are prepared to minimize the risks that may be encountered by Financial Group,
- Provide guidance to the senior management as well as managers and employees of the Bank and Companies of the Group.

Responsibilities

The BoD of the Bank is ultimately responsible for effective implementation of this Policy at Financial Group level.

Compliance Officer of Financial Group is responsible for controlling and supervising the implementation of this Policy approved by the BoD of the Bank.

AML/CFT measures are the main responsibility of Financial Group and its employees.

The Bank and Companies of the Group prepare policies and procedures covering requirements of local and international regulations regarding AML/CFT within the framework of Group Compliance Policy and carry out their activities within the scope of this Policy.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

It is obligatory for managers and employees of Financial Group to be aware of and appropriately act with this Policy and relevant procedures to protect Financial Group against activities of money laundering and financing of terrorism.

All employees of the Bank and Companies of the Group are obliged to assist in identifying activities related to money laundering and financing of terrorism. Therefore, the employees of the Bank and Companies of the Group shall be aware of the fact that a deficiency in implementing the procedures regarding AML/CFT may be evaluated as gross negligence and result in disciplinary proceedings.

Establishment of Corporate Policies and Procedures by the Bank and Companies of the Group

The Bank and Companies of the Group establish their own corporate policies and procedures according to Group Compliance Policy and by considering the nature of the fields of activity. Corporate policies include principles regarding risk management, monitoring and control, training and internal audit at minimum.

A separate policy was prepared by the Bank regarding intragroup information sharing to be implemented at Financial Group level.

Issues stipulated within the scope of local risk assessment are taken into account while preparing corporate policies.

With corporate policies, it is ensured that company employees are informed and aware of below issues;

- Compliance with obligations regarding AML/CFT,
- Assessment of customers, transactions and services with a risk-based approach,
- Determination of strategies, internal corporate controls and measures, operation rules, responsibilities to minimize possible risks.

Responsibilities in processes to be established for AML/CFT, thresholds and rules to be implemented in approval of transactions, reporting and monitoring activities are clearly defined.

Recommendations, principles, standards and guidelines introduced by other local and international organizations are also used while preparing corporate policies and procedures provided that they do not violate local regulations.

Assignment of Compliance Officer and Assistant Compliance Officer and Establishment of Compliance Unit

The BoD of the Bank assigned Financial Group Compliance Officer and Assistant Compliance Officer to carry out compliance program within the scope of Group Compliance Policy.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Financial Group Compliance Officer reports to the BoD of the Bank through a member of the BoD residing in Turkey, delegated by the BoD regarding authorities and responsibilities related with money laundering and financing of terrorism.

BoDs of Companies of the Group assign Compliance Officer and Assistant Compliance Officer to manage compliance programs and risks regarding money laundering and financing of terrorism.

Compliance Officers of Companies of the Group report to the BoDs to which they are responsible and relevant Financial Group Compliance Officer regarding the activities included in the scope of Group Compliance Policy.

Compliance Officers and Assistant Compliance Officers shall have sufficient seniority, knowledge and authorization to fulfill their responsibilities independently.

In order to ensure that Compliance Officers effectively carry out the roles and responsibilities, BoDs ensure that sufficient personnel and resource are allocated to compliance units by considering issues such as transaction volume, the number of branches and employees or criticality of possible risks.

Responsibilities of Compliance Officers

Compliance Officers are responsible for supervising activities of the Bank and Companies of the Group within the scope of AML/CFT, relevant policies and procedures and for implementing them by considering relevant laws and regulations and recommendations of FATF (Financial Action Task Force) and Basel Committee.

Financial Group Compliance Officer is responsible for implementing Group Compliance Policy at Financial Group level.

Financial Intragroup Information Sharing

Information is shared between the Bank and Companies of the Group for customer identification as well as accounts and transactions. Confidentiality provisions written in private laws shall not be applied in intragroup information sharing.

Information is shared between the Bank and Companies of the Group within the scope of the policy covering information sharing at Financial Group level.

Risk management activities

The Bank shall identify, consider, understand, assess, document, monitor, and update their ML/TF risks, on a regular basis in accordance with the National Risk Assessment, their ML/TF risks. The Bank shall consider the risks that may arise from the development of new products, new business practices or new techniques, prior to the use of such products, practices, techniques and the risks identified at the national level and any other underlying factors.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

The Bank and Companies of the Group define risks that may arise from customers and services according to fields of activity. They establish processes to monitor and control risky customers, transactions or services.

They evaluate alarms regarding risky transactions generated by scenarios to be defined in software products by using them to identify risky transactions. Companies of the Group not using software due to company size carry out this process by obtaining reports from the system. They ensure that relevant units are informed to take necessary measures to minimize the risks identified as a result of such engagements.

Risk management activities are continuously reviewed according to changing and developing conditions. Necessary improvement engagements are performed by following up recommendations, principles, standards and guidelines introduced by local regulations and international organizations.

Strict measures are applied for high risk customers and transactions.

Risk monitoring and assessment results are regularly reported to the BoD.

Risk Based Approach and Customer Risk Classification Methodology

Risk based approach is implemented to classify the customers into risk profiles.

The Bank and Companies of the Group use a risk assessment methodology that is appropriate for the size of operations, business profile and risk profile of customers to minimize the risk of money laundering and financing of terrorism.

In risk based approach, customers are classified according to risk profiles which are based on following components:

- Customer Risk – identifying source of income or transaction types,
- Geographic Risk – involvement of customers with regions associated with money laundering and financing of terrorism or other illegal activities,
- Product Risk – specific products and service types,
- Distribution Channel Risk – how the service is provided

KYC methodology is applied within the scope of relevant risk components based on customer risk classification.

High risk customers are subject to continuous monitoring regardless of their risk scores.

A separate process is carried out for certain high risk customers such as Politically Exposed Persons (PEP) and Non Profit Organizations (NPO) in risk based approach.

Customer Acceptance

Having sufficient information within the scope of customer identification (KYC) and using such information effectively is the basis of all other processes related to AML. This helps in

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

prevention of fraud attempts and detection of suspicious transactions and protects the Bank and Companies of the Group from financial and reputation risks.

Employees which establish business relationships with customers are responsible for ensuring that customer ID authentication and verification are conducted based on documents and data obtained from independent sources and for identifying the actual beneficiary of the transaction.

Information required to be obtained within the scope of risk assessment and customer identification is kept up-to-date.

The Bank and Companies of the Group regularly control whether their customers are included in any international sanctions lists issued by UN, EU, UK, OFAC and other regulatory institutions.

Within the scope of this Policy, the Bank and Companies of the Group shall open accounts for their natural and legal customers that comply with the Financial Group's targets and objectives.

Such customers shall be eager to continue the business relationship in line with relevant rules and shall have reasonable information and awareness about tariffs. BoDs may establish other specific rules about these criteria as it may vary in time.

The Bank and Companies of the Group shall not provide service to natural and legal persons whose ID authentication is not performed in an adequate manner.

They shall not form business relationships with natural and legal persons who do not comply with this Policy and/or other relevant local/international regulations. They shall be careful and attentive in customer acceptance and continuous business relationships with PEPs and NPOs.

It is forbidden to open anonymous accounts, deal with anonymous customers and shell banks or open accounts in fictitious names.

All existing and new customers are checked to determine whether they are included in local and international sanctions lists.

Simplified KYC Principles

Simplified due diligence is the basic level of due diligence conducted on a customer. This is appropriate where there is little opportunity or risk for a customer becoming involved in money laundering or terrorist financing, i.e. when the customer risk category is low.

Enhanced KYC Principles

High risk customers are subject to enhanced KYC principles and continuous monitoring.

Such activities are generally carried out for following customer categories:

- Transactions that are not performed face-to-face and new technologies,
- PEPs,

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- Correspondent banking relationships and financial institutions operating in high risk regions,
- Charities, clubs and societies,
- Regional risks (regions that are not internationally collaborative enough, that do not cooperate or are subject to sanctions as per FATF or that have a tendency for corruption),
- Customers who do not reside in Turkey,
- Complex legal institutions/entities, trusts, clubs and communities.

Any account opening involving a Politically Exposed Person (PEP) shall be subject to prior approval of Executive Management through the Group Compliance Division.

The Bank shall not continue the business relationship with any customer found to be a PEP or linked to a PEP unless approved by the Executive Management through the Group Compliance Division.

Trigger Events for Customer Due Diligence

As a general rule, Customer Due diligence must be applied when establishing a business relationship with a new customer. The following circumstances may require the Bank to revisit/review the initially made CDD:

- There is a change to the signatory or the beneficiary of an existing account or business relationship.
- A transaction greater than the transaction threshold stated during on boarding.
- There are material changes in the way the account is operated or material changes in the manner of conducting business relationship.
- The documentation standards change substantially.
- There are doubts about the veracity or adequacy of previously obtained customer due diligence information and documents.
- Carrying out wire-transfers above the prescribed threshold limit.
- There is a suspicion of money laundering or terrorist financing regardless of the amount of the transaction.
- Taking up of a new product or service by a customer.

Updating KYC Information

All existing customers are subject to a periodical KYC information review/update. The frequency of the reviews depends on the customers' AML/CTF risk rating, for "High Risk" customers, KYC information should be reviewed/updated annually, for "Medium Risk" customers KYC information should be reviewed/updated every 3 years, and for "Low Risk" customers KYC information should be reviewed/updated every 5 years.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Beneficial Ownership

A beneficial owner is a natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Beneficial ownership of a customer should be identified on a risk-based approach when establishing a relationship with a customer.

The natural persons owning or controlling more than 25% in all customers will be identified and verified.

Monitoring and Control Activities

The Bank and Companies of the Group integrated some programs into their systems to check whether existing or new customers are included in international sanctions lists in accordance with legal regulations. They benefit from these programs manually and automatically to identify suspicious customers and transactions and to prevent risks of money laundering and financing of terrorism.

They carry out effective process for continuous monitoring of accounts and transactions with the aim of detecting, monitoring and evaluating high risk customers and transactions.

Any deficiencies detected upon such controls are reported to relevant business units so that necessary measures are taken and results are followed up.

Employees responsible for carrying out these activities are given access to internal information sources and systems within the scope of monitoring and control.

The Bank and Companies of the Group may terminate their business relationships with customers they deem to bear suspicion in terms of being included in international sanctions lists. The Bank's AML/CFT Committee decides on whether the business relationship is to be terminated or not and determines on how customers are to be notified about this issue.

Obligation to Report Suspicious Transactions

All employees are made aware via trainings and briefings that they are personally obliged to report any suspicious activity or knowledge within the scope of AML/CFT and that failure to fulfill this obligation will have penal consequences.

Employees in the Bank and Companies of the Group report suspicious transactions via the related special line in intranet system and/or via e-mail in writing to Compliance Officer and Assistant Compliance Officer. Compliance Officers/Assistant Compliance Officers examine the suspicious transaction notifications and report them to MASAK if necessary.

No information is shared about suspicious transaction notifications at Financial Group level.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Tipping off is prohibited in terms of the law and therefore, all employees shall abide by the law or otherwise be subjected to legal punishments and disciplinary actions.

Training Activities

Continuous training programs are organized in the Bank and Companies of the Group to inform the employees about local and international regulations related to AML/CFT, to increase their responsibility awareness and to create an effective corporate culture.

All employees are included in the scope of such training programs (except drivers, manager and platform assistants, technical personnel, security guard, etc.).

Training activities are carried out under the supervision and monitoring of Compliance Officers of the Bank and Companies of the Group. These activities are reviewed by relevant business units based on evaluation and measurement results and they are repeated regularly and upon requirement.

Financial Group Compliance Officer is responsible for coordinating training program engagements at Financial Group level and monitoring effective implementation of programs.

Compliance Officers of the Bank and Companies of the Group submit the annual training program engagements to the approval of the BoD member residing in Turkey (to whom BoD granted money laundering and financing of terrorism-related authority). It is ensured that the approval training program is conducted effectively.

The Bank and Companies of the Group carry out the training activities via seminars, conferences, classroom trainings or online trainings. Trainings are prepared and given by managers in Compliance Units or by experts outsourced from external companies. Training activities are carried out in coordination with Human Resources Training Unit.

Trainings shall at least cover the following issues;

- Money laundering and financing of terrorism concepts,
- Money laundering stages, methods and case studies,
- AML/CFT legislation,
- Risk areas,
- Corporate policies and procedures,
- KYC principles,
- Principles related to suspicious transaction reporting,
- Obligation of keeping and submitting,
- Obligation of providing documents and information,
- Penal sanctions to be imposed in case of failure to fulfill obligations,
- International regulations on AML/CFT.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi

GROUP COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Record Keeping

The Bank and Companies of the Group shall keep the records related to customer accounts for at least 10 years pursuant to Banking Law and relevant regulations.

International Sanctions Policy

Complying with the sanction decisions of UN, EU, UK and OFAC applicable for any business or transaction under all conditions and operating in accordance with best practice guidelines issued by regulatory institutions are a separate policy of the Financial Group. Thus, Financial Group's Compliance Units are responsible for preparing the necessary procedures, guidelines and mechanisms to comply with such regulations and to prevent any violation that may result in sanctions.

Audit

The Bank's Internal Audit Department carries out audits to evaluate adequacy and effectiveness of measures taken by the Financial Group to assess, monitor and manage the risks of money laundering and financing of terrorism.

Internal Audit Departments of the Bank and Companies of the Group carry out audits to evaluate adequacy and effectiveness of measures that they have taken to assess, monitor and manage the risk of money laundering and financing of terrorism.

Sorumlu	Onay	Yürürlük Onay	Gizlilik
İç Kontrol Ve Yasal Uyum Başkanlığı	Yönetim Kurulu	Özge Otmanbölük	Kurum İçi