Approved by decision of
the Council of the Bank
№ 26 as of November 2, 2017

Rules
of internal control on countering money laundering and the financing of terrorism at “Hamkorbank” JSCB

Stamp:
«Registered» on November 6, 2017
in the “Methodology” sector
of Joint-stock commercial bank
with participation of foreign capital
«Hamkorbank»
№ 06-3/2 DDB

2017

Rules of internal control on countering money laundering and the financing of terrorism at "Hamkorbank" JSCB

These Rules have been developed in compliance with the laws "On the Central Bank of the Republic of Uzbekistan", "On banks and banking activity", "On banking secret", "On countering money laundering and the financing of terrorism" and the requirements of the "Rules for internal control on countering money laundering and the financing of terrorism at commercial banks" № 2886 as of May 23, 2017 and establish the procedure for organizing and executing internal control activities in the area of countering money laundering and the financing of terrorism at "Hamkorbank" JSCB.

1.General provisions

1.1. The following basic concepts are used in these Rules:

internal control - activities of a commercial bank on adequate verification of customers, managing the risk of laundering and the financing of terrorism, identifying suspicious and shady transactions, as well as transactions with participation of persons involved or suspected of participating in terrorist activities or distribution mass destruction weapons;

Internal control system - a complex of actions of the Internal Control Service and other departments of the bank aimed at achieving the goals and objectives determined by the "Rules for internal control on countering money laundering and the financing of terrorism at commercial banks" № 2886, these Rules and internal documents;

Rules for internal control - "Rules for internal control on countering money laundering and the financing of terrorism at commercial banks" № 2886;

specially designated public authority - the Department for combating tax, currency crimes and money laundering under the General Prosecutor's Office of the Republic of Uzbekistan (hereinafter - the Department);

customer - a natural or legal person who has applied to a commercial bank with an order (application, petition) to perform a transaction with monetary funds or other property (hereinafter referred to as "transactions");

beneficial owner - a person who ultimately owns the property rights or actually controls a customer and in whose interests the transaction with monetary funds or other property is performed;

participants of the transaction - customers, their representatives, as well as partners of the customer involved in the transaction;

shady transaction – a transaction in relation to which a commercial bank in the process of exercising internal control had doubts about its implementation with the aim of countering money laundering and/or the financing of terrorism, before decision-making whether to include (not to include) it in the category of suspicious transactions;

suspicious transaction – a transaction that is in the process of preparation, accomplishment or which has already been accomplished with respect to which in the process of internal control a commercial bank was suspicious towards its aim of countering money laundering and/or the financing of terrorism;

one-time transactions - transactions performed by customers in a one-time procedure without opening a bank account which is not repeated for at least one month;

customer due diligence - verification of the identity and authority of the customer and the persons on whose behalf he acts, identification of the beneficial owner of the customer, as well as on the constant basis performing the study of the business relations and transactions performed by

the customer in order to verify their compliance with the information about such customer and his activities;

customer identification - identification of the data on customers on the basis of the documents provided by thereto in order to perform customer due diligence by a commercial bank;

identification of the beneficial owner of the customer - determination by the commercial bank of the legal entity of the owner, including the person supervising the customer by examining the ownership structure and management on the basis of constituent documents determined by the law (Charter and (or) constituent contract, regulations);

states not participating in international cooperation in the sphere of countering money laundering and the financing of terrorism - states and territories determined in official statements of the Group on the development of financial measures to counter money laundering that threaten the international financial system and which system for countering money laundering and the financing of terrorism has crucial shortcomings;

offshore zone - states and territories providing preferential tax regime and (or) not envisaging the disclosure and submission of the information when performing financial transactions;

risk - the risk that customers will perform transactions with the aim of money laundering or the financing of terrorism;

distant services - banking services provided for performing transactions with the application of the software that enable transactions to be performed without a customer's arrival at a commercial bank;

public officials - persons appointed or elected permanently, temporarily or by special authority, performing organizational and regulatory functions in public administration bodies and authorized to carry out legally significant actions, as well as persons performing these functions of an international organization or in a legislative, executive, administrative or judicial authority of a foreign country;

freezing of cash or other property - a ban on the transfer, conversion, disposal or movement of cash or other property;

suspension of a transaction - suspension of the execution of customer's orders for the transfer, conversion, alienation and use of funds or other property to other persons, as well as other legally significant actions;

a person participating in or suspected of participating in terrorist activity – an individual or legal person who participates or is suspected of participating in a terrorist activity, directly or indirectly owns or controls the organization performing or suspected of performing terrorist activity, as well as the legal entity who is owned or controlled by an individual or an organization performing or suspected of performing a terrorist activity;

a person participating or suspected of participating in the proliferation of mass destruction weapons – an individual or a legal entity determined by the resolutions of the UN Security Council and international legal documents admitted by the Republic of Uzbekistan aimed at preventing the spread of mass destruction weapons;

List - a list of persons participating or suspected of participating in terrorist activities or the proliferation of mass destruction weapons, compiled by a specially designated public authorities on the basis of the information provided by the public authorities involved in countering against terrorism and the proliferation of mass destruction weapons, as well as the information received through official channels from the relevant authorities of foreign countries and international organizations.

bank – «Hamkorbank» JSCB, its branches and mini-banks, kiosks located outside the building of the bank.

1.2. The aims of the System of the internal control of «Hamkorbank» JSCB on countering money laundering and the financing of terrorism (CMLFT) are the following:

a) efficient identification and suppression of transactions aimed at money laundering, the financing of terrorism and the proliferation of mass destruction weapons;
b) preventing intentional or unintentional involvement of the Bank in the criminal activity, the penetration of criminal capital in its Charter fund (capital), as well as the penetration of criminals in the management of a commercial bank;
c) identification, assessment, documentary recording and reduction of risks;
d) ensuring strict compliance with the requirements of the legislation on countering money laundering and the financing of terrorism.

1.3. The main objectives of System of the internal control of «Hamkorbank» JSCB on countering money laundering and the financing of terrorism (CMLFT) are the following:
a) undertaking appropriate measures to identification and assessment, documentary recording and reduction of risks;
b) implementation of identification procedures and measures for the adequate verification of customers including verification and regular updating of data about the customer and their beneficial owners;
c) identification of beneficial owners, undertaking appropriate measures to verify their identity and detection of sources of funds or other property used in implementing the transaction;
d) implementation of comprehensive monitoring of transactions performed by public officials and their close relatives;
e) identification of shady and suspicious transactions according to the procedure established by these Rules and internal documents;
f) timely submission to the specially designated public authorities the information (documents) on suspicious transactions identified during the implementation of internal control;
g) among the participants in the transaction identification of the persons involved in or suspected of participating in terrorist activities or the proliferation of mass destruction weapons by checking with the List;
h) instant suspension of a transaction, except for transactions on crediting funds received to the account of a legal entity or an individual, and (or) freezing of funds or other property of persons included in the List without their prior notification;
i) ensuring confidentiality of the information related to countering money laundering and the financing of terrorism;
j) ensuring the storage of information on the transactions, as well as identification data and materials on the customer due diligence within the periods established by the legislation;
k) prompt and systematic provision of the management of a commercial bank with reliable information and materials required for proper decision-making;
l) development of the database on the implementation or attempts to perform suspicious transactions, persons (managers, founders, shareholders who own not less than ten percent of the company’s shares, participants) associated with customers who have performed suspicious transactions, as well as mutual change of such information with other commercial banks and government agencies in compliance with the legislation;
m) studying the system of internal control of foreign banks when establishing correspondent relations thereto;
n) applying required measures with the aim of paying a particular attention to curbing the threat of using the services of a commercial bank to commit an offense, in particular, money laundering and/or financing of terrorism, using the latest technologies that raise the anonymity of transactions;
o) in the customer base identification of persons associated with the financing of terrorist activities upon requests.

1.4. The internal control system performs the following functions:

a) undertaking relevant measures stipulated by the legislation, these Rules, internal documents to suppress the threat of using the services of a commercial bank to money laundering and(or) the financing of terrorism;

b) monitoring the observance by a commercial bank over the requirements of legislation and internal documents on countering money laundering and the financing of terrorism;

c) preparation and submission to management's consideration of a proposal to eliminate identified drawbacks and violations in the bank's activities in terms of non-compliance with the requirements of the legislation and internal documents on countering money laundering and the financing of terrorism;

d) monitoring over elimination of errors and drawbacks in the organization and functioning of the internal control system detected during the inspections by authorized representatives of the Central Bank of the Republic of Uzbekistan (hereinafter - the Central Bank), employees of the Bank's Internal Audit Service, external auditors and employees of a specially designated public authorities;

e) compliance of the Bank's internal statutory documents with the requirements established in the Internal Control Rules;

f) systematic submission of a quarterly progress report on the implementation of the requirements of these Rules based on the established plan to the Chairman of the Executive Board of the Bank;

g) interaction with the Central Bank and a specially designated public authority on the organization of internal control, prevention and elimination of violations by employees of the requirements of the legislation, these Rules and internal documents;

h) holding training sessions on countering money laundering and the financing of terrorism.

1.5. The "Internal Control Service" of the head office of the bank performs distant supervision over internal control employees carrying out their activities at branches on the basis of software systems and information from internal control employees on countering money laundering and the financing of terrorism (CMLFT), and internal control officers carrying out their activities at branches supervise the activities on the issues related to countering money laundering and the financing of terrorism.

2. Organization of the internal control system

2.1. The internal control system of "Hamkorbank" JSCB is organized with the account of the peculiarities of the bank' performance, its core business, customer base and the level of risks associated with customers and their transactions.

2.2. The structure of the internal control system of a commercial bank including its branches is determined by the decision of the Executive Board of the bank.

2.3. The structure of the internal control system of the bank includes the Internal Control Service of the head office of the bank, as well as specialists of the Internal Control Service of each branch of the bank.

2.4. The head and employees of the Internal Control Service are appointed and dismissed by order of the Chairman of the Executive Board of the Bank.

2.5. The head and employees of the Internal Control Service are included in the staffing position of the head office of the bank, their salary and payments equivalent thereto are exercised at the expense of the head office of the bank.

2.6. The head of the Internal Control Service must have a university degree in economics or law and experience in managing a subdivision of the bank associated with banking transactions for at least two years or work experience in the Internal Control Service for at least one year.

2.7. A person appointed to the post of the head and employee of the Internal Control Service is obliged to:

a) know banking and financial legislation;

b) know international standards for countering money laundering and the financing of terrorism;

c) possess knowledge of accounting rules, as well as regularly participate in qualification upgrading at specialized courses.

2.8. The following persons cannot be appointed to the positions of the head or employee of the Internal Control Service:

a) demonstrated inadequate management of the entrusted subdivision or dishonest conduct of business in their activities and personal behavior;

b) previously were held criminally liable by the court for crimes in the field of economics.

2.9. The Head of the Internal Control Service reports directly to the Chairman of the Executive Board of the Bank and is independent from other subdivisions of the bank. Employees of the Internal Control Service report directly to the head of the Internal Control Service.

2.10. The head and employees of the Internal Control Service have the following rights:

a) with the aim of exercising internal control, require necessary administrative and accounting documents from managers and employees of the bank's subdivisions;

b) make copies of received documents, receive copies of files and other records stored in electronic databases, local computer networks and autonomous computer systems of the bank for the internal control implementation;

c) request and receive the assistance of specialists from other subdivisions of the bank;

d) enter the premises of the bank's subdivisions, as well as with the written permission of the Chairman of the Executive Board of the bank the premises used for storing documents (archives), cash and valuables (cash safe custodies), computer data processing and storing data on computer media;

e) submit to the Chairman of the Executive Board or his deputy who has relevant powers, a draft decision on the suspension of transactions except for transactions on crediting funds received to the account of a legal entity or an individual, and (or) freezing of funds or other property of persons included in the List ;

f) submit proposals to the Chairman of the Executive Board of the bank on further actions in relation to customer transactions including obtaining additional information or verifying available information about a customer or a transaction in compliance with the law;

g) perform other actions in compliance with these Rules and internal documents.

2.11. The head and employees of the Internal Control Service do not have the right to sign on behalf of a commercial bank or to approve payment (settlement), credit and accounting documents.

2.12. The objectives, duties and rights of the Internal Control Service are determined by the Charter of the Internal Control Service.

3. Customer Due Diligence and identification of their beneficiary owner

3.1. Banks and its branches are obliged to independently undertake measures to adequately verify customers in the following cases:

a) in establishing economic and civil-law relations, including:

when an individual or a legal entity apply for opening a bank account (deposit);

when an individual applies for issuing a bank plastic card;

when legal entities and (or) individuals apply for the purchase of securities issued by a bank;

when legal and (or) individuals own shares in a bank in the amount equal to or exceeding one percent of its Charter capital;

when an individual applies for a loan or a safe custody service in a bank deposit box;

b) when performing one-time transactions in the following cases:

sale of cash foreign exchange in the amount equal to or higher than 500-fold the minimum wage by individuals;

exchange, replacement and (or) exchange for another foreign exchange (conversion) by individuals of cash foreign exchange in the amount equal to or higher than 500-fold the minimum wage;

receiving from customers for collection and (or) for the examination of cash foreign exchange in the amount equal to or higher than 500-fold the minimum wage;

transactions performed by individuals with the use of plastic cards (cash withdrawal, payment for goods and services) through terminals located at a bank (except for payments for public utilities, communication services, payments to the budget, extrabudgetary funds and other compulsory payments) in the amount equal to or exceeding 300-fold the minimum wage;

receiving from the cashier's cash foreign exchange by customers with the use of plastic cards issued by other banks for the amount equal to or higher than 100-fold the minimum wage;

purchase of foreign exchange by individuals;

making or receiving a money transfer without opening or using a bank account (except for payment for public utilities, communication services, payments to the budget, extra-budgetary funds and other compulsory payments);

c) when performing suspicious transactions;

d) if there are doubts about the reliability or adequacy of previously obtained data about the customer.

3.2. Measures on the customer due diligence include the following:

a) verification of the identity and authority of the customer and the persons on whose behalf he acts on the basis of relevant documents;

b) identification of the beneficial owner of the customer;

c) a study of the aim and nature of the business relationship or planned transactions;

d) on the constant basis performing the study of business relations and transactions carried out by the customer in order to verify their compliance with the information about such a customer and its activities.

3.3. Customer due diligence measures are executed by the bank employees servicing customers, making customer's transactions, and opening of accounts thereto.

3.4. Enforced customer due diligence measures include the following:

a) collection and recording of additional confirmed customer information available in open sources and databases;

b) receiving the information about the sources of funds or other property on the transactions performed thereto from the customer;

c) study of the objectives of the transactions planned or performed by the customer;
d) executing continuous monitoring of the transactions of this customer.

3.5. Enforced customer due diligence measures are executed by employees of the Internal Control Service of the branch and the person responsible for the customer's transaction.

3.6. Identification of the customer and the beneficial owner of the customer is executed by the bank on the basis of information stipulated in Annexes 1, 2 and 3 to these Rules, as well as documents that constitute the basis for performing transactions and other operations and other required information.

3.7. Employees who are responsible for rendering the services or performing the customer's transactions, must verify the compliance of transactions and business relationships performed by the customer, information on the such a customer and his activities and in cases of non-compliance they must report these facts to the official of the Internal Control Service.

3.8. Branches of the bank, if they are suspicious about the accuracy of the information (documents) received should undertake relevant measures to examine (verify) this information (documents). In this case, the bank has the right to apply to the relevant agencies with a request to ascertain the reliability (authenticity) of the information (documents) about customers or use state interactive services or other information systems.

3.9. All documents enabling identification of the customer and other participants of the transaction should be valid on the date of their submission.

3.10. Customer identification of an individual is executed on the basis of a document (passport or a document replacing it), certifying his personality. In this case, a responsible employee must independently familiarize himself with the original of such a document.

3.11. With proper verification of the customer - a legal entity, the relevant documents on the state registration, information about the management, as well as information specified in the constituent documents must be requested.

3.12. Receiving this information is executed by the branch's chief accountant (or his deputy) through an automated system of the state registration and registration of business entities or directly from the customer in case when it is impossible to receive the information from this system.

3.13. In the process of due diligence of legal entities, responsible employees must undertake reasonable and accessible measures to identify the individual — the beneficial owner of the customer who ultimately owns or supervises the customer including by examining the customer's ownership and management structure, as well as the founders (shareholders, who own not less than ten percent of the company's shares, participants) of the customer.

3.14. If the customer or the beneficial owner of the customer is a legal entity that is subject to the requirements of statutory acts on disclosing the information about the ownership structure, then identifying and confirming the personality of the founders (shareholders who own not less than ten percent of the company's shares, participants) of such legal entity are not required.

3.15. With the aim of proper examination and more comprehensive study of the customer - legal entity, a particular attention should be paid to:
a) the composition of the founders (shareholders who own not less than ten percent of the company's shares, participants) of the customer, identification of persons owning a share of over 10 percent of the charter fund (capital) of the customer;
b) the structure of the customer's management bodies and their powers;
c) the amount of the registered charter fund (capital) of the customer.

3.16. Customer due diligence measures are not required for public administration authorities and management.

3.17. When establishing and performing correspondent relations with a non-resident bank, the sector for working with International Financial Institutions sends the non-resident bank to fill out the application form provided in Annex 4 to these internal Rules.

3.18. After receiving an application form filled out by a non-resident bank, it should be submitted to the Internal Control Service with relevant documents attached.

3.19. A responsible officer of the Internal Control Service must fulfill the following steps on the basis of the non-resident bank application form and public information:
a) study the peculiarities of business activity of a non-resident bank;
b) on the basis of public information determine the reputation and quality of supervision, including whether investigations of violations related to money laundering and terrorist financing were investigated with respect to this bank;
c) in relation to "transit accounts" receive confirmation that the respondent bank is able to provide required identification data about the customer at the request of the correspondent bank;
d) with the aim of performing transit transfers keep all information about the electronic transfer when establishing relations with other banks;
e) examine the observance of a non-resident bank over the international standards on the issue of countering money laundering and the financing of terrorism;
f) determine the presence of government authorities operating on the constant basis in the territory where a non-resident bank is registered, in case of their absence - undertake measures to cancel the establishment of correspondent relations.

3.20. The results of due diligence of a non-resident bank are formalized upon the conclusion of the responsible officer of the Internal Control Service and are provided for acceptance to the Executive Board of the bank.

3.21. When establishing correspondent relations with the banks located within the territory of the Republic of Uzbekistan, these banks are identified by filling out the application form provided in Annex 4 to these Rules, as well as the Accounting and Reporting Department of the head office of the bank.

3.22. When identifying the customer and the beneficiary owner of the customer, the responsible employees are obliged to verify the information received with the List, as well as with the list of the countries which do not participate in international cooperation in the area of countering money laundering and the financing of terrorism, developed and provided to the bank by a specially designated public authority in compliance with the legislation.

3.23. Responsible employees have the right to refuse to the customer to perform transactions involving cash and other property in case of:

a) the absence at its location (postal address) of the authority governing the legal entity or the person authorized to act on behalf of the legal entity without a power of attorney;

b) provision of deliberate misrepresentations or failure to submit documents requested in compliance with the legislation;

c) in other cases stipulated by the legislation.

3.24. The following is prohibited:

a) open accounts (deposits) for anonymous owners, that is, without providing the documents required for the identification by an individual or a legal entity opening accounts (deposits);

b) open accounts for obviously fictitious names that are not documented;

c) open accounts without the personal presence of the person opening an account or his authorized representative;

d) establish and continue relations with non-resident banks that do not have a physical presence and permanently operating management authorities in the territories of the countries in which they are registered;

e) issue of securities and other financial instruments to bearer;

f) render services on receiving and sending money in foreign exchange including through international money transfer systems without identifying the customer;

g) set up subsidiary banks, branches or representative offices within the territory of the countries which do not participate in international cooperation in the area of countering money laundering and the financing of terrorism.

3.25. In case of absence of possibility to execute customer due diligence this fact should be reported to the Internal Control Service by the responsible employees.

3.26. The Internal Control Service will consider the issue of sending a report about this customer to the specially designated public authority provides instructions about refusing to enter into a business relationship or from performing a transaction of the customer, or terminating any business relationship thereto.

3.27. If there is the information about a violation by a non-resident bank of the requirements of international standards for countering money laundering and the financing of terrorism, the Internal Control Service reports this fact to the Chairman of the Executive Board of the bank.

3.28. The bank’s management should consider undertaking appropriate measures to the extent of terminating the cooperation with this correspondent bank.

3.29. The Internal Control Service is responsible for observing the requirements in the field of countering money laundering and the financing of terrorism by correspondent banks.

3.30. Annual identification forms provided by correspondent banks are filled in by the Internal Control Service and approved by the Chairman of the Executive Board of the bank.

3.31. The Internal Control Service should independently analyze the cases of suspension or refusal of issues and transactions of correspondent banks, and in case of necessity - make proposals for amendments in the bank’s internal regulations.

3.32. The Internal Control Service shall provide the Executive Board of the bank with an opinion on the relations with correspondent banks at least once every six months.

3.33. The instruction determining the objectives of responsible employees and the stages of their implementation regarding the implementation of customer due diligence measures should be developed in compliance with these Rules.

4. The procedure for registration, storage and confidentiality of the required information

4.1. If the documents related to the customer due diligence are developed fully or partially in a foreign language, in necessary cases responsible employees are have the right to request a document with a translation into the state or Russian language.

4.2. Responsible employees have the right to require the submission of original documents for review if they are suspicious about the authenticity of the submitted copies or in other necessary cases.

4.3. In the process of the customer due diligence, the received information about the customer is recorded in the customer's application form in compliance with Annexes 1, 2 and 3 to these Rules. In compliance with internal documents responsible employees and officers of the Internal Control Service have the right to enter other information into the customer's application form.

4.4. Application forms on all customers (except for the customers who do not require due diligence) are filled out electronically with the application of the special software. Application forms for customers engaged in suspicious and/or shady transactions included in the high-risk category are also filled in the paper form.

4.5. When transferring into the paper version of the application form filled in the electronic form, it is certified by the signature of the chief accountant of the branch, and in case of his absence, by the signature of his deputy and the responsible officer who has filled in the application form.

4.6. Employees who identify customers have a constant opportunity to use electronic application forms that are stored in the electronic database of the Internal Control program of the IABS system.

4.7. Application forms of customers filled in the paper form are stitched in a separate folder in chronological order according to the status of customers (legal entities and individuals) and are stored by the employee of the Internal Control Service.

4.8. Application form of the customer profile is stored for at least five years from the date of terminating relations with the customer.

4.9. Information on transactions, as well as information on the identification and materials related to customer due diligence must be stored within the terms established by the legislation, but after performing transactions or terminating business relations with a customer - at least for 5 years.

4.10. As the information specified in the application form of the customer changes, as well as changes in the nature of financial transactions, officers of the Internal Control Service should review the risk level of working with such customers.

4.11. The information received as a result of customer due diligence and identification, while admitting a high level of risk of money laundering and the financing of terrorism is reviewed by the officers of the Internal Control Service at least once a year and the relevant information is recorded in the customer's application form.

4.12. During the review process, the customer, whose risk level of money laundering and the financing of terrorism is admitted as high can be excluded from the category of high risk in the following cases:

a) if business relations with customers are terminated;

b) if a year has passed since the date of the last transaction of the customer or change of information about the customer.

4.13. If the conditions specified in clause 4.12. are executed, but there is a risk of money laundering and the financing of terrorism, then this customer remains in the category of customers with a high risk level.

4.14. The information received as a result of an adequate examination and identification of customers with a low risk level money laundering and the financing of terrorism should be reviewed by responsible employees once every three years.

4.15. Regardless of the customer's risk level, when a change in the customer's information occurs, the responsible employees must record the changes not later than the day after receiving the information about the change.

4.16. The information received as a result of due diligence of customers who have made one-time transactions is updated the next time a transaction is made that requires undertaking adequate customer due diligence measures.

4.17. Managers and responsible employees of the bank limit access to the information related to countering money laundering and the financing of terrorism including documents stored in the archives of a commercial bank and ensure its non-disclosure.

4.18. Employees of the bank have no right to inform legal entities and individuals on the provision of the data on their transactions to a specially designated public authority.

4.19. It is strictly forbidden to disclose (or use for personal purposes or in the interests of third parties) the information received in the process of performing internal control assignments by the head of the bank and the responsible employees. Only cases specified in the Internal Control Rules constitute exceptions.

4.20. Providing the third parties with the information including the information constituting customer identification is executed in compliance with statutory documents.

4.21. With the aim of formalizing the measures undertaken, in compliance with the requirements of the Internal Control Rules employees of the Internal Control Service are provided with special journals.

4.22. A special journal must be stitched, numbered and on its reverse side it must contain the information on number of pages, the date (day, month, year) of the beginning of the journal. This journal must be signed by the head of the Internal Control Service.

5. Control over violation of statutory documents related to money laundering and the financing of terrorism

5.1. The head of the Internal Control Service and employees exercise overall control over the violation of statutory documents related to money laundering and the financing of terrorism in compliance with the Charter of the Internal Control Service and the job description.

5.2. If a violation of statutory documents related to money laundering and the financing of terrorism is detected, or if there is information about it, all employees of the Internal Control Service must report to head of the Internal Control Service in a written form.

5.3. The information must specify the name of the violated statutory document, the content of the violation of the statutory document, the surname, name, patronymic and position of the employee who committed the violation of the law and the date of violation of the statutory document. Information in electronic form must be sent via the IBM Lotus program to the e-mail address of the head of the Internal Control Service or submitted in person in a written form.

5.4. In compliance with the information provided the head of the Internal Control Service performs the following functions:

a) examines information on violation of the law and performs an inspection in case of necessity;

b) clarifies the reasons for violating the law;

c) receives an explanatory note from an employee who committed a violation of the law;

d) submits a staff report to the Chairman of the Executive Board to consider the issue of undertaking relevant actions against the employee who committed the violation;

e) undertakes measures to eliminate violations, errors and omissions;

f) undertakes other measures stipulated by the statutory documents.

6. Requirements for training and education of the personnel

6.1. With the aim of providing the bank employees with the information on modern methods and ways of money laundering and the financing of terrorism, clarifying statutory documents related to money laundering and the financing of terrorism and all aspects of tasks training sessions are held in the following order:

a) Classes on economics;

b) Seminars;

c) Internal trainings on qualification upgrading;

d) Advanced training at special courses located in the republic;

e) Participation in training sessions of foreign countries.

6.2. Classes on economics are held at the head office of the bank and its branches at least once a quarter.

6.3. The topics for the classes on economics for the next year are provided to the Training and Development Department on the basis of the staff report of the head of the Internal Control Service and included in the annual curriculum.

6.4. Learning materials on classes on economics should be provided by the Internal Control Service to the Training and Development Department 10 days before fixing the date of the classes on economics.

6.5. At branches, economic training classes are held by the head of the Internal Control Service, at the head office - by the Head of the Internal Control Service (or an employee entered in the internal trainer's reserve staff).

6.6. On the initiative of the head of the Internal Control Service, the topic of explaining the requirements of statutory documents related money laundering and the financing of terrorism can be included in the plan of seminars held in various areas of the banking activities. The training program is approved by the Chairman of the Executive Board of the bank. This program should be include the following aspects:

a) the procedure for holding classes, its form (primary instruction, planned and unscheduled training) and terms;

b) the appointment of persons responsible for organizing the classes;

c) the procedure for examining the knowledge of employees.

6.7. Changes in the legislation related to the CMLFT as well as the changes related to the internal rules of the bank and other bank documents should be communicated to the employees at training seminars.

6.8. Test questions created to test learning materials and knowledge of employees are placed electronically in the "Moodle" program. Employees can freely use training materials and answer test questions.

7. Criteria for suspicious and shady transactions, the procedure for their identification and representation.

7.1. Transactions associated with cash or other property, if they have one of the following criteria and indications are admitted as "**suspicious transactions**".

1) the bank has assigned a high risk level to a transaction or a customer who performs this transaction;

2) systematically performed the of the previously received amount return by the resident customer in favor of a non-resident under the contract for the supply of goods (performance of works, provision of services);

3) the documents submitted for performing a transaction raise doubts on their authenticity (reliability), and (or) information on the transaction including on one of its parties, does not correspond to the information available at the bank;

4) unusual behavior of the customer when submitting an application form (instruction, petition) to perform the transaction, for example: nervousness, uncertainty, aggression with simultaneous presence of persons guiding the customer's actions, or his phone call to other persons for advice on an insignificant matter;

5) unusual concerns of the customer on confidentiality or unreasonable refusal or unjustified delays in the submission of information about the transaction requested by the bank by the customer;

6) impossibility of identifying partners of the customer on the transaction performed;
7) a transaction does not have a precise economic sense and does not correspond to the nature and type of the customer's activity;
8) unreasonable increase of cash turnover on the customer's account which is nor associated with the nature of its activities and (or) occurred after more than a three-month period of low activity or the absence of signs of activity on the customer's accounts;
9) unreasonable and (or) pre-schedule termination of business relations on the initiative of the customer accompanied by the withdrawal or transfer of all funds to other commercial banks;
10) instant termination of business relations on the initiative of the customer after the bank undertakes reasonable measures stipulated by the Internal Control Rules;
11) obvious non-compliance between the transactions performed by the customer with the participation of the bank and the generally accepted practice of making transactions;
12) unjustified splitting of the amounts of similar transactions performed by the customer;
13) settlement procedure contains non-standard or unusually complicated schemes that differ from the customer's usual activities;
14) making significant amendments regarding the direction of cash flow or other property by the customer in the previously agreed scheme of performing the transaction immediately before the commencement of its implementation;
15) exchange of banknotes of one denomination into banknotes of another denomination by an individual for an amount equal to or higher than 500-fold the minimum wage established on the day of exchange;
16) making a deposit by an individual in cash of an amount equal to or higher than 500-fold the minimum wage on the day of performing the transaction to the bank account of a legal entity or an individual entrepreneur as borrowings, loans, financial assistance, contribution to the Charter fund (capital) ;
17) the transfer of funds as grants, financial assistance, loans or gratuitous assistance by the non-resident to the resident except for the transactions performed by decisions of the authorized public administration authorities of the Republic of Uzbekistan;
18) transfer from the accounts of legal entities or individual entrepreneurs of funds in the amount equal to or higher than 500-fold the minimum wage on the day of performing the transaction, as financial assistance or a loan;
19) transfer of funds from accounts of legal entities or individual entrepreneurs to accounts of individuals for an amount equal to or higher than 500-fold the minimum wage on the day of performing the transaction, as dividends;
20) withdrawing cash from an individual's account in the amount equal to or higher than 500-fold the minimum wage on the day of performing the transaction;
21) the customer's appeal for withdrawing cash previously received in his account within a period not exceeding 3 banking days from the date of receiving in the amount equal to or higher than 100-fold the minimum wage;
22) performing transactions (payment or cash withdrawal) from five or more international payment cards within one day at the terminal of one counterparty, when the amount of transactions with each card is equal to or exceeds 25-fold the minimum wage.

7.2. Transactions associated with cash or other property, if they have one of the following criteria and indications are admitted as a "**shady transactions**":

1) one of the parties of the transaction is a permanent resident, resided or registered in the country which does not participate in international cooperation in the area of countering money laundering and the financing of terrorism;

2) receiving money transfers sent from abroad or sending money to foreign countries by individuals in foreign exchange including through money transfer systems, for a total amount equal to or higher than 500-fold the minimum wage, one-time or several times over a period not exceeding 3 months;
3) sale or purchase by individuals of funds in foreign exchange in the amount equal to or higher than 500-fold the minimum wage, one-time or several times over a period not exceeding 3 months;
4) transfer of funds outside the Republic of Uzbekistan to the account opened for an anonymous owner, and cash inflow into the Republic of Uzbekistan from the account opened for an anonymous owner or in case of absence of information on the sender;
5) transfer of funds outside the Republic of Uzbekistan to the recipient's account opened with a bank registered in an offshore zone different from the place of the beneficiary registration;
6) funds are transferred outside the Republic of Uzbekistan to accounts or for the benefit of persons permanently residing or registered in offshore zones, or are entered the Republic of Uzbekistan from the accounts of such persons at one time or several times within 30 days for a total amount equal to or higher than 500-fold the minimum wage established on the day of the last transfer (receipt);
7) transactions with non-resident customers, information about the founders of which is not available and impossible to obtain it by all available methods;
8) cash withdrawal or payment for goods (services) in the amount equal to or higher than 100-fold the minimum wage accomplished within 30 days using a bank plastic card in active combat zones or controlled by terrorist organizations or in the areas directly adjacent thereto;
9) a transaction associated with the use of cash or other property to which access is available including an attempt to perform it;
10) other transactions that do not have the criteria and indications stipulated in this clause established by these Rules and the internal rules of a commercial bank, in respect of which there are suspicions of involvement in money laundering and/or the financing of terrorism.

7.3. A list of countries which do not participate in international cooperation in the sphere of countering money laundering and the financing of terrorism is compiled by the Department and enters into force upon the date of its official publication.

7.4. A list of offshore territories and countries includes the territories and countries specified in the Charter, registered by the Ministry of Justice of the Republic of Uzbekistan under № 2467 "Regulations on the procedure for monitoring over the validity of foreign exchange transactions by legal entities and individuals".

7.5. Identification of customers and current examination of their transactions are executed by employees who directly render service to customers (executives, cashiers, and the others).

7.6. The Internal Control Service daily detects shady and suspicious transactions and prepares reports through the "Internal Control" and the "Bank Reporting System" programs.

7.7. Subsequent examination of the customer's transactions is executed by employees of the branch's Internal Control Service through the analysis of transactions performed by the customer during the past period with the aim of detecting shady transactions that were not revealed in the process of the current examination.

7.8. When detecting suspicious and shady transactions, in case of necessity, branch employees directly serving customers on behalf of the Internal Control Service (or the Internal Control

Officer in the branch), contact the customer regarding additional information about the transaction.

7.9. Employees of the branch's Internal Control Service study the information on the customer and transactions, record relevant information in a special journal and the application form of the customer, and, if there are sufficient reasons make a proposal to the head of the Internal Control Service on classifying a suspicious transaction as a shady transaction.

7.10. If there are reasonable doubts, the head of the Internal Control Service decides on admitting a suspicious transaction performed by a customer as a shady transaction and in addition informs the Chairman of the Executive Board of the bank thereof. This decision is made in writing and signed by the head of the Internal Control Service. Information on a suspicious transaction admitted as shady is submitted to the specially designated public authority according to the procedure established by the legislation.

7.11. Admitting of a suspicious transaction as shady in each certain case is executed on the basis of a comprehensive analysis with the application of criteria and characteristics determined by the Internal Control Rules.

7.12. When performing comprehensive analysis of transactions, employees of the Internal Control Service should pay a particular attention to the following aspects:
a) the territory (state) of the registration of the transaction participants;
b) the frequency and number of transactions similar to that performed by the customer;
c) the complexity of the transaction;
d) the content of the transaction and its compliance with the documents that constitute the basis for its performance;
e) information obtained as a result of the customer due diligence;
f) basic partners of the customer.

7.13. With the aim of detecting shady transactions, the Internal Control Service of the bank's head office may introduce reports, assign inspections and execute thereof by the employees of the Internal Control Service.

7.14. After admitting the customer's transaction as shady, the Internal Control Service should undertake the following measures:
a) inform specially designated public authorities about the shady transaction;
b) obtain additional information about the customer;
c) reconsider the risk level of the customer;
d) intensify monitoring of the customer's transactions;
e) make a proposal to the Chairman of the Executive Board of the Bank on termination of the contractual relationship with the customer in compliance with the law and the contract concluded thereto.

7.15. In compliance with the established procedure the report on a shady transaction is submitted to the specially designated public authority appointed by the Cabinet of Ministers of the Republic of Uzbekistan not later than the next business day upon the date of its receipt.

7.16. Reports of shady transactions are preliminary prepared by an employee of the Internal Control Service of the branch and transferred through the Lotus Notes program to the Internal Control Service of the bank's head office. The Internal Control Service of the head

office of the bank gathers messages from all branches, examines them, adds in the list and sends them to the Department in an electronic form.

7.17. Information on each report is recorded in a special journal of the Internal Control Service by the officer of the Internal Control Service of the branch.

7.18. On the daily basis the Internal Control Service compiles in paper form the information about the transferred reports to the specially designated public authority indicating all the information from the electronic message. This table must be signed by the performer and approved by the head of the Internal Control Service. When transferring an electronic message sent to the specially designated public authority into the paper, it is certified by the signature of the head of the Internal Control Service.

7.19. Each information confirming the suspiciousness of the transaction is to be instantly reported to the specially designated public authority.

8. The procedure for identifying transactions of persons included in the List and instant suspending the transaction and (or) freezing funds or other property without their prior notification

8.1. Employees who directly render services customers in carrying out their transactions are obliged to verify the received information with the List.

8.2. In case of full compliance of the identification information of the customer or one of the participants in the transaction with the information of the person included in the List, the employee who renders services to the customer must instantly suspend the transaction without prior notification (except for transactions on crediting funds received to the account of a legal entity or an individual) and notify the employee of the branch's Internal Control Service in writing.

8.3. Employees who render services to customers must suspend the transaction under the following cases:

- if one of the participants in the transaction acts on behalf of the person included in the List or at his instruction;
- if the funds or other property used in performing the transaction is partially or fully owned by the person included in the List;
- if the participant of the transaction is a legal entity owned or under control of the person included in the List.

8.4. In compliance with the identification information the employee of the Internal Control Service of the branch re-examines the case of compliance, and if full compliance is not established, permits the transaction.

8.5. If the employee of the Internal Control Service confirms full compliance, the relevant information on the customer and the transaction are recorded in a special journal and an application form of the customer, and in turn, in the electronic software "Money Oper" and then immediately reported on the same day electronically to the Internal Control Service of the head office of the bank.

8.6. The Internal Control Service of the head office of the bank undertakes the following measures immediately and without a prior notification in relation to the suspended transaction:

- detailed identification of the customer's personality, the beneficiary owner of the customer or one of the participants of the transaction to the possible extent;
- detecting funds or other property on the transaction to be frozen in compliance with the requirements of the law and these Rules;
- preparation and submission of the instruction to suspend the transaction for signature of the management of the bank, except for transactions on crediting funds received to the account of a legal entity or an individual, and freezing of funds or other property by such a transaction;
- preparation of the report on a suspicious transaction specifying the amount of frozen cash or other property and sending it to a specially designated public authority on the day of its suspension;
- receiving additional information on the customer (including type of activity, amount of assets, information available through open databases, etc.);
- determining the source of funds or the source of the customer' financial condition including by receiving the information from the customer;
- entering the information on the transaction in a special journal.

8.7. The received instruction of the Internal Control Service to suspend transactions associated with the cash or other property must immediately be executed by all subdivisions responsible for performing the function of suspending (blocking) transactions related to accounts and writing off funds from accounts on the basis of the customer's instruction.

8.8. The Internal Control Service maintains a separate journal for recording instructions of customers whose transactions are suspended. The information about the suspended transaction and the information that enables identifying the participants in this transaction is recorded in such a journal.

9. The procedure for identifying, assessing, monitoring, managing, reducing and documenting the risks

9.1. The risk in the sphere of money laundering and the financing of terrorism supposes the activities of the bank to manage these risks, assess these risks and activities on their reduction. Risk management is based on a risk based approach.

9.2. The system of assessing the level of risks in the sphere of money laundering and the financing of terrorism of a bank includes the following risks:

a) customer's actions performed with the aim of money laundering and the financing of terrorism;

b) the risk of attracting the bank and its employees into money laundering and the financing of terrorism.

9.3. According to this assessment program, the level of risk is divided into "low" and "high". In terms of risk, measures undertaken in relation to the customer and transaction are executed in the following form:

a) standard measures in relation to customers and low-risk transactions in the sphere of counteracting money laundering and the financing of terrorism;

b) enforced measures in relation to customers and high-risk transactions in the sphere of counteracting money laundering and the financing of terrorism.

9.4. Employees of the Internal Control Service determine the risk level of customers and transactions and conduct their monitoring.

9.5. Risk assessment is executed in relation to all customers including with respect to customers performing one-time transactions without opening bank accounts.

9.6. The risk of money laundering and the financing of terrorism of customers is recorded in their identification application forms.

9.7. With the aim of reducing risks in the process of distant customer service, the Internal Control Service supervises the introduction of the requirements of the Internal Control Rules for countering money laundering and the financing of terrorism at commercial banks №2528 in contracts for rendering such services.

10. The procedure for maintaining and monitoring customer accounts classified as high risk, as well as monitoring the transactions of such customers

10.1. The Internal Control Service is obliged to refer the customers to the category of high risk level who initially meet the following criteria and which deserve a particular attention:

a) the persons included in the List are either owned or controlled by the person included in the List, either directly or indirectly owning or controlling the agency included in the List;

b) persons permanently residing, staying or registered in the country which does not participate in international cooperation in the field of countering money laundering and the financing of terrorism;

c) representative offices of foreign companies and individuals who are not citizens of the Republic of Uzbekistan;

d) persons permanently residing or registered in the offshore zone;

e) residents and non-residents who have accounts in offshore zones;

f) agencies and individual entrepreneurs whose actual location does not correspond to the information specified in the constituent or registration documents;

g) agencies and individual entrepreneurs whose activity period does not exceed one quarter of a financial year;

h) agencies the beneficial owner of which is the person referred to in subclauses “a” and “b” of this clause;

i) customers performing suspicious or shady transactions on the constant basis (for example, for 3 consecutive months);

j) customers using software systems that exclude the possibility of proper customer due diligence;

k) public officials and members of their families;

l) persons whose beneficial owners permanently reside are located or are registered in the offshore zone.

10.2. The Internal Control Service is obliged to refer the transactions to the category of high risk level who initially meet the following criteria and which deserve a particular attention

a) transactions which participants are the persons referred to in subclauses “a”, “b”, “h” and “k” of clause 10.1 of these Rules;

b) transactions performed through accounts opened in offshore zones;

c) transactions with precious metals, precious stones, as well as jewelry containing precious metals and precious stones except for the transactions performed commercial banks themselves;

d) transactions related to money transfers in which the information about the sender (last name, first name and patronymic of individuals, full name of legal entities, location (postal address) and the number of the sender's account) are not fully presented.

10.3. When referring a customer performed by a customer to a high-risk category, the Internal Control Service should apply enforced due diligence measures towards such a customer.

10.4. The employees of the Internal Control Service of the branches keep accounts of all customers included in the high-risk category and submit them in the form of a report to the Internal Control Service of the head office of the bank.

10.5. The information on referring the customer in the category of risk and content of risk is recorded in the identification application forms of customers referred to the category of high-risk level. The application form is formalized in a paper-form and kept by an employee of the Internal Control Service.

10.6. The information received as a result of proper verification and identification of a customer, in case of recognizing the risk level of money laundering and the financing of terrorism is recognized and in case of change when of the customer's information should be updated at least once a year, in other cases at least once every three years.

11. The procedure for entering into business relations with public officials and their close relatives and comprehensive monitoring of their transactions.

11.1. If a customer or his beneficiary owner is a non-resident in the process of customer due diligence, a responsible officer applies to the employee of the Internal Control Service to clarify whether he is referred to the category of a public official or not.

11.2. In turn, an employee of the Internal Control Service reports the application of the responsible officer to the Internal Control Service of the head office of the bank. The Internal Control Service of the head office of the bank examines the person listed in the application through special software with a list of public officials and the results of this inspection are reported to the responsible officer.

11.3. If the customer or its beneficiary owner is a public official, with the aim of receiving the permission to enter into business relations with the customer, the head of the Internal Control Service contacts the Chairman of the Executive Board or his deputy and informs the branch on the decision of the Chairman of the Executive Board or his deputy.

11.4. Prior to receiving a written permission from the Chairman of the Executive Board or his deputy, the branch suspends its activity of entering into a business relationship with this customer.

11.5. If the customer or his beneficial owner is a public official, the employees of the Internal Control Service of the branch must undertake the following additional measures in relation thereto:

a) verification of the information on the status of a public official and other measures to identify sources of funds and other property in the transaction performed;

b) arranging activities on receiving the permission to enter into business relations with a public official from the Chairman of the Executive Board or his deputy;
c) regular implementation of comprehensive monitoring of business relations.

11.6. Public officials and their close relatives, as well as transactions performed thereto are included in the high-risk category by the Internal Control Service and enforced measures of due diligence are also applied thereto.

12. Execution of the Department request

12.1. A specially designated state authority has the right to request and receive free of charge the information required for the implementation of measures on CMLFT including from the automated information and reference systems and databases of the bank.

12.2. The Department's requests are executed in compliance with the procedure established by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 272 as of October 12, 2009 "On improving the procedure for providing information related to counteracting money laundering and the financing of terrorism" and additional information is provided.

12.3. The response to the Department's requests is prepared in writing in official forms and signed by the Chairman of the Executive Board (or his deputy), the head of the Internal Control Service and the employee who has prepared the information.

12.4. If the requests do not imply other requirements, the response letters are sent in an envelope via mail to the address specified in the request.

12.5. The Internal Control Service is responsible for providing timely and complete responses to requests.

12.6. To execute the requirements of requests, the Internal Control Service has the right to receive the data from the relevant subdivisions and information databases.

13. Measures undertaken to prevent the use of technological achievements with the aim of money laundering and the financing of terrorism

13.1. The Internal Control Service should determine the risk associated with the development of new types of services and new business practices using advanced technologies for new and existing types of services, assess it and report it to the management of the bank.

13.2. Subdivisions introducing new types of services or new technologies in cooperation with the Internal Control Service should undertake appropriate measures to monitor and reduce the level of these risks, provide information on the results of the measures undertaken to the Executive Board of the bank.

13.3. If it is not possible to monitor, reduce or prevent the risks associated with the introduction of new types of services or new technologies, the Internal Control Service has the right to submit a staff report the suspension of the use of a new type of service and a new technology until these drawbacks are eliminated.

13.4. The Executive Board of the bank should undertake measures to prohibit the use of technologies that cannot meet the requirements of statutory documents on countering money laundering and the financing of terrorism.

14. Measures undertaken in detecting money transfers in foreign exchange in case of absence of the required information about the recipient and (or) sender

14.1. When performing international money transfers including when making transactions through the international money transfer system, the director of the Retail services department and the head of the “Money transfer and non-commercial activity” division should ensure the following:

a) maintaining an account of the divisions rendering international money transfer services (stations, branches, etc.) and employees of these divisions;

b) implementation of transactions related to money transfers after proper verification of customers - individuals;

c) ensuring sending of funds with accurate information about the sending customer (last name, first name, patronymic, if any), with an identity document (passport or the document used in lieu thereof), series and number; if an account is used during the transaction - its number or the number associated thereto and information about the recipient (last name, first name, patronymic, if accurate information is available);

d) the requirement to provide the minimum information (last name, first name, patronymic, if any) about the senders of money transfers from non-resident banks and international money transfer systems of the amount not exceeding 25-fold the minimum wage, if accounts are used during the transaction, provision of their numbers or the inherent number of the transaction;

e) the requirement to provide minimum information (surname, name, patronymic, if any) about the senders of funds from non-resident banks and international money transfer systems equal to or over 25-fold the minimum wage; identity document (passport or the document used in lieu thereof); sender’s address or date and place of birth; if accounts are used during the transaction - then provision of their numbers or the inherent number of the transaction.

14.2. Employees performing transactions on international money transfers must verify the availability of the required information about the recipient and/or the sender (counterparty) of funds, in the absence of the required information they must refuse the customer to perform the transaction.

14.3. Employees of the Internal Control Service of the branch when performing money transfer transactions, monitor the availability of the required information about the recipient and (or) sender (counterparty) of funds, in particular, the presence of the last name, first name and patronymic of the transaction participants.

14.4. The Internal Control Service of the head office of the bank has the right to make a proposal to suspend the transaction of international money transfer, if the information about the beneficiary and (or) sender is not provided or not provided to the full extent.

15. Final provisions

15.1. The Executive Board and the Council of the Bank, taking into account external and internal circumstances, assess the efficiency of the bank's Internal Control Service, and, if necessary, undertake relevant measures to improve its efficiency.

15.2. The Internal Audit Service, when conducting internal audit at the bank branches monitors the efficiency of the Internal Control System of the bank and its branches.

15.3. Drawbacks of the Internal Control System detected by the Internal Audit Service or other control services are promptly communicated to the Chairman of the Executive Board and the Council of the bank. After receiving such information, the Chairman of the Executive Board and/or the Council of the bank should ensure timely elimination of the detected drawbacks.

Head of working group:

Director of the Department on Managing branches: **A. Perpiyev**

Director of the Risk management department: **M. Arslanov**

Member of working group:
Chief accountant **N. Irgahev**

Head of the Internal Control Service **Kh. Yuldashev**

Head of the Legal service department **K. Teshaboyev**

Head of the sector on of operation risk and fraud risk management **D. Madrakhimov**

Leading specialist of the department of standards and business processes (business processes management **O. Yusupov**

Secretary of the Commission: **N. Israilova**