ASIA ALLIANCE BANK

Money Laundering and Sanctions Program:

Sanctions verification procedure

Tashkent - 2024

Abbreviations :	
Bank	"ASIA ALLIANCE BANK" ATB
AML	Fight against money laundering
TF	Terrorism financing
FPWMD	Financing the proliferation of weapons of mass destruction
Central Bank	Central Bank of the Republic of Uzbekistan
SASB	The Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan
KYC	Know your customer
IRM	Internal referral message
List	The list of persons participating or suspected of participating in terrorist activities or distribution of weapons of mass destruction compiled by a specially authorized state body on the basis of the information provided by the state bodies and other authorized bodies of the Republic of Uzbekistan, which fight against terrorism and the proliferation of weapons of mass destruction, as well as information provided through official channels from the competent authorities of foreign countries and international organizations
ROBS	Regional Banking Services Office
Field of activity	Employees responsible for providing customer service and carrying out customer banking transactions, including managers
Internal and external regulatory documents:	
The Law of the Republic of Uzbekistan "On Banks and Banking Activity";	
The Law of the Republic of Uzbekistan No. 660-II of August 26, 2004 "On combating the money laundering, the TF and the financing of the proliferation of weapons of mass destruction";	
"INTERNAL CONTROL RULES on Combating Money Laundering, TF, and Financing of Proliferation of Weapons of Mass Destruction in Commercial Banks" registered in the Ministry of Justice of the Republic of Uzbekistan on May 23, 2017 with No. 2886.	
Regulation "On the procedure for suspending the operations of persons included in the list of persons participating or suspected of participating in terrorist activities or the proliferation of weapons of mass destruction, suspending funds or other property without using it, allowing the use of the suspended property that was not being used , and resuming operations" registered in the Ministry of Justice of the Republic of Uzbekistan on October 19, 2021 with No. 3327	
Regulation "On the procedure for monitoring the validity of foreign exchange transactions by legal entities and individuals" registered in the Ministry of Justice of the Republic of Uzbekistan on June 12, 2013 with No. 2467.	

In accordance with the Central Bank's letter No. 23-26/28xfu dated June 23, 2022, Decision of the Central Bank of the Republic of Uzbekistan No. 14/3 dated June 18, 2023 "On improving the effectiveness of the risk management system related to financial sanctions in banks".
According to the letter of the Central Bank dated August 8, 2022 No. 23-26/38xfu "COPY from the minutes of the meeting held at the Central Bank of the Republic of Uzbekistan on August 3, 2022".
In accordance with the Central Bank's letter No. 23-26/2xfu dated January 10, 2023 "Central Bank of the Republic of Uzbekistan Management Decision No. 30/6" on the state of risk management related to economic sanctions and export bans in the banking system in 2022 Extract from December 24.
In accordance with the letter of the Central Bank dated January 23, 2023 No. 23-26/24xfu "Report of the meeting No. 1 on January 6, 2023, held at the Central Bank of the Republic of Uzbekistan on issues related to risk management related to economic sanctions and export bans in commercial banks".
In accordance with the letter of the Central Bank dated October 24, 2023 No. 23-26/99xfu on the "List of goods of general high priority importance, prohibited for export to Russia by the European Union and its allied countries" dated September 20, 2023 No. Ares 2023) extract No. 6374481.

1. General analysis

This charter of "ASIA ALLIANCE BANK" (hereinafter referred to as the Bank) is aimed at identifying and preventing the legalization of proceeds from criminal activities, the financing of terrorism, the distribution of weapons of mass destruction, and criminal activities. Adherence to international standards for combating money laundering, financing of terrorism and proliferation of weapons of mass destruction announced by the Special Group on Bank Financial Actions ("FATF 40 Recommendations"), sanctions restrictions adopted by the United Nations developed the Sanctions Compliance Program. The Bank adheres to the sanctions and restrictions adopted by the United Nations ("UNSC"), the Specially Authorized State Body of the Republic of Uzbekistan ("SASB"). Also, based on Central Bank directives and Decisions, the European Union ("EU"), the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the United Kingdom's Office of Financial Sanctions Enforcement ("OFSI")) and apply sanctions and restrictions adopted by other international jurisdictions. This Regulation of the Bank is intended to regulate its day-to-day Sanctions compliance activities and applies to all its constituent structures. The purpose of the sanctions compliance program is to prevent misuse of the Bank and (or) its products and services to bypass relevant sanctions programs.

According to the instructions and decisions of the Central Bank

1.1. Related internal regulatory documents

This Regulation should be read together with the following internal regulatory documents:

- ✓ The Bank's Anti-Money Laundering and Sanctions Policy;
- ✓ Regulation of the Bank's Compliance-control Department.
- ✓ Bank's Know Your Customer ("KYC") Procedure
- ✓ The Bank's Transaction Monitoring and Reporting Procedure ("TM");
- ✓ Bank's Risk Assessment ("RA") Procedure;

2. Purpose

The Bank strictly observes all applicable economic and trade sanctions. Among other things, all employees of the Bank must comply with all applicable laws, rules and regulations adopted and enforced by the relevant competent authorities, as well as the Bank's internal regulatory documents. Failure to comply with applicable laws and internal regulatory documents may result in criminal and civil liability and may pose a risk to the Bank's reputation.

"Sanctioned Parties" countries, individuals and legal entities, organizations, ships or aircraft, which the Bank is directly or indirectly on or included in the current Sanctioned List, as well as , will not carry out any transactions, transfer or receive funds on prohibited goods and services. The Bank will not carry out any transaction until the end of the current Sanction regime period and (or) until the sanctions of the sanctioned persons, ie individuals or legal entities, are lifted.

The Bank undertakes to comply with the requirements of economic and trade sanctions under:

- Develop a comprehensive Sanctions program, including a Sanctions risk assessment process, management oversight, policies and procedures that identify and control risks within the Sanctions Compliance Program, and appoint qualified Sanctions Compliance Officers;
- Determining personnel and structures responsible for day-to-day compliance with sanctions;
- Implement a Sanctions Compliance process that focuses on Sanctions-related risk areas (eg, list updates, "Misfit");

- Conduct training for employees based on their duties, including jurisdiction-specific sanctions;
- Constant communication with employees, management, regulatory bodies.

This document sets out the requirements and procedures for ensuring compliance with the Sanctions Program.

3. Basic terms

Sanctions

The dictionary meaning of "Sanctions" is an official order (eg, suspension of trade, etc.) issued against a country to ensure compliance with international laws and regulations. In these Procedures, "Sanctions Screening" means the act of identifying a Sanctioned Party and taking appropriate action (such as blocking, freezing, and repudiation) without delay for the Sanctioned Party's funds or other assets. Also, it should be ensured that funds or other assets are not provided directly or indirectly for the benefit of any individual or legal person and organization (hereinafter referred to as Legal Entity) as a result of the imposed sanctions.

Sanctioned parties

A sanctioned party means a specific country, region, individual, legal entity, product, etc., which is prohibited from entering into economic, trade or financial relations with an international or national, government or international organization.

Sanctions program

Clause 6 of the sanctions program. Based on relevant laws and regulations adopted by sanctioned institutions to restrict or prohibit operations with sanctioned purposes.

Sanctions Compliance Program

The Sanctions Compliance Program provides internal controls in terms of operating procedures and standards for compliance with the Sanctions Program.

Sanctions risk assessment

The Sanctions Risk Assessment is a Sanctions Risk Assessment and Sanctions Compliance Program, the results of which are presented in numbers.

Sanctions screening

Sanctions Screening (hereinafter referred to as Screening) is the process of verifying names and other relevant identifying information to determine whether or not a screened party matches any records included in the applicable sanctions.

Sanctions warning

An alert is a potential action that appears during the sanctions screening process and may match a party's designation on the applicable Sanctions List. The notice may or may not fully match the person's designation as a party on the sanctions list and may require further investigation. The Bank will not allow the transaction to be executed until the transaction causing the warning has been reviewed, removed from the account and found to be inconsistent with the designations of the party on the Sanctions List .

Sanctions screening system

The sanction screening system effectively identifies the sanctioned target during the KYC process and transaction execution. **"SWIFT Screening Utility**" , **the IABS (Internal Control Screening)** system and the **World-Check** system are used to screen SWIFT messages and other internal and external transactions.

List of SASB

A specially authorized state body based on the information provided by the state bodies and other competent bodies of the Republic of Uzbekistan, as well as the information provided by the

competent bodies of foreign countries and international organizations through official channels List of persons involved or suspected of involvement in terrorist activities or proliferation of weapons of mass destruction compiled by the Ministry of Defense.

Sectoral Sanctions List (SSI)

Implements sectoral sanctions against certain individuals operating in various sectors of the economy of Russia and Belarus as determined by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC") and publishes their names on the Sectoral Sanctions List (SSI).

List of SDN

This list may include US government-sanctioned terrorists, drug traffickers, individuals and legal entities supporting authoritarian regimes (their beneficiaries), and financial institutions. The Bank does not carry out any transactions with those on the SDN list.

FinCEN United States Financial Crimes Enforcement Network

The mission of the Financial Crimes Enforcement Network is to protect the financial system from illicit use, combat money laundering and related crimes, including terrorism, and the strategic use of financial authorities through the collection, analysis and dissemination of financial information. is to ensure national security.

BIS Bureau of Industry and Security at the US Department of Commerce

To advance US national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting US strategic technology leadership.

4. Responsibility and accountability

This paragraph defines the responsibilities and liabilities of the Bank's employees in terms of the "Sanctions Verification Procedure" (SS).

4.1. Employees of the field of activity

The Employees of the field of activity assume the following responsibilities:

- Sanctions screening;
- Forwarding to employees of Compliance-control department to perform initial analysis and review alerts.

4.2. Deputy manager of ROBS

Deputy managers of ROBS assume the following responsibilities:

- Monitor any risk(s) associated with sanctions against its customers, including re-execution of blocked or denied transactions;
- Respond to requests for additional information and requests from employees of Compliance-control department with detailed comments;
- Send a report on blocked or frozen funds to the head of the Compliance-control Department for review every six months;
- Submit a sanctioned permit or license to the Head of Compliance for review and approval of eligibility and validity;
- Review termination of customer relations in consultation with the Head of Compliance.

4.3. Manager of ROBS

The manager of ROBS assumes the following responsibilities:

- Making a decision on termination of relations with customers in agreement with the head of the Compliance-control department

4.4. Employees of the sanction-compliance department

The Sanctions Compliance Department assumes the responsibilities:

- Review and disposition of alerts escalated by employees of the field of activity;
- Escalate potential valid or unresolved alerts to the Deputy Chief employees of Compliance-control department.

4.5. The head of the sanction-compliance department

The head of the sanction-compliance department assumes the following responsibilities:

- in screening systems automatically monitoring the updated files;
- Review alerts generated by staff and/or the screening system;
- Review any amendments to the laws and regulations relating to sanctions;
- Reviewing warnings raised by sanctions-compliance officers and reporting to the head of the Compliance-Control Department on cases that have been fully confirmed;
- Notify Sanctions-Compliance staff about appropriate actions taken after reviewing and disposing of alerts;
- Control over blocked (frozen) or rejected transactions and notify the head of the Compliance-control Department;
- Providing monitoring statistics related to the Sanctions program to the head of the Compliance -control department;
- Assisting the Head of the Compliance-control Department in performing various tasks related to the Bank's Sanctions Program.

4.6. Head of the Compliance-control Department

The head of the Compliance-control department assumes the following responsibilities:

- The Board having the relevant authority to draft a decision on blocking (freezing) or rejecting operations of persons included in the list of SASB and (or) suspending cash funds or other assets without using them introduction to the chairman or deputy chairman;
- Ensure timely submission of sanctions-related reports to relevant regulatory agencies;
- Liaising with bank regulators and governments regarding sanctions compliance;
- Review of the validity and application of the Permit, License and confirmation of permission to use blocked (frozen) funds;
- Ensure prompt remediation of sanctions-related audit and learning deficiencies;
- To advise the head of the activity on the decision to terminate relations with customers; and
- Conduct quality control audits and report to the Bank's Board;
- Review any changes to laws and regulations related to sanctions.

4.7. Chairman of the board

The chairman of the board assumes the following responsibilities:

- Making a decision on suspending or rejecting operations of persons included in the list of SASB without using them, (or) suspending cash funds or other property without using them.

4.8. Bank Supervisory Board

The Bank Board assumes the following responsibilities:

- Review and discuss sanctions-related reports, including regulatory reporting, pending and denied transactions, sanctions risk assessments, quality control reports, and more.

4.9. Responsibilities of bank employees

The bank, including employees of the Compliance-control Department, managers and employees of other departments, are responsible for violating this Regulation in accordance with the law.

The Bank shall ensure that its payment agents and sub-agents comply with the requirements of this Regulation.

The Bank is responsible for the violation of the requirements of this Regulation by its payment agents and payment subagents.

In the event that evidence of violation of legislation, as well as legal acts in the field of AML, TF and FPWMD by Bank employees in the course of operations becomes known, Bank employees shall immediately report these evidence to the Compliance-control Department. they deliver to their manager or employees in writing.

5. List of sanctions

Sanctions list means a list of sanctioned parties, including a specific country, region, financial institutions, legal entities, individuals, goods, services, etc., with which economic, trade or financial relations are prohibited. The bank's list of sanctions consists of lists developed by major international organizations and SASB, as well as an internally developed list.

5.1. List of international sanctions

The list of international sanctions is developed by the following international institutions:

- United Nations Security Council ("UN");
- European Union (“EU”);
- United States Office of Foreign Assets Control ("OFAC") Sanctions List. For specific regulatory requirements related to OFAS *(see Appendix J for additional regulatory requirements of OFAS)* ;
- United Kingdom ("OFSI") Office of Financial Sanctions Implementation;
- Other Sanction Lists applicable to the Bank's activities in a particular jurisdiction.

5.2. List of SASB

The list of SASB - information provided by state bodies and other competent bodies of the Republic of Uzbekistan, engaged in the fight against terrorism, proliferation of weapons of mass destruction, as well as information provided through official channels by the competent bodies of foreign countries and international organizations is established by the Specially Authorized State Body - the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan.

6. Sanction restrictions

In order to prevent the risk of secondary sanctions against the Bank, the Bank prohibits entering into practical business relations with the activities listed below. It also suspends operations for the following types of cases identified during the ongoing review process:

- List of prohibitive sanctions produced and adopted by the United Nations;
- Lists of financial institutions, entities, individuals and other situations produced by the US Office of Foreign Assets Control ("OFAC");
- list of financial institutions, legal entities, individuals and other cases produced by the European Union ("EU");
- A list of financial institutions, legal entities, individuals and other situations produced by the United Kingdom's Office of Financial Sanctions Implementation ("OFSI");
- List of individuals produced by the Bureau of Industry and Security (“BIS”) of the US Department of Commerce;
- Guidelines implemented by the US Financial Crimes Enforcement Network (“FinCEN”);

- export, import and re-export of **goods used in the military sphere to the Russian Federation, Belarus and "Transit countries" (as declared by the "FinCEN" organization)** as part of contracts concluded with foreign enterprises ;
- export and re-export of **dual-purpose goods to the Russian Federation and Belarus** as part of contracts concluded with foreign enterprises ;
- **dual purpose** goods to "Transit countries" (as declared by FinCEN) as part of contracts concluded with foreign enterprises is allowed, but in the following cases:
  - if the goods are imported for use in the territory of the "Transit State" (information about the " final consumer " of the goods from the customer, study of the customer's activities);
  - if the goods are imported for sale to another enterprise located in the territory of the "Transit State" (information from the customer about the " final consumer " of the goods, study of the activities of the customer who buys the goods, and the seller and buyer o contract between');
- Export of goods to the Russian Federation and Belarus prohibited by the US Department of Commerce's Bureau of Industry and Security ("BIS") from EU and US jurisdictions and "branded" goods from these territories' enterprises;
- **Re-export** operations carried out to the Russian Federation, Belarus and "Transit countries" where there is no opportunity to study by Compliance-control officers ;
- Goods produced in the Republic of Uzbekistan that correspond to the goods code in the Commodity Code ("BIS") list, if the goods contain more than 25 percent of raw materials (spare parts), equipment and technologies belonging to the United States, are imported into the Russian Federation and export to Belarus;
- and in other cases.

The Bank fully complies with the services and other conditions restricted by the above-mentioned jurisdictions. Also, based on its risk appetite, the Bank may introduce restrictions or mitigations based on the orders of the Bank's Management.

For detailed information on servicing foreign trade contracts in relation to goods subject to restrictions/prohibitions on export, re-export and transit of foreign states to an embargoed country, see Appendix A.

7. Sanctions Verification Process (Screening)

Sanctions review is one of the primary control tools used by the Bank to ensure compliance with applicable sanctions laws and regulations. Sanctions checks include checking names and other relevant identifying information for any applicable sanctions.

The Compliance Oversight Office is responsible for establishing and communicating minimum audit requirements to ensure consistency in the Bank's sanctions review process.

7.1. KYC Sanctions Verification Process

The Bank must check all customers, including prospective customers, against the applicable Sanctions List to ensure that they are not a Sanctioned Party. Sanctions checks must be conducted before establishing customer relationships and opening accounts. Related parties of customers who are legal entities (representatives, beneficial owners, authorized signatories, etc.) and partners of legal entities should be checked against the Sanctions List.

7.2. Transaction Sanctions Review Process

When the bank initiates incoming or outgoing transactions, it uses an automated verification system to verify these transactions before they are executed. All transactions, including SVIFT messages, are automatically verified through the interface between the Payment System and the Sanctions Verification System. Transaction parties and payment purposes of transactions are checked against the Sanctions List. Transactions that potentially qualify or are confirmed eligible

for the Sanctions List may not be amended, reversed or reversed, but must be reviewed and disposed of in accordance with the *Notice Management process in Section 9* .

7.3. Review process for trade-based sanctions

The Bank verifies its customers and business partners, as well as contractual goods and services, using an automated verification system before the transaction takes place. Transactions will not be carried out until it is confirmed that these goods and services are not under sanctions.

7.4. Other sanctions review process

The Bank uses the Watch List filtering system to check its employees, trade partners. The Compliance Oversight Office shall obtain the information of employees and business partners in accordance with the inspection requirements and conduct a Sanctions inspection in accordance with this Procedure. Therefore, all employees of the Bank should be alert to sanctions risks and be aware of red flags during their work.

8. Red flags

All employees of the Bank to prevent, identify and report any activity or information related to Sanctions, including alerts arising through Red Flags, to the head of the activity area and the Department of Compliance to prevent, detect and report sanctions. is responsible.

Sanctioned activity can be determined in several ways. Therefore, the Bank defines Red Flags based on the Bank's direction, activity and volume of customers, as well as on the basis of the sanctions risk approach, in order to identify transactions related to sanctioning situations by customers.

The Bank, based on its *sanction risk approach,* finds out that one of the following criteria and symptoms is present, these cases are defined as sanction "Red Flags":

1. Customers who use trade corridors that serve as shipping points for export to Russia and Belarus by sea;
2. Purchases new ships for economic or business purposes or for use in cargo corridors involving one or more shipping countries identified;
3. Reluctance of the customer to provide information about the end user of the goods being exported or imported, including the unwillingness to fill out the end user form;
4. Customer's use of IP addresses inconsistent with location information;
5. Payment originating from a third party country not specified in the End User Statement or other applicable End User Form;
6. Using personal email addresses instead of company email addresses;
7. Transactions involving organizations that do not exist on the Internet or do not exist at all;
8. A late change of activity inconsistent with the customer's history or business practices;
9. Inclusion of citizens of Russia or Belarus in the controlling share of the company's shareholders;
10. Entry of citizens of Russia or Belarus into the management of the enterprise;
11. Goods without HS code;
12. Contracts where the HS code does not correspond to the brand name;
13. Funds from transit countries on prohibited (BIS) goods;
14. Funds from all countries on dual-purpose goods;
15. Foreign trade transactions where commodity prices are much higher than the average price.

Compliance-control department can change, add and cancel red flags based on the geopolitical changes taking place in the world and new sanctions packages expected to be introduced by international organizations.

9. Sanction increased due diligence

When the customers and/or their operations are classified as high risk from the point of view of sanctions, the Bank will carry out the due diligence process with enhanced sanctions against this customer and/or his operations *(see section 9.3 of this procedure regarding the types of customers with a high risk level of sanctions).* . Sanction enhanced due diligence consists of measures to collect and study additional documents in order to reduce possible sanction risks.

9.1. Sanction enhanced due diligence process

In the event that the transaction carried out by the customer or the customer is included in the sanctioned high-level risk category, the Bank should take the following enhanced due diligence measures against the customer regarding the foreign trade operations carried out by this customer:

- identification of the beneficial owners of the counterparty ;
- determining the final consumer of goods and services;
- determining the source of funds of the counterparty enterprise;
- studying the activity of the counterparty enterprise;
- study the history of the counterparty;
- study of the chartered fund of the counterparty.

All submitted information must be verified.

Employees of Compliance-control department may request additional information to effectively conduct an investigation.

9.2. Request for additional information (RAI)

Customers with a high level of sanctions risk may request additional information necessary for the purpose of effective investigation of operations carried out with the participation of countries. If the available information is not sufficient to confirm or verify the existence of the counterparty's beneficiary and/or it is not possible to sufficiently study the nature and purpose of the intended transactions, the need for a RAI arises. These requests will be sent to the front office staff.

The following additional information can be requested from the personnel of the ompliance-control department:

- Information about the beneficial owners of the counterparty organization;
- Information on the organizational legal form of the counterparty;
- Electronic web page of the counterparty;
- And information related to another counterparty organization.

Requested additional documents should be submitted within 5 (five) working days. Until the Bank receives the additional information requested from the Customer within the specified period of time, the Customer shall not carry out these foreign trade operations and international payment transactions.

If the customer or transaction participant does not provide or refuses to provide additional documents, the Bank will refuse to carry out such customer's transactions and will consider measures to terminate business relations with the customer.

9.3. Types of customers with a high level of sanction risk

In terms of sanctions, the customers belonging to the category of high risk consist of the following criteria:

a) enterprises whose beneficiary owner is a citizen of the Russian Federation or Belarus;

b) enterprises with a citizen of the Russian Federation and/or Belarus in the management structure (Director and/or Chief Accountant);

c) Customers engaged in foreign trade operations established after February 24, 2022;

d) Export to Russia, Belarus and "transit countries" and enterprises engaged in re-export activities;

e) customers who changed the product HS code;

f) enterprises engaged in the export of dual purpose goods;

g) the presence of sanctioned persons in the amount of less than 50 percent of the share of the enterprise;

h) persons previously associated with the sanctioned person in open sources;

i) customers carrying out foreign trade operations where the prices of goods are much higher than the average price.

High types of sanctions risks may be subject to changes in the high risk category based on geopolitical changes taking place in the world and new sanctions packages expected to be introduced by international institutions.

9.4. Sanction monitoring of high-risk customers

The employees of the Compliance-control Department use the "Transaction Monitoring System" to carry out real-time monitoring of the customers mentioned in paragraph 9.2 of this procedure before foreign trade operations and international payments.

In the process of foreign trade operations and international payments of customers who are in the high risk category in terms of sanctions, the operation will be continued if there are no symptoms provided for in paragraph 6 of this procedure.

10. Manage alerts

10.1. General analysis

Alert Management is the process of ensuring that each alert generated during the Sanctions Review process is properly and consistently identified, reviewed and analyzed for appropriate disposition of the alert prior to entering into a practical business relationship with customers or executing a transaction, and the rationale behind all decisions. is the process of ensuring that it is clearly documented.

Manage alerts:

- Time frame requirements for notification review;
- Standardization of the analysis process;
- Use a consistent basis for posting notices;
- Requests to increase warnings that cannot be verified as not being in compliance with the Sanctions List, as well as any other Sanctions issues that may arise.

After reviewing the Alert, the Bank will dispose of the Alert through one of the following:

- Exact Match: “Exact Match“ occurs when an alert term being checked (eg customer name, date of birth, address or commodity HS codes) is indeed found to be the same as an entry in the relevant Sanctions List. Customers marked as "Fully Eligible" will not be able to perform any transaction, activity or relationship.
- Incorrect Match: A “Mismatch” exists when it is determined that the alert term under investigation is not actually the same as the corresponding Sanctions List entry.
- Unresolved Match: If the review cannot clearly identify a complete match or an incorrect match, it is considered an "Unresolved Match". The Bank shall not execute any transaction until an outstanding match has been fully reviewed and a complete or incorrect match has been determined.

10.2. Create an alert

Alerts can be generated during real-time transaction review, statistical review, and red flag situations. Regardless of the source, each warning should be treated consistently. Once generated, alerts must be reviewed and disposed of by an authorized person.

The Bank will not carry out any transaction or offer products or services to any individual or legal entity in accordance with the national and international sanctions list until the sanctions review is completed and any Notices are duly reviewed and non-compliance is identified with the exception of the transfer of funds to the accounts of individuals and legal entities on the SASB list.

10.3. Review of notices

The Four Eyes principle ensures that Alerts are identified and disposed of correctly and consistently, and that the rationale for all decisions is clearly documented. Each alert generated during a sanctions review is required to be reviewed by two (2) different personnel.

After a first-level review, each alert that is found to be "Fully Compliant" or "Unresolved and Needs Further Review" ("Second-Level Review") will be reviewed by the Chief Compliance Officer or Deputy must be notified.

10.3.1. First class review

After a warning appears during the sanctions review process, employees of the field of activity informs the employees of the Compliance-control Department about the appearance of the warning. Employees of the Compliance-control Department will consider the warning in the following order.

In the event that employees of Compliance-control department determine that the alert is "Mismatched," the alert will be closed and the corresponding transaction may be executed. If employees of Compliance-control department determine that an alert is "Full Compliance" or an "Unresolved Compliance" occurs, this should be documented and reported to the Chief or Deputy Chief Compliance Officer for secondary review.

Employees of Compliance-control department should document the relevant grounds and provide supporting details as necessary to provide detailed information on the alert.

When adding a comment to a notice review, after reviewing the comment, employees of Compliance-control department will consider whether an independent third party can understand the nature of the review performed and the rationale for the filing, and due diligence on the Notice. it should be concluded that it was carried out.

each alert review, there are several elements that can be considered when determining whether an alert is Fully Compliant or Poorly Compliant. The following may be taken into account when deciding whether to give notice.

Country Eligibility

Review the warning text and determine if it is a country name or an authorized geographic region name. If the alert text is the name of a country or a sanctioned geographic region, review the name to determine whether it is a sanctioned country or a region with an applicable Sanctions program. If the employee of Compliance-control department determines it to be "Fully Compliant", this should be reported to the Head of the Compliance-control Department or his deputy and commented on in the Sanctions Review System. If it is "Mismatched", please include the following comment and details to explain the underlying logic:

"Incorrect match: The country name does not match the name of the country on the Sanctions List.

Customer type compatibility

Review the text of the alert and determine if the legal entity related to the alert and the legal entity on the Sanctions List or the Internal List are the same (for example, an individual and an entity). If it is clear that the legal entity type associated with the alert does not match the legal

entity type on the Sanctions List, the alert may be "Mismatched" and comments and relevant justifications for decisions must be entered into the Sanctions Review System:

"The Mismatch: Incompatible Types of Legal Entities".

After verifying that the warning text and the listed person are not the same legal entity type, confirming that there is no additional information related to the warning text and the listed person. For example, even if an entity is not itself an actual Sanctioned Party, an alert may be generated because one of its agents, owners/controllers, acting on its behalf, is a Sanctioned Party. Similarly, an alert will be generated if the funds or other property transacted belong in whole or in part to a Sanctioned Party. Even if the type of Legal Entity does not match, it must be ensured that the relevant Party of the Legal Entity does not match the Sanctioned Party.

Compatibility of the name

Review the alert text and determine if the full name matches or partially matches the name on the Sanctions List or SASB List. If the first name, last name, and middle name (if any) match, the alert may be "Exactly Matched", in which case the relevant information on the basis of such a decision shall be submitted to the Head of the Compliance-control Department or should be reported to his deputy.

If the name partially matches but does not match the citizenship/date of birth/passport information, it may be a 'Bad Match' and the following comment may be entered into the Sanctions Verification System as a rationale for decisions (optional) :

"Incorrect match: Only partial name matches. (Only first, last, or middle name matches)"

If the alert information corresponds to the address of a party listed on the relevant Sanctions List for the Sanctions Region, the alert should be reported to the Head of the Compliance Oversight Office or his/her deputy.

The employee of Compliance-control department may use external sources and make inquiries to the relevant organizations to verify the validity of the above information or conduct additional research to facilitate proper posting of the alert. If the additional information of the alert and the information provided in the Sanctions list are the same, it is considered to be a potential "Full Match" and the head of the Compliance-control Department or his deputy will be informed about it. should be reported and explained in the Sanctions Verification System. If the alert object information and the information in the Sanctions List are not the same, the alert may be "Mismatched".

10.3.2. Secondary review

The second-level review is carried out by the head of the Compliance-control department or his deputy on all warnings made by the employees of the Compliance-control department after the first-level review.

10.3.3. Requests for Notification Information

As part of the investigation, employees of Compliance-control department may request additional information to properly dispose of the alert. In such cases, the employees of Compliance-control department will determine the necessary information and notify the relevant Department of Business Officer responsible for:

- Dispose of the notice and determine the necessary information;
- Transfer of identified data to the employees of the field of activity;
- The employee of the field of activity reviews the relevant information and submits the necessary documents to the Compliance-control Department no later than 5 working days.

Responses will be made within 3 working days of the relevant information being provided, with an additional 4 working days for any follow-up questions. If no response is received within 3 business days and a follow-up request is requested, the employee of Compliance-control

department will report to the Deputy Head of the Compliance Department. If no response is received after 7 working days from the date of initial information submission, the Deputy Head of the Compliance-control Department may cancel the transaction. If the Deputy Head of the Compliance-control Department decides to cancel the transaction due to insufficient information for the disposal of the Warning, he will communicate this decision to the relevant Compliance-control employees and the Activity Department employee.

10.3.4. View more information about the warning

If additional information is provided by the Operations Officer, employees of Compliance-control department will review the alert in detail and dispose of it. The final decision must be reviewed and approved by the Deputy Head of the Compliance Office. Once the decision is approved, the employee of Compliance-control department documents the Sanctions Review System and notifies the Deputy Head of Compliance and the Operations Officer of the action(s) taken.

The Compliance-control Department confirms that the warning is "Inappropriate", the review process can be completed with the appropriate documents. If the warning is disposed of as "Fully Compliant", the Deputy Head of the Compliance-control Department will take action to ensure that the transaction is suspended or rejected without triggering. Notifies the head of the Compliance-control Department about the actions taken. The Suspicious Transaction Notification (STN) shall be delivered to the SASB no later than the business day following the day the suspicious transaction was detected.

10.3.5. Deadlines

The deadlines for completing notice review are as follows:

First-level review: employees of Compliance-control department must review alerts within the business day they are generated. If an alert is created after 5:00 p.m., the alert must be processed on the next business day.

Second Level Review: Second level reviews are conducted by the Deputy Chief Compliance Officer or the Chief Compliance Officer on the same day if the alert is determined to be “Fully Compliant” or “Resolved” by employees of Compliance-control department. delivered as "unmade match", should be implemented.

10.4. The process of automatic verification of the bank's customer base

The Bank, when conducting transactions, including through its payment agents and (or) payment subagents, verifies the identification data of its participants with the List. The process of comparison with the list is carried out by a submodule (verification module) in the bank's automated system.

In particular, the verification module verifies client transactions through the automated banking system, remote banking channels and a mobile application.

To determine whether the List was created or changed by a specially authorized government agency, the verification module automatically accesses the SABS database once an hour.

If it is established that the List has been created or changed, the verification module uploads it to the bank's database and automatically compares the updated part of the List with the database of all bank clients and prepares a report on the result.

Verification of the List update on the official website of the SABS or receipt via an electronic communication channel is carried out by the Sector for Work with Requests and Sanctions Lists of the Compliance Control Department.

The Sector provides access to relevant employees, including employees working directly with clients, by entering the List into the Bank's automated system within an hour from the moment the

List is posted on the official website of a specially authorized government agency or received in electronic form via communication channels.

An SMS message about the formation of the list or the introduction of changes by the SABS will be sent to the phone number of the head of the Bank's Compliance Control Department, his deputy and the head of the sector for working with requests and sanctions lists. The Deputy Head of the Compliance Control Department monitors the configuration of control modules and updates to its database.

If all identification data of the client or one of the participants in the transaction completely coincides with the information of the person included in the list, the employees of the Compliance Control Department will suspend this transaction without delay and without prior notice.

The verification module automatically checks all clients of the Bank, including its payment agents and/or payment subagents, against the List of Included Persons and Persons under International Sanctions once a day.

11. Blocking and rejecting transactions

11.1. General analysis

During the establishment of relations with clients, during the execution of transactions, during one-time transactions requiring due verification of the client, during the registration process via the mobile application, an automatic check of the transaction participants (stop list) is carried out by the Bank's iABS software (without the human factor) and is compared with the List.

If the identification data of the transaction participants matches the persons specified in the List, the iABS system automatically notifies the employees of the Compliance Control Department about blocking this transaction.

The employees of the Compliance Control Department, in turn, visually compare these matching identification data of the client (full last name, first name, patronymic, date and place of birth, address, passport number and series) with the identification data of the person included in the List. If during the comparison process the client and the person(s) from the List do not completely match, the employees of the Compliance Control Department will carry out the procedure for unblocking this transaction.

If the Bank considers the customer or party to be included in the list of targeted financial sanctions in accordance with the applicable laws on sanctions, and if the Bank makes a decision that the customer or party will no longer be able to carry out transactions, will be suspended or refused, the Bank will take the following measures must see:

- The head of the Compliance-control Department makes a decision on suspending or rejecting the transaction without activating the customer or his customer, makes a report and suspends transactions without activating the corresponding authorized Chairman of the Board or the deputy chairman submits a draft decision on granting or refusing and (or) suspending funds or other property of sanctioned persons included in the list of SASB. The final decision on suspension/rejection of the transaction without activation, suspension of funds or other property without activation in accordance with the list of SASB shall be made by the Chairman of the Board or his authorized representative. is accepted by the deputy;
- employees of Compliance-control department shall submit the STN to the Head of the Compliance Department for submission to the SASB based on the reporting procedures established by relevant national laws and regulations.

11.2. Abort transactions without triggering them

Sanctions laws and regulations may require the Bank to freeze the following transactions:

- if it is carried out by or on behalf of or by the order of an individual or legal entity suspended from the list of SASB;
- If it is directed to or through an individual or legal entity that has been suspended without activation;
- If it is related to the transaction being carried out in the interest of an individual or legal entity that has been suspended without starting;
- If the funds or other assets used for the transaction are fully or partially owned by an individual or legal entity listed in SASB;
- If the legal entity participating in the transaction is owned or controlled by an individual or legal entity listed in SASB; or
- Although under certain circumstances a country or region under comprehensive sanctions is involved.

In accordance with the laws and regulations of the Republic of Uzbekistan relating to JFODL and Sanctions or other applicable laws and regulations in a particular jurisdiction, the Bank may suspend the financial operations of the Sanctioned Party, including funds or other assets, received from the Bank without using them. The Chairman of the Board may decide to suspend the financial assets of the sanctioned party without using them in accordance with the requirements of the applicable national legislation. A Financial Asset Suspended Without Operation is managed separately from the Sanctioned Party, but Financial Assets Suspended Without Operation must be marked to indicate the name of the Sanctioned Party.

11.3. Rejection of transactions

Clause 6 *(Sanction restrictions) of this procedure* prohibits entering into practical business relations with the listed activities in all cases. It also rejects transactions for these types of cases identified during the ongoing review process.

11.4. Measures required by national legislation

If all the identification details of the customer or transaction party match with the individual or legal entity entered in the SASB register, the Bank immediately and without prior notice suspends the transaction without starting it, deposits funds into the account of the individual or legal entity, and with the exception of suspending funds or other assets without using them.

The head of the Compliance-control Department submitted a report to the relevant authorized Chairman of the Board or the Deputy Chairman to suspend or refuse the transactions of the persons under the sanction and (or) the funds of the persons included in the list of SASB or submits a draft decision on suspending other assets without using them. According to the list of SASB, the decision on suspension/rejection of the transaction without activation, suspension of funds or other property without activation is made by the chairman of the board or his duly authorized deputy accepted by.

On the same day, the employees of the Compliance-control Department notified the SASB of suspending the transaction without activation and suspending without activation the funds or other assets related to the transaction. to indicate the amount of suspended assets to the head of the Compliance-control department, submits the STN.

11.4.1. Suspension of Customer Transactions for a period of not more than thirty business days

In order to ensure the execution of the instruction provided by SASB, the following tasks are performed to suspend the customer's operation for a period of no more than thirty working days:

1. Upon receipt of an instruction by the SASB to suspend the customer's operation for a period of not more than thirty working days, the Bank's Compliance Department shall record it in a special

electronic journal. The special journal will consist of order number, document number, date of receipt of the instruction, date of execution, name of the customer, date of the execution period, and signs noting the termination of this instruction;

2. In connection with the implementation of this instruction, it is approved by the Chairman of the Bank's Management Board and/or his deputy;

3. Accepted for execution by the relevant department, department and branches, notified to the customer by the relevant department, and within the framework of its execution, the Chairman of the Bank's Management Board and/or his deputy, and The Compliance Office will be notified;

4. The Compliance Department will send a written message to the SASB's instruction on suspending the customer's operation by the SASB for a period of not more than thirty working days and ensuring its execution. Also, the Compliance Department will wait thirty business days for further action related to the directive;

5. The Compliance Department shall notify the respective departments, divisions and branches by corporate mail of this instruction after the expiration of thirty working days of the resumption of operations of the customer mentioned in the instruction;

6. The Compliance Department will send a written and electronic reply to the SASB about the restoration of the customer's operations due to the expiration of this instruction.

11.4.2. Monitoring of declined transactions

If the Bank suspends or rejects a transaction or determines that a payment has been suspended or declined by another financial institution, the Head of the Compliance-control Department shall ask the relevant Compliance-control Department Officer for any future may request tracking of transaction accounts to prevent attempts to circumvent Sanction restrictions by making the same payment again with altered or omitted information to avoid transactions or detection.

If such a re-implemented transaction is identified by daily monitoring or by employees of Compliance-control department or employees of the field of activity, the alert will be forwarded to the Chief Compliance Officer for further review. The Head of Activity, in consultation with the Department of Compliance, makes the final decision to terminate the relationship with the customer.

11.5. Management of funds suspended without activation

In the event that funds are withheld for Sanctions purposes, the withheld funds shall be held in this bank account. The head of the compliance-control department is obliged to immediately report to the relevant state body in the event that the funds are identified and the suspension without use is activated.

The head of the Compliance Department has the right to authorize the use of suspended funds in accordance with the legislation of the Republic of Uzbekistan on JFODL and Sanctions.

A sanctioned person included in the SASB list has the right to apply to the Bank for permission to use the funds or property suspended without use for the purpose of ensuring the following basic human needs:

- average market prices for food, rent, utility bills, medicine, medical supplies and medical services, taxes, other mandatory and insurance fees, lawyers and legal advice, current fees and bank pay within the scope of fees related to managing accounts and property; and payment of emergency expenses.

The following information must be specified in the application for permission to use funds or property suspended without operation: purpose, amount and grounds of payment, property not suspended without operation type, details and identity of the recipient of funds or other property, bank of the recipient of funds.

The bank shall send the received application for permission to use funds or property suspended without use to the SASB no later than one working day from the date of receipt. The decision to allow the use of funds or property suspended without being put into operation shall be taken by the Ministry of Internal Affairs and Communications, notifying the Bank.

Semi-annually, the Head of Operations must submit a statement of funds suspended without starting, only if a written license or authorization from the relevant government agency is submitted and approved by all relevant internal agencies, it must send a report.

11.6. Allowing use of suspended funds without activation

It is not allowed to use the suspended financial asset, except for the following cases approved by the sanctioning regulatory authorities:

- If the facility is registered and approved by the relevant government agency;
- If the sanctions program is canceled;
- The Customer has obtained all relevant permits/licenses for the use of the property;
- If an instruction is received from the SASB to allow the use of the suspended financial asset of individuals or legal entities, and this instruction corresponds to the identification information of the sanctioned person in the list of the SASB ("Incorrect match");
- If the court decision is accepted.

The Head of Compliance control department must review whether the use of property or funds is permitted in accordance with a court order, license or instructions provided. Check first with the Operations Officer and then with the Compliance Office at Headquarters to make sure there are no legal issues with allowing the use of suspended funds without deploying an employee of Compliance-control department. must consult and obtain appropriate permission. The head of the Compliance-control department should also provide additional information requested by the SASB in a timely manner if there are no confidentiality concerns.

The bank allows the use of suspended transactions and suspended funds subject to the following conditions:

- In case of exclusion of persons from the list of SASB, no later than 3 working days from the date of receipt of the updated list of SASB;
- On the same working day of receipt of the instruction on "Incorrect compliance" from SASB, but not later than the next working day.

At the same time, in order to improve the efficiency of the internal control system in banks and to comply with international requirements, the Central Bank, based on the "Recommendation on activities to suspend the activities of persons included in the list of persons involved in terrorist activities or the proliferation of weapons of mass destruction, as well as suspending the use of their funds or other property", determines the beneficial owner of the Bank's client, introduces guidelines on the identification methodology. For more details, see the "Methodology for suspending the activities of persons included in the list, freezing funds or other assets of Appendix A" of this Regulation.

11.7. Monitoring of authorized transactions of persons in the List

In order to monitor a portion of financial assets suspended without involving persons included in the list who have received permission to use them under the SABS, the Compliance Control Department employee includes the person included in the list in the "List of clients with a negative reputation" of the bank's automated system.

During the process of inclusion, the Compliance Control Department employee enters all identifying data into the "List of clients with a negative reputation".

The bank's automated system automatically restricts this operation when the listed person attempts to use that portion of their suspended funds that are authorized for use under the SABS.

The Compliance Control Department employee compares these funds with the authorized amount provided by the SABS.

During the comparison, the Compliance Control Department employee checks the withheld amount in the bank's automated system against the "Management of suspended funds of a person included in the list" journal before issuing permission to use the SABS.

If it does not exceed the permitted portion, it issues a “One-time” permit and records it in the “Management of Suspended Funds of a Listed Person” log. It also immediately informs the SABS about this operation through the bank’s automated system.

12. Reporting

12.1. Submission of internal reports

The Bank is committed to continuing effective oversight of the Sanctions Program through regular reporting. Also, the employee of the Compliance-control department submits the monthly monitoring statistics related to the Sanctions program to the head of the Compliance-control department, and the head of the Compliance department, in turn, summarizes and submits a quarterly report to the Bank Council.

The sample of internal reports is approved by the Chairman of the Head Office.

12.2. Submit an external report

considers that it is not possible to process the transaction made by the customer of this party , the Bank will provide the SASB with a certificate: the head of the Compliance-control Department "Full compliance" with the list of the SASB submits a report to SASB not later than on the working day of the elimination. The head of the compliance-control department must follow the reporting procedures established by the relevant legal documents of the Republic of Uzbekistan.

13. Sanctions risk assessment

The Compliance-control Department is responsible for ensuring that the Bank carries out a Sanctions Risk Assessment ("Risk Assessment") at least once a year. Risk assessments are performed to identify risk factors (e.g. customers, products and services, geographic area) and to assess the effectiveness of sanctions-related controls (e.g. internal control system, operation and management of the Sanctions Review System, training, etc.) .

The Compliance Office assesses the level of risk and uses the results to improve existing controls, policies, procedures and processes. In addition, the obtained results are submitted to the Central Bank of the Republic of Uzbekistan. You are requested to refer to *(Risk Assessment Procedure)* for further guidance .

14. Quality control

14.1. General analysis

The quality control process enables the Bank to assess the quality and consistency of its Sanction Alerts management process, which ensures that Sanction Alerts are implemented and documented by the Sanction Alert Reviewer in a manner consistent with the Bank's compliance with the Bank's standards. The quality control review process for sanction review follows a two-step approach for first-level review alerts and second-level review alerts, respectively.

The quality control review process for alerts disposed of at Tier 1 review can be referenced below in the process for alerts placed at Tier 2 review.

Quality control qualified the third by a party (for example , an external auditor). done increase can Compliance department chief' i the third of the person compatibility and qualification in advance checks.

14.2. Quality control review period

Quality control inspection should be conducted every six months. If the review is not completed by the quality control reviewer within the required time frame, the reviewer will notify the Head of Compliance by email of the reasons for the delay (eg, time or resource constraints) and proposed steps to complete the review.

14.3. Quality control inspection process

Once the alerts are reviewed and resolved, the resolved alerts become part of the quality control content.

Depending on the type of investigation for a sanctions investigation (primary or secondary investigation), each designated investigator is responsible for conducting the following procedures:

Sample selection

To select a quality control sample, the analyst must obtain a list of all Sanction Alerts generated for the period to be reviewed.

In the list provided by the IT Department or downloaded from the Sanctions Review System, quality control should select sample Alerts for review during the target period (ie, alerts cleared during the previous period). For details on sample selection, see the Quality Control Sample Selection Appendix *(Appendix I on Quality Control Sample Selection and Evaluation).*

Map of quality control indicators

After the sample is selected, the quality control analyst analyzes the description, consistency of content and supporting documents of each sample. The result of the analysis should be included in the quality control indicator map.

A quality control analyst will perform an inspection based on the following criteria:

- Customer and (or) transaction review
- Document review
- Description and content review

Quality control rating and overall assessment

The quality control analyst provides a control rating of Pass or Fail for each sample reviewed. If no errors are found, a "Successful" rating is given for each sample reviewed. Each reviewed sample with an error will be given a "Fail" rating.

If the description does not contain information important to support a final decision on the quality or evidence presented, the reviewer may issue a quality control rating of “Fail”. If "Full Compliance" is not identified or missed during a Sanctions review (ie, a Sanctions Violation), the review period rating will be "Fail," regardless of the number of errors. The head of the Compliance-control department should take appropriate measures immediately.

14.4. Preparation of quality control report

A quality control report *(see Appendix K on the Quality Control Report)* is prepared based on the results of the quality control audit and submitted to the Supervisory Board. The quality control report shall contain the following information:

- number of samples considered;
- Number of indicators assessed as "successful";
- Number of indicators evaluated as "failed";
- that any serious Compliance risk has been identified in the relevant process;
- It has been determined that there is a need for training for the relevant process;
- That the results of the quality control audit carried out during the relevant period, which need to be discussed, are included in the agenda of the next meeting of the Supervisory Board.

15. Sanctions verification system

Access to sanctions verification systems is limited to authorized users only. Users authorized to log in to the system should not have the ability or access to change the system settings of the sanction system (ie, fuzzy logic thresholds, list of sanctions), individual users who are granted the right to change the system settings with the exception of Cases of unauthorized access to the system must be reported immediately.

16. Maintain confidentiality of information and documents

All relevant records related to compliance with sanctions, including transaction data, account files, business correspondence, violations, audit work papers, or special licenses authorizing the transaction or use of suspended funds, must be kept in a safe place accessible only to an authorized person for at least 5 years from the date of transactions or termination of business relations with customers.

Records related to idled assets must be maintained for at least 5 years after the idled asset is permitted to be used.

The Compliance-control department (responsible for receiving, analyzing and transmitting transaction reports) should be provided with a special register to record the actions taken by all its structural structures and responsible employees.

The special register must be bound, numbered and the number of pages, the date of opening of the special register (day, month, year) and the signature of the head of the Compliance-control Department must be placed on the back of this register.

All information about the transaction in the special register (order number and date of entering the data into the special register; name of the customer (indicating the unique code of the customer), type, amount and date of the transaction, about the counterparty of the customer information, the name of the structure that provided information about the transaction, information about the measures taken in connection with the transaction, including the date and number of the message, etc. should be reflected).

Transaction information should be recorded in such a way that the details of the transaction can be retrieved if necessary.

documents used in the activities of the Compliance-Control Department (correspondence with the Central Bank of the Republic of Uzbekistan, including paper and electronic copies of messages sent to SASB, paper and electronic questionnaires of customers; registers, etc.); such documents and their inventory are stored in specially designated buildings or in a fireproof and sealed safe directly by the Compliance-control Department.

Electronic versions of documents are archived by software, recorded on electronic media and stored in a fire-resistant and sealed safe along with the inventory by the head of the Compliance-control Department. After the storage period ends, the documents are submitted to the Bank's archives in the prescribed manner.

17 Appendices

Information	Headline	File
Appendix -A	Methodology for suspending the activities of persons included in the list, freezing funds or other assets	