'Approved'
Central Bank of
the Republic of Azerbaijan
Decision № 09/3
21 February 2024

Regulation
on the organization and implementation of activities by the payment system operator

1. General provisions

1.1. This Regulation has been developed in accordance with Articles 43.3, 55.3 and 62.4 of the Law of the Republic of Azerbaijan 'on Payment Services and Payment Systems' (hereinafter – the Law) and determines the amount of minimum authorized capital of the licensed payment system operator (hereinafter - the operator), the requirements for the operator's business plan, internal control system, the risk management system, including security for protection against fraud, illegal use of sensitive payment and personal data, and the format, content and submission procedure of reports by the operator on its activities.

1.2. The minimum amount of operator's authorized capital should be one million manats. A payment institution or an electronic money institution should have additional authorized capital specified for the operator to perform operator activities.

1.3. Minimum requirements for ensuring the information security of the operator, the business continuity and recovery plan in case of emergencies, as well as procedures and criteria for reporting operational or security incidents by the operator to the Central Bank of the Republic of Azerbaijan (hereinafter - the Central Bank) are regulated by information security-related regulations of the Central Bank. The operator should restore the functional activity of the payment system within 2 (two) hours from the moment of emergency.

2. Definitions

2.1. The definitions used in this Regulation bear the following meanings:

2.1.1. **operational risk** – the risk arising from errors and mistakes made by operator's employees, problems and deficiencies in the information system and technologies, as well as external events beyond the organization's control.

2.1.2. **compliance risk** – the risk of enforcement measures and sanctions, financial losses, or damage to reputation that the operator may face in consequence of non-compliance with legislative requirements, including legal acts regulating financial markets.

2.1.3. **business risk** – the risk of the operator's financial situation deteriorating due to a decrease in revenues and/or an increase in costs.

2.1.4. **credit risk** – the risk that the payment system participant may fail to meet liabilities due to the operator and other payment system participants on time and/or in full.

2.1.5. **liquidity risk** – the risk that the payment system participant will not have sufficient liquid funds to cover its liabilities.

2.1.6. **direct payment system participant (direct participant)** – a person who, to use payment system services, enters into an agreement on participation in the payment system with the operator, opens a correspondent or current account with the settlement agent to

make settlements with other payment system participants, and has the right to directly access payment system services.

2.1.7. **indirect payment system participant (indirect participant)** – a person who enters into an agreement with the relevant payment system participant on participation in the payment system and opens a correspondent or current account with the direct participant to conduct settlements with other payment system participants and does not have direct access to payment system services.

2.1.8. **stress-test** – a tool for assessing potential impact of one or more shocks on the functioning of the payment system.

2.2. Other definitions used in this Regulation bear the meanings specified in the Law.

3. A business plan on operator activities

3.1. The business plan prepared for the first 3 (three) years of the operator's activity should include at least the following information:

3.1.1. information on activities to be conducted by the operator, considering the requirement of Article 43.6 of the Law.

3.1.2. financial forecasts for the first 3 (three) years to enable to ascertain the adequacy of systems, resources, and procedures to ensure stable operations and reflect the following:

3.1.2.1. forecasted income statement, balance sheet, cash flow statement.

3.1.2.2. the probable transaction volume and number, the number of participants, service fees to be charged for service types.

3.1.3. information about the organizational structure, indicating powers (rights and duties) of each structural unit, the number of employees to work in those units.

3.1.4. the name and legal address of third-party providers from which the operator receives services related to its activities, and detailed information on the services obtained from each third-party provider.

3.1.5. detailed description of the business model of the payment system (diagram and disclosure of information flow on payment transactions, distinguishing between direct and indirect participation, parties involved in the transaction chain and their functions, as well as the procedure for conducting clearing and settlements).

4. The internal control system

4.1. The operator should have an appropriate organizational structure and an internal control system covering all areas of its activity to ensure reliable and safe management of the payment system.

4.2. The operator should have regulatory documents (statutes, rules, procedures, etc.) that define the functions, powers, subordination and reporting rules of structural units approved by the competent management body.

4.3. The operator should continuously monitor the operation of the payment system as part of the internal control system and assess the achievement of the set goals.

4.4. The operator’s internal control system should provide at least the following:

4.4.1. compliance of operator's activities, including the payment system rules with the legislation, as well as internal regulatory documents.

4.4.2. clear segregation of authorities in decision-making regarding the organization of payment system activities.

4.4.3. complete, accurate and timely preparation and delivery of information required for activities of managerial bodies.

4.4.4. lack of conflicts of interests between structural units, and availability of procedures for timely identification and prevention of situations and areas where a conflict of interest may arise.

4.4.5. substantiated operational costs and investments.

4.4.6. timely, complete, and correct preparation and submission of information and reports in accordance with the legislative requirements.

4.4.7. reliable, continuous, and secure management of the operator's information systems in accordance with the legislation and internal regulatory documents.

4.4.8. ensuring confidentiality and completeness of information.

4.4.9. conducting internal audit reviews.

4.4.10. internal and external audit reviews related to information and communication technologies and security risk management.

4.4.11. timely notification of operator's managerial bodies about violations and deficiencies found as consequence of external or internal audit reviews in the operator's activity and internal control system, and monitoring of the measures taken to eliminate them

4.5. With respect to internal audit the operator should provide the following:

4.5.1. the operator’s authorized management body should approve internal audit plans, create necessary conditions for the implementation of audit activities and take appropriate actions to eliminate violations and deficiencies identified by the internal audit service

4.5.2. the operator's internal audit service should be separate from day-to-day operational and control functions.

4.5.3. the operator's internal audit service should report to the operator's management bodies at least once a year on the inspections conducted, violations and deficiencies detected, recommendations provided, and the status of their implementation.

4.6. All areas of operator's activities (including outsourcing activities) are included in the scope of internal audit.

4.7. The requirements of the Law of the Republic of Azerbaijan ‘on Internal Audit’ should be adhered during the organization and implementation of the internal audit.

5. The risk management system

5.1. The operator should have an effective risk management system that ensures the identification, assessment, monitoring, and control of the risks it, and its participants, may be exposed to.

5.2. The risk management system should cover at least:

5.2.1. the procedure for identifying, evaluating, monitoring, and controlling all existing and potential risks of the operator, including operational, compliance, business, credit, liquidity, and other risks, as well as the tools used for risk management.

5.2.2. the procedure for managing outsourcing risks.

5.2.3. the procedure for managing the risks that may arise when using services of other organizations (Internet, power supply, etc.) to ensure payment system operations.

5.2.4. the procedure for allocating authorities on risks between operator’s structural units, as well as facilitating interaction and data sharing.

5.2.5. the procedure and scenarios for conducting risk-related stress-tests.

5.2.6. the risk management reporting system.

5.3. Internal risk management rules and procedures should be reviewed at least once a year. If the risk management system fails to mitigate the risks encountered by the operator, or if there is an incident related to the risk not accounted for in the operator's risk profile, or if there are interruptions in operator's operations, as well as when significant alterations are made to information systems and technologies, essential adjustments should be made to the risk management system within 3 (three) months and these changes should be documented.

5.4. To manage compliance risks, the operator should ensure the compliance of payment system rules, including payment system operator's regulatory documents and contractual relations with the requirements of the legislation.

5.5. In the risk management provisions of payment system rules the operator should outline the mechanisms to be applied to regulate credit and liquidity risks, as well as to minimize the impact of these risks on other participants.

5.6. If operator's payment system rules include provisions for indirect participation, procedures for direct participants to inform the operator about indirect participants, and rules governing the relationship between direct and indirect participants, should be clearly defined.

5.7. To manage operational risks, the processing power of the payment system should ensure that possible increases in transaction volumes are met.

5.8. Depending on types of risks that the payment system may encounter, stress tests should be conducted every 6 (six) months. The operator should have adequate resources (human and IT) to conduct these stress tests. If the operator lacks appropriate resources, the conduct of stress tests can be outsourced to the organization specialized in this field.

5.9. When conducting stress tests, the 'worst', 'best' and 'most likely' scenarios should be drawn up and specific criteria and shocks should be identified per scenario, including probabilities. Potential risks and maximum losses should be considered during the scenario development process.

5.10. To prevent risks identified by outcomes of stress tests, an action plan should be prepared and implemented.

5.11. Confidentiality of sensitive payment data should be ensured when outsourcing services by the operator, and in case of integration with information systems of third-party providers, data sharing should be organized in accordance with security requirements.

6. Security measures related to operator activities

6.1. The operator should have an anti-fraud security policy in place to at least include:

6.1.1. fraud detection and prevention measures, including tools used and procedures applied.

6.1.2. designating employees or a structural unit responsible for monitoring and preventing frauds and managing related complaints.

6.1.3. a procedure for receiving and processing fraud appeals from payment system participants, and from payment service users, if provided for in agreements concluded with participants.

6.1.4. determining a procedure for informing relevant structural units in case of frauds.

6.2. To protect against the illegal use of sensitive payment and personal data, operator's internal rules should contain at least the following:

6.2.1. a register of location(s) where sensitive payment data are stored.

6.2.2. a description of the flow of sensitive payment data for the services provided.

6.2.3. information about the persons who have the right to access relevant infrastructure components and systems, including the database.

6.2.4. the order of storage of sensitive payment data.

6.2.5. cases of using sensitive payment data.

6.2.6. technical security measures applied for the security of sensitive payment data, including information systems and technologies, encryption and/or tokenization, and monitoring tools.

6.2.7. the procedure for determining subjects who have the right to access sensitive payment data.

6.2.8. procedures for identifying and preventing unauthorized access to sensitive payment data and related vulnerabilities.

7. Reporting and notification

7.1. The operator submits the report on activities as per Annex No. 1 herein to the Central Bank quarterly no later than the first 5 (five) working days of the following quarter.

7.2. By the last working day of January of each year, the operator submits to the Central Bank a list of core equipment and software used, detailing any changes that occurred during the previous calendar year, the topological diagram of connections between them (the services and integrations received from external organizations).

7.3. Reports on the requirements specified in Item 1.3 herein are submitted in the manner and within the period set by information security regulations of the Central Bank.

7.4. When new participants enter or an existing participant exits (is removed) from the payment system, and when the participant's status (direct or indirect participant) changes, the operator submits the report to the Central Bank as per Annex No. 2 of this Regulation within 5 (five) working days.

7.5. The operator should designate a person responsible for promptly answering questions that may arise in the operator's activity and submitting information (reports) related to the operator's activity to the Central Bank and submit written information about that person (last, first, middle names, position and contact details) to the Central Bank. If the responsible person changes, the operator should submit written information about the new responsible person to the Central Bank within 3 (three) working days.

7.6. Written information by the coordinator about unplanned outages in the operator's activity (interruption of the work in the system or information sharing with participants for 15 (fifteen) minutes or more) should be submitted to the Central Bank 15 (fifteen) minutes after the occurrence of the event and about planned outages no later the at least 3 (three) working days.

7.7. Reports specified in this Regulation are approved by the enhanced electronic signature of the head of the operator’s executive body or the official(s) authorized by him/her and are submitted through the Central Bank’s electronic information system.

Annex 1
to the 'Regulation on the organization and implementation of activities by the payment system operator'

Report on operator's activities		
1. Balance sheet data *(Thousand manats)*		
1.1.	Cash*, total*	
1.2.	Funds in payment accounts	
1.3.	Investment to securities	
1.4.	Accounts receivables	
1.5.	Fixed assets (less amortization)	
1.6.	Intangible assets (less amortization)	
1.7.	Other assets	
	Total assets	
1.8.	Funds attracted from credit institutions	
1.9.	Funds attracted from other financial institutions	
1.10.	Other liabilities	
	Total liabilities	
1.11.	Authorized capital	
1.12.	Net retained earnings	
1.13.	Total reserves	
	Total equity	
2. Information about gains and losses		
2.1.	Income related to operator activities	
2.2.	Other income	
2.3.	Operating expenses	
2.4.	Other expenses	

Annex 2
to the 'Regulation on the organization and implementation of activities by the payment system operator'

Payment system operator name	Name and TIN of the payment system participant	Participant's status (direct/indirect)	Services received from the payment system operator	The change occurred (entry of a new participant, termination of participation, change of the participant's status)