

## **Regulation on operational risk management in banks**

### **1. General provisions**

1.1. This Regulation has been developed in accordance with Article 34.5 of the Law of the Republic of Azerbaijan ‘on Banks’ (hereinafter – the Law) and establishes minimum requirements for the operational risk management in banks, as well as in local branches of foreign banks (hereinafter – banks).

1.2. The organizational structure of the operational risk management in banks is regulated with the ‘Corporate governance standards in banks’ approved by Resolution No 41/1 of the Central Bank of the Republic of Azerbaijan (hereinafter – the Central Bank) dated 28 August 2023.

### **2. Definitions**

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

2.1.1. operational risk – the risk of loss arising from inadequate or failed internal processes, people, systems, or external events.

2.1.2. incident – an event that causes the disruption or interruption of bank’s critical operations.

2.1.3. total loss – the damage incurred by the bank resulting from a risk event.

2.1.4. recoverable amount – the amount paid or refunded by the liable party and/or a third party for the total loss.

2.1.5. outsourced service – a service where certain activity/ies is/are continuously performed by a third party (whether it belongs to the bank’s corporate group) based on an agreement between the parties.

2.1.6. market approach – the valuation of an asset based on a comparison with identical or similar assets available in the market.

2.1.7. cost approach – the valuation of an asset based on the principle that its cost should not exceed the expense a buyer would incur to acquire (purchase, construct, etc.) an asset of equal utility.

2.1.8. operational resilience – bank’s ability to deliver critical operations during an incident.

2.1.9. critical operations – operations, processes, and services essential for the bank’s business continuity.

2.2. Other definitions used in this Regulation bear the meanings as defined in the Civil Code of the Republic of Azerbaijan, the ‘Corporate governance standards in banks,’ and other legal acts regulating financial markets.

### **3. The operational risk management system**

3.1. The bank establishes an operational risk management system, adequate for the type, volume, and nature of its operations, the environment it operates in, and its risk profile.

3.2. The operational risk management system is integrated into the bank's overall risk management process, covering all areas of its activities, including business lines, products, services, processes, and systems.

3.3. The bank's Supervisory Board ensures the establishment and assessment of the effectiveness of the bank's operational risk management system.

3.4. The bank's Supervisory Board reviews at least once a year the adequacy of the operational risk management system in addressing risks arising from new products, services, processes, and systems, and external environmental changes and other factors, as well as findings of reviews conducted by internal audit, external audit, and other specialized third parties and makes relevant decisions accordingly.

3.5. The operational risk management system should be designed in alignment with the bank's operational policies and should cover at least:

3.5.1. operational risk management policies and procedures.

3.5.2. tools for identifying and assessing operational risks.

3.5.3. operational risk monitoring and reporting.

3.5.4. operational risk control and risk mitigation methods.

3.5.5. bank's operational resilience and business continuity plan.

3.6. The operational risk management system applies to all structural units of the bank, both domestic and international operational units, as well as its subsidiary entities.

### **4. Operational risk management policies and procedures**

4.1. The operational risk management policy is developed in accordance with the bank's business strategy and risk appetite. In addition to the requirements specified in the 'Corporate governance standards for banks' regarding risk management policies, the operational risk management policy should include at least the following:

4.1.1. types of operational risks inherent to the bank in relation to occurred and potential incidents.

4.1.2. procedures for utilizing outsourced services.

4.1.3. limits on operational risks the bank may be directly or indirectly exposed to, including loss limits, risk mitigation methods, and other related matters, in line with the bank's risk-taking capacity and risk appetite.

4.1.4. fundamental principles of the Management Information System (hereinafter – the MIS) used in monitoring and reporting processes.

4.1.5. the scope and use of operational risk information, including potential loss information and scenario analyses.

4.1.6. creating a favorable environment for external auditors to assess operational risks.

4.1.7. reviewing and updating the policy as needed if the growth dynamics of bank's assets exceed the sector's asset growth dynamics.

4.2. The bank develops internal rules for managing operational risks in accordance with the nature of its activities and the scope of its operations. These rules comprehensively

regulate bank's risk-generating activities and the process of operational risk management, serving as a guiding framework for implementing the operational risk policy. Internal rules on operational risks should be aligned with other policies and internal rules.

4.3. To identify and assess potential operational risks associated with new products, services, activities, processes, and systems internal rules should cover at least:

4.3.1. operational risks inherent to new products, services, activities, processes, and systems.

4.3.2. changes in the overall operational risk profile (including risks related to available products and activities), risk appetite, including risk limits, and risk-taking capacity.

4.3.3. due diligence, risk management, and mitigation strategies.

4.3.4. residual risk after implementing all measures to identify, measure, and mitigate risks.

4.3.5. measuring, monitoring, and managing risks associated with new products, services, activities, processes, and systems.

4.4. Internal rules should designate the structural unit responsible for centralized oversight of operational risk management, and define its authority, reporting structure, reporting procedures, and interactions with other structural units within the bank.

4.5. The bank should review its operational risk policy and internal rules at least once a year and make necessary amendments as required.

## 5. Tools for identifying and assessing operational risks

5.1. Each bank identifies and assesses operational risks associated with its products, activities, processes, and systems.

5.2. To effectively identify operational risks, the bank should consider both internal (organizational structure, nature of operations, staff capacity, organizational changes, employee turnover, etc.) and external factors (changes in the economic environment and banking sector, technological innovations, etc.).

5.3. The bank utilizes at least the following tools to identify and assess operational risks:

5.3.1. **audit findings:** information from internal and external audits is used to identify operational risks.

5.3.2. **collection and analysis of operational risk incident information:** a database is created and analyzed to assess the scale of operational risks and the effectiveness of internal controls (the collection and reporting of operational risk event information are regulated under Part 9 of this Regulation).

5.3.3. **operational risk self-assessment:** the Risk and Control Self-Assessment (RCSA) process is conducted to identify potential threats, risk-sensitive areas, and evaluate control effectiveness on operations arising from activity directions of the bank and is conducted at least once a year for critical operational units and at least once every two years for the bank.

5.3.4. **process mapping:** during RCSA various, including interconnected risks are identified with the process mapping, and vulnerabilities in risk management and control functions are detected and analyzed. The process mapping is developed considering the opinion of the structural unit responsible for risk management.

5.3.5. **heat map:** a heat map is prepared based on RCSA results, operational risk incident information, and other sources to visualize encountered risks, prioritizes them, and

an action plan is developed to mitigate risks. A sample heat map is provided in Annex 1 to this Regulation.

5.3.6. **Key Risk and Performance Indicators:** Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) analyze major risks the bank is exposed to. The KRI is the tool that measures the impact of major risks and KPIs provide information on operational gaps, errors, and potential losses in systems and processes (both indicators serve as early warning tools for risk limit breaches).

5.3.7. **scenario analysis** is the process which identifies and assesses potential impacts of potential operational risk incidents based on the judgement of experts from business units and risk specialists (this analysis may use the information from loss databases, self-assessments (RCSA, KRI, KPI), monitoring results, and other risk information).

5.3.8. **comparative analysis:** results of different risk assessment tools are compared for a comprehensive understanding of the bank's risk profile (e.g., the frequency and impact of observed risk events from the loss database can be compared with RCSA results to measure the effectiveness of the self-assessment process).

5.4. Using the data collected through the risk assessment tools listed in Item 5.3 herein, the bank calculates its exposure to operational risk through internally developed models.

## 6. Operational risk monitoring and reporting

6.1. A bank should have written procedures and an information system for monitoring operational risks that are adequate for its risk profile and business activities. For monitoring of operational risks, at least:

6.1.1. an early warning mechanism is established, and trends in KRIs are regularly monitored.

6.1.2. trends in risk events recorded in the operational risk events database are tracked.

6.1.3. the implementation status of the action plan developed for mitigating operational risks is tracked.

6.1.4. risk events exceeding the limit set by the bank for losses, in accordance with sub-item 4.1.3 of this Regulation, are investigated.

6.1.5. back testing (comparison of projected losses with actual results) is conducted for losses forecasted in previous periods.

6.1.6. external events and their potential impact on operational risks are assessed.

6.1.7. operational risks arising from outsourcing is monitored.

6.2. The Management Board should ensure that employees responsible for monitoring operational risks are independent of the operational units they oversee (e.g., a monitoring employee should not work in the operational unit being monitored, there should be no conflict of interest regarding monitoring results, and the monitoring report should be unbiased and objective).

6.3. The bank should have a reporting mechanism that supports the effective management of operational risks for the Supervisory Board, Risk Management Committee, Management Board, and relevant operational units. The report should include at least:

6.3.1. information on the bank's risk appetite and breaches of risk limits.

6.3.2. information on internal operational risk events and related losses during the reporting period.

6.3.3. events that may have a potential impact on the bank and its capital, including external incidents and regulatory changes.

6.3.4. causes of operational risk incidents and measures taken to mitigate them.

6.3.5. information on high-risk areas related to operational risks.

6.3.6. operational risks identified by the bank, monitoring results, verification of the process for recording operational risk incidents in the database, and risks identified by external auditors and the Central Bank.

6.4. to ensure the effectiveness of operational risk monitoring and risk reporting, an MIS is implemented, enabling at least:

6.4.1. identification, assessment, management, and control of daily risks.

6.4.2. verification of compliance with established rules and limits.

6.4.3. monitoring trends in risk indicators.

6.4.4. preparation of reports in accordance with legal acts and internal policies.

6.5. The MIS should be capable of tracking risk limits and notifying the Management Board and other relevant users when predefined thresholds are reached.

6.6. Reports generated by the MIS should be accessible to members of the Supervisory Board, Management Board, Risk Management Committee, and employees responsible for risk management.

6.7. The bank determines the frequency of monitoring and reporting based on the scale and nature of risks arising from its activities and changes in financial markets.

6.8. In cases of external events and threats that may impact bank's operations (e.g., martial law, state of emergency, pandemic, terrorism, etc.), an additional report is prepared and submitted to the Supervisory Board, Risk Management Committee, and Management Board, in addition to periodic operational risk reports.

6.9. The information covered in operational risk reporting should be regularly analyzed to improve the bank's strategy, policies, and procedures.

## **7. Operational risk control and risk mitigation**

7.1. The bank should have a strong control environment that utilizes policies, procedures, systems, internal controls, and strategies for risk mitigation and/or transfer.

7.2. Internal control oversees efficiency of operations, minimization of human errors, security of assets, guarantees the completeness, timeliness, and reliability of financial reports and other information, and ensures compliance with legal and regulatory requirements.

7.3. Control processes cover the bank's operational resilience both under normal conditions and in the event of incidents and necessary corrective measures.

7.4. Effective internal control consists of risk assessment, control, information and communication, and monitoring, all of which are integral to the risk management process.

7.5. The control process should be structured in accordance with the legislation, regulations of the Central Bank, and the bank's internal policy. To assess the adequacy of the control process to the bank's policy, at least the following should be considered:

7.5.1. regular monitoring by the Management Board of actions taken to achieve established objectives.

7.5.2. oversight by the Management Board on the implementation of corrective actions plans designed to address identified violations.

7.5.3. reviewing the preparation, approval, and submission of internal reports to ensure they are completed within the deadline.

7.5.4. ensuring accountability and regular monitoring of deviations from limits (e.g., risk limits, authority thresholds) and/or the bank's policy.

7.6. To establish an effective control environment, the bank should clearly segregate duties and responsibilities, as well as enforce dual control (the 'four-eyes' principle). In addition to segregation of duties and dual control, the bank should at least:

7.6.1. conduct intensive monitoring of established limits and investigate any breaches.

7.6.2. ensure the security of bank's assets and database usage (e.g., access permits, necessary infrastructure, authentication, etc.).

7.6.3. recruit qualified personnel and provide training opportunities to ensure specialization across all areas of the bank's operations.

7.6.4. implement procedures to identify business areas or products generating higher-than-expected profits and analyze reasons behind their profitability (e.g., if the bank earns unusually high profits from a low-risk, low-expected-return activity, it should be investigated to find out whether this is due to regulatory violations or internal control weaknesses).

7.6.5. regularly review and reconcile transactions and accounts.

7.6.6. establish a substitution policy to address potential disruptions in authority execution when employees are unable to perform their duties for two weeks or more due to leave, illness, or other reasons.

7.6.7. develop an internal risk culture through training programs and enhance communication on risk management within the bank.

7.7. Given the significant impact of information and communication technologies (ICT) on the efficiency of internal control, the bank should adopt a unified approach to identifying, measuring, monitoring, and managing ICT risks. The management of ICT risks in banks is regulated by the 'Information security requirements for supervised entities in financial markets' approved by Decision No. 14/2 of the Central Bank dated 28 March 2024.

7.8. The bank may utilize outsourcing, considering the opinion of the structural unit responsible for the risk management function. The bank remains responsible for any risks arising from outsourcing. When using outsourcing, the bank should ensure at least the following for effective management of operational risks associated with outsourcing:

7.8.1. establishing an internal policy for managing risks associated with outsourcing.

7.8.2. procedures for conducting operations through outsourcing.

7.8.3. a selection process for potential service providers.

7.8.4. ensuring that agreements with service providers explicitly outline responsibilities, authority distribution, and confidentiality of information, including banking secrecy.

7.8.5. procedures for monitoring and managing risks related to external service providers, including evaluating their financial stability.

7.8.6. creating effective control environment in the bank and at the service provider.

7.8.7. a business continuity plan for outsourced activities.

7.9. When outsourcing banking activities, information technology, or information security services, the bank should submit details regarding the outsourced service and the service provider (including the provider's business scope and experience in the relevant

service area) to the Central Bank along with the signed agreement within five (5) business days.

7.10. If the bank is unable to manage risks arising from outsourcing but considers discontinuing the outsourced service impractical, it may transfer its exposure to such risks to a third party through insurance or other risk mitigation mechanisms.

## **8. Bank's operational resilience and business continuity plan**

8.1. In the case of an incident, the bank should have operational resilience for the execution of critical operations. Operational resilience is built on incident response measures, situational adaptation, recovery plans, and practices.

8.2. In the event of business disruptions, in martial law and emergency situations, including natural disasters, epidemics and pandemics, terrorism, and other emergencies, the bank should develop as part of the bank's overall emergency plan a business continuity plan to manage operational risks and ensure business continuity to limit losses and ensure the continuity of its operations.

8.3. To ensure operational resilience, the bank should identify at least its critical operations, conduct stress tests in various scenarios, form a business continuity plan, and effectively manage dependencies on third parties.

8.4. The business continuity plan is developed in accordance with the size, business direction, operational volume, and complexity of the bank, and is based on scenarios to which the bank is vulnerable. The business continuity plan should at least cover:

8.4.1. analysis of the impact of the scenarios listed in section 8.2 herein on business operations.

8.4.2. business recovery strategy.

8.4.3. segregation of roles and responsibilities in emergencies.

8.4.4. organization of communication.

8.4.5. recovery procedures.

8.5. To ensure the effective implementation of the Business Continuity Plan, the bank should provide training and awareness programs for employees, test the plan at least once a year, and report test results and any necessary changes to the bank's Supervisory Board.

## **9. Collection and reporting of operational risk events related information**

9.1. The bank should collect information on operational risk incidents to verify its operational risk management system and conduct empirical (experience-based) risk forecasting related to losses.

9.2. The operational risk incident database should include information directly related to bank's current business activities, technological processes, and risk management procedures. To achieve this, the bank should have written procedures for identifying and collecting information on operational risk incidents.

9.3. To adequately measure operational risks using internal models, the bank should maintain an operational risk incident database covering at least the past three (3) years. This database should facilitate the identification of risk incidents, support for operational units in minimizing or eliminating risks through action plans, statistical analysis of risk types, causes, frequency, and impact for forecasting and prioritization.

9.4. In forming the operational risk incident database, at least the following should be ensured:

9.4.1. the information on operational risk incidents is collected in accordance with the business areas and risk events specified in Annexes 2 and 3, and the impact of losses resulting from operational risks is classified based on the example provided in Annex 6.

9.4.2. key activities and risks across the bank's entire service network (branches, departments, etc.).

9.4.3. the operational risk incident database includes at least the indicators specified in Annex 4 of this Regulation.

9.4.4. operational risk incidents that have resulted or have the potential to result in credit and market risks are recorded in the database with a special note.

9.4.5. operational risks arising from outsourced services are included in the database.

9.4.6. when utilizing the operational risk incident database, the date when the loss was identified (if a monetary loss occurred), or the date when the operational risk incident took place (if no monetary loss occurred) is taken as the basis.

9.4.7. interrelated incidents and losses are grouped and reflected as a single entry in the database.

9.4.8. if an operational risk incident affects multiple business areas, the resulting loss is recorded in the database proportionally across relevant business areas.

9.4.9. total loss recorded in the operational risk incident database is calculated with the market and/or cost approach. The following requirements should be met in the loss calculation:

9.4.9.1. direct costs recognized in the income statement related to the operational risk incident (e.g., asset impairments and write-offs), indirect costs (e.g., legal expenses, payments to consultants or providers), and restoration costs incurred to restore the situation to its pre-incident state.

9.4.9.2. maintenance costs for land, buildings, and equipment, insurance premiums are not considered in the total loss calculation.

9.5. The bank collects quarterly information on operational risk incidents related to its subsidiary banks. Based on this information, the bank establishes a separate database for subsidiary banks in accordance with Annex 4 of this Regulation.

9.6. To facilitate the collection of operational risk incident information, the bank should designate an operational risk coordinator in each structural unit. The coordinator:

9.6.1. investigates and records the risk incident using the single format established by the bank.

9.6.2. obtains approval from the head of the structural unit for the recorded risk incident.

9.6.3. submits the approved information and related documents to the risk management unit within two (2) business days from the date of identification of the incident, as per sub-item 9.6.1 of this Regulation. The coordinator immediately reports the incident to the risk management unit if:

9.6.3.1. the risk incident results in a breach of risk limits.

9.6.3.2. the risk incident could lead to binding instructions against the bank, including sanctions or enforcement measures.

9.6.3.3. cases of internal or external fraud occur.

9.6.3.4. the monetary loss caused by the risk incident exceeds the threshold limit set by the bank in accordance with sub-item 4.1.3 of this Regulation.

9.7. To ensure the accuracy and completeness of the information, operational risk incident records are reviewed at least quarterly. In case of any changes, the risk management unit is notified accordingly.

9.8. After the information on the risk incident is submitted, the operational risk responsible employee in the bank's Risk Management Unit investigates and confirms the incident within three (3) business days and registers it in the bank's database.

9.9. The bank should submit information on the following incidents to the Central Bank as per Annex 5 of this Regulation, no later than fifteen calendar days after the end of each quarter:

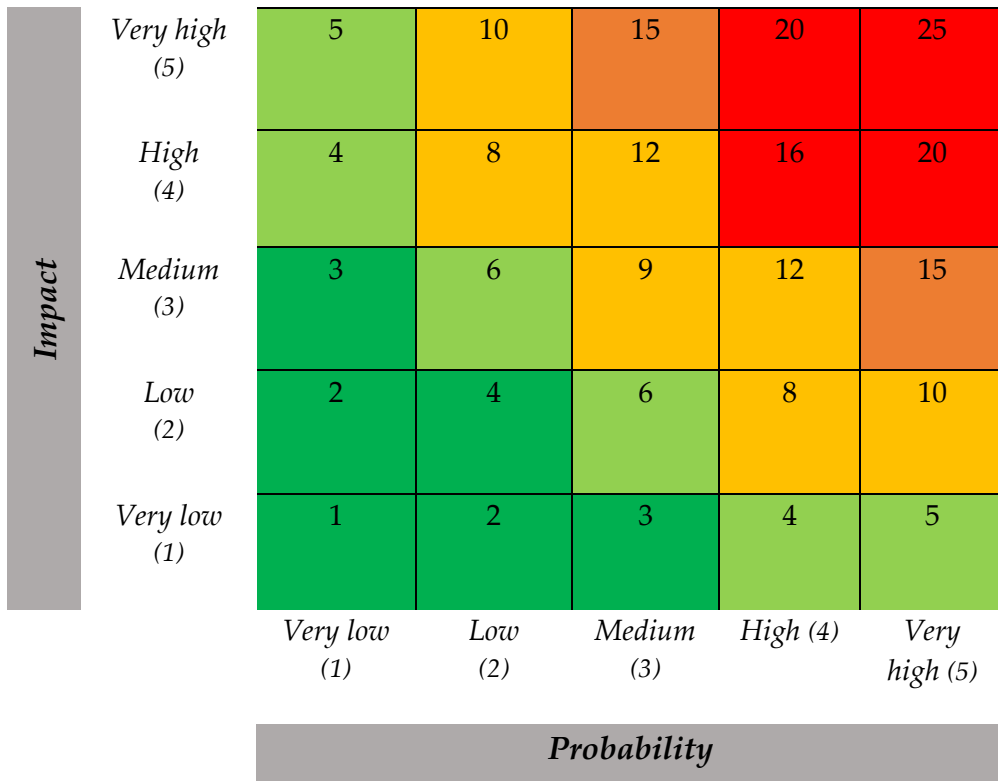
9.9.1. incidents where total loss amount is AZN100,000 (one hundred thousand) or more per incident.

9.9.2. incidents that have occurred frequently (10 or more times within the last 12 months).

9.9.3. incidents where potential loss is AZN100,000 (one hundred thousand) or more.

9.10. If the Central Bank requests additional information or documents related to operational risk incidents for supervisory purposes, the bank should provide the relevant information and documents within the deadline.

**Sample heat map**



	<i>Very high</i>
	<i>High</i>
	<i>Medium</i>
	<i>Low</i>
	<i>Very low</i>

**BREAKDOWN OF BUSINESS AREAS**

<b>Business areas</b>	<b>Classification code</b>	<b>Description</b>
Corporate finance	BS1	Provide financial advisory services to businesses for long-term and strategic operations, and increasing liquidity, as well as investment services (operations) with securities and derivative financial instruments in accordance with the scope and procedure stipulated in the Law of the Republic of Azerbaijan 'on the Securities Market.'
Asset management	BS2	Provide investment services (operations) with securities and derivative financial instruments to individuals in accordance with the scope and procedure stipulated in the Law of the Republic of Azerbaijan 'on the Securities Market.'
Consumer banking	BS3	Issue loans to individuals for purposes unrelated to entrepreneurship or professional activities, including real estate loans, attract deposits from individuals, issue payment instruments, and provide other services.
Commercial banking	BS4	Provide business financing, including project financing, export financing, factoring, leasing, guarantees, and services unrelated to other business areas
Payment systems and settlements	BS5	Payments, money transfers, clearing and settlements
Agency services	BS6	Financial agent services

**BREAKDOWN OF RISK INCIDENTS**

Type of operational risk	Risk event category (Level 1)	Definition	Risk event category (Level 2)	Risk event (Level 3) (Sample) <sup>1</sup>
Processes	Work relations and workplace safety (R1)	Losses arising from violations of labor, health, or safety laws and/or regulations, as well as from actions contrary to agreements, compensation for health-related damages, or unlawful conduct and discrimination against employees.	Employee relations (R1.1)	Compensation and issues related to termination of labor agreements Strikes within the workforce
			Safe environment (R1.2)	Occupational Safety Incidents related to employee health and safety Compensation for employees
			Unlawful conduct and discrimination (R1.3)	All types of discrimination and unlawful actions
	Customers, products, and business relations (R2)	Losses arising from the unintentional or negligent failure to fulfill professional obligations to certain customers (including reliability and compliance requirements), as well as from the nature and design of the bank product.	Violations related to compliance, data disclosure and reliability (R2.1)	Violation of fiduciary duties / Violation of rules Issues related to compliance / disclosure of information ('Know Your Customer' principles, etc.) Violations regarding the disclosure of customer information Breach of confidentiality Aggressive sales practices Inflation of accounts Misuse of confidential information Violation of lending obligations
			Unprofessional business or market relations	Illegal trade / market relations Market manipulation Insider trading (conducted from the bank's account)

<sup>1</sup> The bank may increase the samples related to Level 3 risk incidents.

Processes			(R2.2)	Unlicensed activities Money laundering activities	
			Defects in products (R2.3)	Defects in products	
				Model errors	
			Violations related to customer selection, sponsorship, and the volume of loan claims (R2.4)	Failure to conduct customer due diligence according to instructions Violation of customer limits	
			Advisory service (R2.5)	Disputes related to the provision of advisory services	
	Execution, delivery, and process management (R3)	Losses arising from incorrect execution of operations, inadequate process management, or relationships with business partners and suppliers	Work, execution, and attendance (R3.1)	Information asymmetry Errors in data entry, implementation, or upload Fail the deadline or to fulfill the obligation Mismanagement of the model/system Accounting error / error in company's details Delivery error Error in collateral managing Other job violations	
				Monitoring and reporting (R3.2)	Failure to comply with the reporting requirements set by legislation Inappropriate external reporting (resulting in monetary loss)
				Customer onboarding and documentation (R3.3)	Incomplete customer consent / refusal documents Incomplete / missing legal documents
				Customer account management (R3.4)	Unauthorized / unapproved access to accounts Incorrect customer registration (resulting in monetary loss) Loss or damage to customer assets due to negligence
				Trade partners (R3.5)	Failure of non-customer counterparties to properly fulfill their obligations

				Disputes with non-customer counterparties
			Vendors and providers (R3.6)	External services Disputes with vendors
Human	Internal fraud (R4)	Losses arising from fraud involving at least one bank employee, embezzlement of bank property, or violations of legislation, as well as bank's internal policies and rules	Unauthorized operations (R4.1)	Unauthorized transactions (resulting in monetary loss) Undeclared and unnotified transactions (deliberately) Incorrect reporting of financial indicators (deliberately)
			Embezzlement and fraud (R4.2)	Fraud / credit fraud / worthless (fake) deposits Theft / robbery / misappropriation of funds / pillage Asset misappropriation Willful destruction of assets Forgery Writing a non-existent check Customer account takeover / identity impersonation Abusive tax transactions / (deliberate) tax evasion Bribery / illegal payment Insider trading (not conducted from the bank's account)
	External fraud (R5)	Losses arising from fraud, embezzlement of bank property, or other illegal acts committed by a third party	Embezzlement and fraud (R5.1)	Theft / robbery / misappropriation or waste / pillage Fraud Issuing a worthless check
			System security (R5.2)	Cyberattack Data theft
System	Operations disruption and system errors (R6)	Losses arising from disruption of operations or system errors	Systems (R6.1)	Equipment Software Communication Utility Outages / Disruptions
External events	Damage to physical assets (R7)	Loss or damage to physical assets due to natural disasters or other events	Natural disasters and other events (R7.1)	Losses caused by natural disasters Losses due to external factors (Vandalism, Terrorism)

**OPERATIONAL RISK INCIDENT DATABASE**

№	Information about damages	
1.	Registration date (d.m.y)	
2.	Registration code <sup>2</sup>	
3.	The employee who enters information into the database	
4.	Structural unit, the risk incident occurred in	
5.	Employee who provided the information (coordinator)	
6.	Date and time of the risk incident (d.m.y.)	
7.	Date and time the risk incident was found out (d.m.y.)	
8.	Employee who found out the risk incident	
9.	Description of the risk incident	
10.	Cause of the risk incident	
11.	Frequency rate	
12.	Impact rate	
13.	Business area code	
14.	Bank product	
15.	Risk incident category code (Level 1)	
16.	Risk incident category code (Level 2)	
17.	Risk incident (Level 3)	
18.	Damage impact category	
19.	Total loss amount, in thousand manats	
20.	Potential loss amount	
21.	Recovery date (d.m.y.)	

<sup>2</sup> For instance, in the event of an external fraud in the payment systems and settlements business area the registration code - BS5R5.1

22.	Recovered amount (in thousand manats)	
22.1.	Part of loss recovered through insurance (in thousand manats)	
23.	Date of actions on elimination of the risk incident (d.m.y.)	
27.	Description of actions on elimination of the risk incident	
25.	Structural unit responsible for the actions on elimination of the risk incident	
26.	Status of execution of the actions on elimination of the risk incident	
27.	Date of recent change (d.m.y.) and brief description of the change	

**Note:** Sections 23-26 of this Annex are filled out for losses exceeding the limit set by the bank's internal rules.







**Sample damage impact categories**

Category	Description	Scope
<b>Legal responsibility</b>	Mediation and other pre-trial dispute resolution methods, legal costs related to court decisions, as well as other legal expenses	<ul style="list-style-type: none"> <li>• Expenses related to court or mediation proceedings (including lawyer fees, enforcement of court decisions, etc.)</li> <li>• External legal costs directly related to the incident</li> </ul>
<b>Supervisory measures</b>	Fines or other financial sanctions, enforcement measures resulting in monetary loss, license revocation	<ul style="list-style-type: none"> <li>• Fines paid for regulatory violations</li> <li>• Other expenses related to regulatory violations</li> </ul>
<b>Damage to assets</b>	Events leading to direct decrease in asset's value (e.g., negligence, accident, fire, earthquake) and related damages	<ul style="list-style-type: none"> <li>• Depreciation/write-off of assets due to natural disasters</li> <li>• Loss/destruction of intangible assets (e.g., data)</li> <li>• Costs for adapting premises for business use after a natural disaster or other events</li> <li>• Temporary relocation costs for business continuity</li> <li>• Use of external service providers for business continuity</li> </ul>
<b>Payment for the damage</b>	Payments to third parties related to operational losses for which the bank is responsible	<ul style="list-style-type: none"> <li>• Customer claims for damages due to business interruption (where the bank is responsible)</li> <li>• Payments due to delays in fulfilling obligations</li> <li>• Claims against the bank for theft or loss of customers' confidential information</li> <li>• Irrecoverable erroneous or duplicate payments, mistakenly transferred funds, and unjustified write-offs</li> </ul>

<b>Loss of resources</b>	Losses incurred due to a third party's failure to fulfill its obligations to the bank resulting from operational risk for which the bank is responsible	<ul style="list-style-type: none"> <li>• Loan related operational losses: (e.g., errors in credit documents).</li> <li>• Inability to execute agreements due to unidentifiable third parties, document errors, or incomplete information</li> </ul>
<b>Asset depreciation</b>	Direct reduction in asset value due to market or credit losses arising from theft, fraud, unauthorized activities, or operational risk events.	<ul style="list-style-type: none"> <li>• Failure to deliver/acquire an asset on time and changes in market value</li> <li>• Full recognition of an asset as a loss due to internal fraud</li> <li>• Loss of bank assets/income due to external fraud or theft</li> <li>• Costs incurred for consultants/experts to identify and resolve external security breaches</li> </ul>
<b>Additional judgements (w/o a special category)</b>	<ul style="list-style-type: none"> <li>• Expenses incurred for consultants/third parties (which may include various categories)</li> <li>• Expenses arising from the failure of outsourced services (which may include various categories).</li> </ul>	