‘Approved’
The Central Bank
of the Republic of Azerbaijan
Resolution # 24/3
9 December 2013

Regulations on risk management in banks

1. General provisions

1.1. These Regulations have been developed in accordance with Article 48.1.5 of the Law of the Republic of Azerbaijan on the Central Bank of the Republic of Azerbaijan and Article 34.4 of the Law of the Republic of Azerbaijan on Banks.

1.2. These Regulations set minimum requirements on the launch of a risk management system to allow identify, evaluate, manage, monitor and report on risks in banks operating in the Republic of Azerbaijan within the corporate governance framework.

2. Definitions

2.0. The definitions used herein bear the following meanings:

2.0.1. risk – probability of negative impact of expenses (losses) resulting from presumable or unexpected events on bank capital;

2.0.2. risk management system – system, consisting of the risk management elements specified herein;

2.0.3. bank product – means to present bank implemented activity types;

2.0.4. Chief Risk Officer (CRO) – a member of the Management Board who controls (is accountable for) operations of risk management related structural units;

2.0.5. business units – units, that carry out different types of bank activities and generate risks;

2.0.6. risk assumption capacity – maximum volume of the risk a bank may assume provided that capital, liquidity and other prudential requirements are not violated;

2.0.7. risk acceptance – coverage of possible losses at the expense of bank capital subject to observing capital adequacy requirements;

2.0.8. risk minimization – subdue risks via various regulatory methods;

2.0.9. risk transfer – transfer of operations, that a bank finds risky, to external parties;

2.0.10. risk avoidance – non-implementation of operations, which are riskier than the risk level set by the risk strategy;

2.0.11. risk appetite – the volume of the risk, the bank wants to assume, to hit strategic targets within the risk assumption capacity framework;

2.0.12. risk limit – the maximum risk limit accepted per activity type;

2.0.13. risk profile – generalized level of risks the bank is exposed to;

2.0.14. shock – internal or external, probable and measurable, previously observed event, or the event potentially to affect the bank performance;

2.0.15. stress-testing – tool to evaluate a potential impact of a number of shocks on the bank's financial condition.

3. Risk classification and management

3.1. The key types of risks, banks face when carrying out bank activities, and the reasons for their occurrence are as follows:

3.1.1. Credit risk results from a borrower's failure to perform his/her obligations to the bank timely or in full;

3.1.2. Market risk occurs due to changes in interest rates, exchange rates, shifts in value of securities and commodities in the market. The market risk has the following sub-categories:

3.1.2.1. interest rate risk –risk caused by unfavorable shifts in interest rates;

3.1.2.2. currency risk –risk resulting from adverse changes in foreign exchange rates;

3.1.2.3. capital risk –risk resulting from adverse shifts in value of securities purchased by the bank;

3.1.2.4. commodity risk –risk resulting from adverse changes in commodity prices in the market;

3.1.3. liquidity risk results from failure to timely and effectively discharge planned and unforseen liabilities;

3.1.4. Operational risk occurs as a result of faults and errors by bank staff, problems and deficiencies in information systems and technologies, as well as external events. The operational risk is divided into the following sub-categories:

3.1.4.1. Human resources risk –risk resulting from violation of existing legal acts, faults and errors by bank staff intentionally or unintentionally when executing bank operations;

3.1.4.2. IT risk –risk occuring from problems in bank's information system or technologies;

3.1.4.3. Legal risk –risk resulting from violation of legal acts, non implementation in full, timely or properly, non-adoption of internal regulations, as well as discrepancies and gaps in internal regulations;

3.1.4.4. External risk –risk occuring from damage caused by a third party or nature;

3.1.5. Strategic risk occurs from improper selection of strategic targets;

3.1.6. Reputation risk results from lesser confidence in the bank and negative public perception.

3.2. Banks create a risk management system, adequate to types, the scope of their operations, specifics, environment and complexity of their activities, and risks they face.

3.3. The risk management system includes the following elements:

3.3.1. a risk management strategy;

3.3.2. an organizational structure of risk management;

3.3.3. a risk management policy;

3.3.4. risk limits;

3.3.5. management of risks on new products and services;

3.3.6. consolidation of data and risk reporting;

3.3.7. a contingency plan.

4. Risk management strategy

4.1. Every bank develops a risk management strategy which addresses risk management targets and includes at least the following:

4.1.1. risk appetite in line with bank's strategic targets;

4.1.2. all risks, the bank may be exposed to, as a result of implementation of its activity strategy;

4.1.3. bank's risk approach on introduction of new activity types and systems;

4.1.4. bank capital related strategic targets;

4.1.5. strategic targets related to assets and liabilities structure;

4.1.6. management of risks likely to result from changes in global and macroeconomic environment;

4.1.7. risk management system control;

4.1.8. risk management in emergency situations.

4.2. The risk management strategy is reviewed based upon results of the previous year upon the end of each calendar year within the first quarter of the next year and, if necessary, relevant changes are made.

5. Organizational structure of risk management

5.1. The organizational structure of risk management in banks provide the following:

5.1.1. clearly define risk management auhorities and responsibilities;

5.1.2. coordination and information flow across all levels of the organizational structure;

5.1.3. preventive measures to avoid conflict of interests between structrual units and authorized persons;

5.1.4. independent and transparent decision-making;

5.1.5. effective risk management reporting system.

5.2. Authorities of the bank's Supervisory Board, Risk Management Committee (hereinafter – the RMC), Management Board, the CRO, the risk management unit, business units and internal audit in the risk management process are defined as follows:

5.2.1. The Supervisory Board:

5.2.1.1. ensures launch of an effective risk management system adequate to the bank's risk profile;

5.2.1.2. approves risk management strategy, policy, internal procedures and organizational structure;

5.2.1.3. oversees Management Board's risk management efforts and receives direct reports from the risk management unit;

5.2.1.4. takes decisions on risk management related issues in the bank submitted by the Management Board and the RMC;

5.2.1.5. approves risk limits;

5.2.1.6. evaluates how effective the risk management system is at least annually;

5.2.1.7. approves a contingency plan.

5.2.2. The RMC:

5.2.2.1. reviews risk management strategy, policy and regulations, as well as changes therein and submits to the Supervisory Board for approval;

5.2.2.2. reviews risk limits and submits to the Supervisory Board for approval;

5.2.2.3. determines the selection of relevant methods and tools to identify and evaluate risks and frequency of their implementation;

5.2.2.4. develops a report on status of risks the bank is exposed to and effectiveness of the risk management system and submits to the Supervisory Board;

5.2.2.5. monitors compliance of assumed risks with the bank's risk management strategy;

5.2.2.6. develops proposals to the Supervisory Board on improvement of the risk management system;

5.2.2.7. evaluates the risk management unit, and keeps the Supevisory and Management Boards informed on evaluation findings;

5.2.2.8. develops proposals to the Supervisory Board on authorities of structural units engaged in risk management and internal committees;

5.2.2.9. reviews the contingency plan with the Management Board and submits to the Supervisory Board;

5.2.2.10. holds meetings at least monthly and reports to the Supervisory Board on their results.

5.2.3. The Management Board:

5.2.3.1. ensures implementation of risk management strategy and policy;

5.2.3.2. organizes a risk management process;

5.2.3.3. analyzes risks the bank is exposed to and takes critical measures to eliminate revealed weaknesses;

5.2.3.4. takes a decision on introduction of a new bank product;

5.2.3.5. submits reports to the RMC and the Supervisory Board on risks and their management;

5.2.3.6. create relevant conditions to enable the risk management unit to operate adequately to bank risks;

5.2.3.7. reviews the contingency plan with the RMC and submits to the Supervisory Board;

5.2.3.8. ensures cooperation of bank's other structural units with the risk management unit, as well as takes measures to prevent interventions to its operations.

5.2.4. The Chief Risk Officer:

5.2.4.1. develops and submits to the RMC the risk management strategy and policy considering opinions of the Management Board and the CFO;

5.2.4.2. coordinates risk management related activities of the Management Board and structural units;

5.2.4.3. ensures reliable, transparent, single-package and timely development of periodic reports addressing types and the scope of bank risks;

5.2.4.4. issues proposals to the RMC and the Supervisory Board on improvement of the risk management system;

5.2.4.5. ensures compliance of risks, the bank is exposed to, with its risk assumption capacity, the risk management strategy and prudential requirements on risk management;

5.2.4.6. takes measures to raise knowledge and skills of the staff of structural unit engaged in risk management;

5.2.4.7. attends Supervisory Board meetings to review the risk management strategy, as well as to discuss risk management related issues.

5.2.5. The Risk Management unit:

5.2.5.1. coordinates risk management efforts;

5.2.5.2. develops internal risk regulations, as well as changes therein;

5.2.5.3. monitors compliance with the risk management strategy and policy and submits reports on deviations to the RMC and the Management Board;

5.2.5.4. issues proposals to the RMC and the Management Board on estimation of and changes to limits on acitivity types with bank's related structural units;

5.2.5.5. develops and monitors implementation of risk mapping;

5.2.5.6. permanently controls compliance with risk limits and immediately informs the CRO on violations;

5.2.5.7. does work on selection and introduction (with bank's related structural units) of methods and models to identify and evaluate risks;

5.2.5.8. submits to the Management Board, the RMC and the Supervisory Board a report on risk evaluation, analysis and findings;

5.2.5.9. isues opinions on all processes covering the bank performance, new products and services to recognize and manage risks;

5.2.5.10. conducts stress-testing with related structural units and develops an actions plan to mitigate identified risks;

5.2.5.11. analyzes information received from bank's other structural units to manage risks;

5.2.5.12. issues proposals to the RMC to establish and improve effective control procedures adequate to manage risks;

5.2.5.13. develops and submits to the RMC and the Management Board a contingency plan with bank's related structural units;

5.2.5.14. renders methodological assistance to bank's related structural units to manage risks.

5.2.6. Bank's business units:

5.2.6.1. manage risks within their authorities in their daily activities;

5.2.6.2. comply with related risk limits.

5.2.7. Internal audit:

5.2.7.1. reviews risk management system effectiveness and adequacy;

5.2.7.2. submits reports, proposals and recommendations to the Supervisory Board and the Audit Committee on review findings;

5.2.7.3. exchanges information with the risk management unit.

6. The risk management policy

6.1. The risk management policy should encompass at least the following:

6.1.1. organization of risk management and segregation of authorities;

6.1.2. the risk management process on bank's activity types, business processes and information systems.

6.2. The risk management policy is reviewed at least annually and, if necessary, relevant changes are made.

7. The risk management process

7.1. The risk management process covers procedures and evaluation methodologies critical to effectively manage risks in the bank.

7.2. Methods to identify and evaluate risks arising in bank performance are applied in line with the scope and complexity of the bank's risk profile. The applied methods and related assumptions are assessed on a regular basis.

7.3. The risk evaluation frequency should be adequate to the scope and specifics of risks arising in bank performance.

7.4. Risks are identified at least through the following methods:

7.4.1. Risk mapping addresses risks, the bank may be exposed to, internal and external reasons generating risks, other risks and possible losses likely to be generated by the risk, as well as determines the frequency of risk occurrence, risk management and evaluation tools, a responsible person or a structural unit on risk management. The risk mapping is reviewed and, if necessary, changes are made at least twice a year;

7.4.2. Enquiries are used to detect various risks which are hard to identify. The topic of enquiries is based upon bank's risk indicators. Enquiries are developed clearly, concisely and in line with the topic;

7.4.3. Empirical analyses (based upon true historical data). The bank regularly analyses based upon its and/or other banks' empiric data (e.g. on losses) to identify risks;

7.4.4. Early warning systems are used to monitor bank risks. The early warning system ensures issue of probabilities of occurrence of various threats as a result of approximating of various coefficients and factors used in bank activities to limits set thereof and information on risks.

7.5. Risks identified by the risk management unit are groupped under relevant categories, results documented and relevant reports developed.

7.6. Risks are evaluated based upon findings of the risk identification process. The bank's risk assumption capacity is identified based upon analysis of quantitative and qualitative indicators and the risk level estimated. Methods used in risk evaluation should be comprehensively explained in internal regualtions. At least the following models should be used for evaluation:

7.6.1. Value at risk (VAR) models. VAR is the maximum amount of expected loss at a previously set level of confidence over a specified time (at least 1 year). That amount reflects the size of expected bank losses on various risk types. The minimum confidence level is set 99% when applying any VAR model;

7.6.2. The portfolio at risk (PAR). This tool assists to evaluate the credit risk groupping loans on delinquencies. Delinquency groups should cover monthly periods up to 1 year, annual periods up to 2 years and over 2 years overall. Groups of this period may be groupped by the bank on shorter periods;

7.6.3. Insolvency equivalent risk. Insolvency probability is assigned per delinquency group and the scope of potential insolvency of total portfolio is forecast. The insolvency probability is determined based upon bank's empirical data. The higher the delinquency period, the higher the probability is, which is set 100% on credit groups with over 1 year delinquency;

7.6.4. Vintage analysis. This tool ensures more effective mitigation of problems on the portfolio creating a detailed analysis opportunity of delinquent

loans on dates of issue, unit, administrator, loan officer and other criteria. Additional analysis indicators may also be set along with the above criteria based upon the credit portfolio structure;

7.6.5. Stress-testing. Every bank develops and updates annually stress-testing models depending on the size and complexity of its operations to identify and evaluate events likely to have an adverse impact on its risk profile:

7.6.5.1. The stress-testing model considers probability of fluctuation of each shock up to the most unfavorable level. These shocks concentrate components of market, credit, liquidity, operational and other risks;

7.6.5.2. Stress-tests identify resilience of bank capital to shocks, maximum loss the bank may be exposed to as a result of shocks and other gaps in bank performance;

7.6.5.3. 'Very unfavorable', 'favorable' and 'probable' scenarios are developed when conducting stress-tests, separate criteria and shocks are set per scenario including probabilities. The bank uses empirical data, probable scenarios considering potential risks and maximum losses when developing stress-tests;

7.6.5.4. stress-tests are conducted at least semiannually;

7.6.5.5. an action plan is developed and implemented to prevent the risks identified on stress-test findings;

7.6.5.6. the bank develops a program on elimination of potential capital shortfall depending on stress-test findings.

7.7. Quantitative models used at risk evaluation should comply with the countercheck principle, which allows determine how adequate the applied method is, comparing expected and actual results. If the previously estimated expected result differs from the actual one incisively, models undergo relevant changes and are aligned to current macro- and micro-economic situation.

7.8. Stress-test findings are attached with prudential statements of the relevant period and submitted to the Central Bank.

7.9. A report is developed on findings of adopted and applied methods and models. The RMC analyses and issues instructions to the risk management unit with respect to risk acceptance, minimization, transfer, as well as risk avoidance to effectively manage risks.

7.10. If the CRO disagrees with resolutions of the Management Board and internal committees on issue of loans, investments and new products, the Management Board brings up the matter to the Management Board for discussion within 7 (seven) business days (with the CRO's written substantiation). The Supervisory Board takes a decision on the issue within 15 (fifteen) business days. Within that period the implementation of resolutions by the Management Board and internal committees on related issues is suspended.

7.11. The CRO should be a member of decisionmaking internal committees on risk management, remuneration, issue of loans, investments and new products.

7.12. Head of the risk management unit should have at least 4 (four) year work experience on risk management and be appointed by the Supervisory Board at a request letter by the RMC. Unit staff should have access to bank's any database, internal operating systems, as well as internal audit reports.

8. Risk limits

8.1. Limits should be set on measurable credit, market, liquidity and operational risks, as well as other existing risks faced by the bank to contain them from the moment they occur.

8.2. Risk limits are set on business unit's staff, structural units and accross the bank in line with the bank size, risk profile, activity directions, complexity of products and services.

8.3. Risk limits are reviewed at least monthly, and adjusted to existing market conditions and the bank strategy.

9. Management of risks on new products and services

9.1. The bank maintains a preparatory process prior to introduction of a new product or service, which includes analysis of compliance of a product or a service with the bank strategy and identification of product related risks.

9.2. The following is considered in line witn the bank's risk policy when introducing a new product or a service:

9.2.1. comprehensive analysis of a product or a service;

9.2.2. evaluation of risks likely to generate from products or services;

9.2.3. analysis of effect of products or services on bank's financial condition;

9.2.4. identification of resources criticalfor effective risk management of new products or services;

9.2.5. management of probable risks.

9.3. The bank evaluates new products or services upon their introduction in the context of their impact on risk profile and consider findings of this evaluation if similar products or services are offered in future.

10. Data consolidation and risk reporting

10.1. The bank creates an adequate risk data consolidation and reporting framework to identify, evaluate, manage and control credit, market, liquidity, operational and other available risks to be approved by the Supervisory Board.

10.2. A management information system (MIS) is launched in the bank to consolidate risk data and ensure effective risk reporting, which:

10.2.1. identifies, evaluates, manages and controls daily risks;

10.2.2. checks compliance with established rules and limits;

10.2.3. traces trends in risk indicators;

10.2.4. develops reports in the format established under prudential requirements and internal regulations;

10.3. The MIS should be capable to trace risk limits and, if they approximate to pre-set level, inform the Management Board and other users.

10.4. Bank's Supervisory Board, Management Board, RMC and other related staff should have access to MIS generated reports.

10.5. The riks management unit develops analytic reports covering at least the following directions and submits to the RMC, the Management and Supervisory Boards:

10.5.1. key risks and their structure;

10.5.2. capital structure and its adequacy;

10.5.3. analysis of current and future capital requirements;

10.5.4. bank's liquidity position;

10.5.5. assets and liabilities in a foreign currency and an open currency position;

10.5.6. usage of risk limits;

10.5.7. stress-test findings.

10.6. Data in the reports should be clear, accurate and comprehensive enough for decision-making.

11. Contingency plan

11.1. Every bank develops a contingency plan, which includes measures to be taken to prevent risks arising in emergency situations and ensure bank's business continuity.

11.2. The contingency plan should address the following:

11.2.1. classification of emergency situations;

11.2.2. authorities of responsible persons to recover activities disturbed in emergency situations;

11.2.3. measures to be directed at preventing various risks in emergency situations;

11.2.4. source of capital to be attracted in emergency situations;

11.2.5. the policy to protect the bank from the reputation risk in emergency situations;

11.2.6. classification of bank operations and activity types on the significance level emergency situations.

11.3. The bank's contingency plan is reviewed at least annually and, if necessary, undergoes relevant changes. When reviewing the contingency plan, various scenarios are tested on internal and external factors and test findings are considered in changes to be made to the plan.

11.4. Each bank employee, involved in mitigation of risks in emergency situations, is informed on the contingency plan and changes therein by the risk management unit with relevant trains conducted no less than once a year.