CODE
050.0102 N. 16.04.13

April 16, 2013 No 102-N

ON APPROVAL OF "MINIMUM REQUIREMENTS FOR IMPLEMENTATION OF INTERNAL CONTROL OF BANKS" REGULATION 4 AND REPEALING RESOLUTION NUMBER 71-N DATED MARCH 11, 2008 OF THE BOARD OF THE CENTRAL BANK OF THE REPUBLIC OF ARMENIA[1]

Intending to increase the effectiveness of internal control system in banks, as well as to bring the requirements of the internal control system of banks to compliance with the principles of the Basel Committee of Banking Supervision,

having regard to the Law of the Republic of Armenia "On the Central Bank of the Republic of Armenia", Article 20 (e)(kb), the Law of the Republic of Armenia "On Legal Acts", Article 16, Article 72(1), the Board of the Central Bank of the Republic of Armenia

d e c i d e s:

1. To approve "Minimum requirements for implementation of internal control of banks" Regulation 4, pursuant to Appendix (attached).
2. From the moment of entering of this decision into force, to repeal Resolution No 71-N of the Board of the Central Bank of the Republic of Armenia, dated March 11, 2008. "On approval of minimum requirements for implementation of internal control of banks, repealing Resolution No 250-N of the Board of the Central Bank of the Republic of Armenia, dated October 12, 2004 and repealing Resolution No 40 of the Board of the Central Bank of the Republic of Armenia, dated March 16, 1999".
3. This decision shall enter into force on July 1, 2014.

Chairman of the Central Bank
of the Republic of Armenia **Arthur Javadyan**

April 18, 2013
Yerevan

---

[1] This Regulation includes the amendments and supplements and all other changes endorsed under the following Resolution of the Board of the Central Bank:
No. 256-N, dated 08.12.15, No. 38-N, dated 30.03.18, No. 148-N, dated 11.10.19

Appendix
Approved by the Decision No 102-N of the Board
of the Central Bank of the Republic of Armenia
on April 16, 2014

MINIMUM REQUIREMENTS FOR IMPLEMENTATION OF INTERNAL CONTROL OF BANKS

REGULATION 4

PART 1. GENERAL PROVISIONS
Chapter 1. General provisions

1. This Regulation defines the minimum requirement for implementation of internal control in banks.
2. This Regulation is used by the banks and the branches of foreign banks, operating on the territory of the Republic of Armenia, as much as it is applicable.

PART 2. INTERNAL CONTROL SYSTEM
Chapter 2. Internal control system

3. Internal control system is a set of internal organizational structure, business processes, risk management system, reporting, as well as measures of control over them. Internal control system is aimed to keep the bank's assets, ensure the business continuity of the bank, timely identify, measure and continuously manage the inherent risks of the bank's activities, ensure compliance of accounting and financial reports with current standards, increase efficiency of transactions, ensure compliance of bank's activities to current legislation and internal legal acts of bank.
4. The main objectives of internal control are:

1) disclosure and management of risks inherent to banking activity, efficient organization of bank's activities and efficient management of personnel (operational objective),

2) ensuring reliable, complete and in time provision of necessary accounting, financial and other reports for decision making in the bank, as well as necessary information flows within bank (informational objective),

3) ensuring compliance of bank's activities with the requirements of laws and other legal acts of the Republic of Armenia, internal legal acts (policies, procedures, rules, regulations, orders, guidelines, etc.), approved by authorizes management authority of bank (compliance objective).

5. The internal control system of the bank includes internal control systems of the bank's head office and branches, which forms a logical single whole and is based on the same criteria and principles.

6. Separate internal control systems of the bank and its subsidiaries and/or associated and/or controlled companies (if such companies exist) form a logical single whole and are based on the same criteria and principles, when:

1) activities or operations of the bank and its subsidiaries and/or associated and/or controlled companies are affiliated, or

2) subsidiaries and/or associated and/or controlled companies of the bank have significant influence on financial results, financial condition or reputation of the bank.

7. Implementation of business processes can fully or partially be ensured by subsidiaries, associated or controlled companies of the bank insofar as it does not contradict the legislation of the Republic of Armenia.

8. Bank ensures that its internal control system satisfy at least the requirements defined by this Regulation. If the profile, volume of separate operations provided by the bank, or the financial results of the bank from such operations are not significant for the bank or do not create significant risks, then the bank might not maintain the requirements of internal control for such operations, defined by this Regulation, with the evidence, approved by the board resolution of the bank.

9. The bank's board (hereinafter Board), executive body, oversight functions, bank's all employees within their responsibilities, defined by laws and/or other legal acts, are responsible for formulation, operating and effective continuous monitoring of the bank's internal control system. The responsibilities of the Board according to this Regulation are implemented by adopting the bank's internal control standards.

10. The internal control system of a bank is described by its internal acts, which can be presented as policies, procedures, rules, regulations, orders, guidelines and other acts.

11. Internal control system, its separate parts are assessed and, if necessary, are revised, in frequency defined by the Board, but not less than once a year, and in case of changes of environment, as well as in cases of identification of new risks or any significant risk, significant deficiency or gap of existing system that was previously out of control, the assessment and revision takes place in reasonable terms. Significant changes and their

arguments, as well as the arguments of the absence of need of such changes are being properly documented.

12. Changes of the environment are:

1) change of the business-strategy of the bank,
2) significant changes of the operational environment,
3) significant changes of the personnel,
4) new or modified information systems,
5) new or modified technologies,
6) new services, types of activities,
7) change of the organizational structure,
8) bank's restructuring,
9) establishment of subsidiaries and/or affiliated and/or controlled companies by the bank, participation in subsidiaries or affiliated companies,
10) extension of international transactions,
11) significant changes in economic, financial and/or banking regulation,
12) appearance of other internal and external circumstances, which have significant influence on bank's activities and risk level.

13. Internal control system of the bank ensures implementation of secure and normal banking activity, taking into consideration the profile of the bank's activity, its existing and possible risks, requirements of laws and other legal acts, business traditions and environment of bank's activity.

14. Deficiencies and gaps of internal control system, detected by the bank's executive body, internal oversight functions and bank's personnel, are presented to the Board in the form and terms, defined by the bank's internal legal acts.

15. Bank ensures availability of its internal legal acts, describing its internal control system, to the bank's personnel. Bank ensures that its personnel are informed about provisions of internal legal acts, describing bank's internal control system, within the functions operated by the personnel.

16. Appropriate control mechanisms should be introduced in the bank for each significant business process of the bank. Control mechanisms can be preventive (to prevent undesirable results), detective (to detect undesirable transactions), as well as removing undesirable results (to remove undesirable results). The control mechanisms to detect, prevent and remove undesirable results/transactions are the followings:

1) regular study and assessment of bank's activity by management bodies (by requiring reports from employees about their performance, asking the employees some questions about their work and getting answers, clarifications and explanations),

2) ensuring physical defense of bank's property and more important documents (including loan and deposit contracts), which assumes that bank's property and more important documents are protected from loss, unauthorized removal or usage,

3) definition and maintenance of internal limits, allowed deviations from those limits (for example, for single transactions, for indicators of activities, etc.)

4) in case of exceeding the limits, making decisions, approving transactions and/or permission of transaction by appropriate authorized managers,

5) appropriate segregation of duties of employees and recommendation of duties that are free from conflict of interests,

6) jointly storing of property ad records, when two or more people are equally accountable for certain processes (for example, when each of two or more keys or passwords, that should be used for getting right to enter bunker, archive or other depository, are being entrusted to separate individuals),

7) double checking,

8) comparison of data and records,

9) regular inventory,

10) requirement of double or multiple signatures,

11) giving recommendations to remove detected violations, shortcoming, undesirable outcomes, that occur as a result of them, as well as implementing appropriate and timely control over such recommendation and, if necessary, applying appropriate sanctions,

12) other control mechanisms by the bank's discretion.

PART 3. ORGANIZATIONAL STRUCTURE, BUSINESS PROCESSES, HUMAN RESOURCES MANAGEMENT

Chapter 3. Organizational structure, business processes, human resources management

17. Internal control system, concerning bank's organizational structure, at least includes:

1) detailed description of the bank's organizational structure in graphical and/or text form,

2) properly segregated duties and authorities of bank’s divisions and employees. During the segregation of duties and authorities, at least possible cases and areas of conflict of interests are disclosed and controlled.

18. Bank’s internal control system, concerning bank’s business processes, at least includes:

1) description of bank’s business processes, which includes detailed description of all commercial transactions and managerial procedures, implemented by the bank, in graphical or text format, including:

a. the sequence of steps for implementing the described business process,
b. the final result of the business process, in form of a document, transactions, information, etc.,
c. the terms of implementing the business process by steps,
d. the connection among separate business processed of the bank,
e. necessary links to laws, other legal acts or other internal acts, regulating the process.

2) defined and segregated duties and authorities of employees, involved in the business process,

3) internal control mechanisms to prevent or minimize the risks of implementing separate steps of business processes,

4) the ways to provide necessary information for sustainable and effective implementation of the business process, as well as information flows within the bank (divisions, managers, employees, etc.).

19. Implementation and accounting of bank’s separate process and transaction (including further control (post control)) from the beginning to the end is not done by one or affiliated people.

20. Internal control system, concerning human resources management policy (HR policy), at least includes:

1) the procedure of hiring and dismissal of employees,
2) the principles of employees’ trainings,
3) the policy and procedure of employees’ remuneration, reward or other form of material stimulation (hereinafter` remuneration policy) and applying disciplinary sanctions,
4) the procedure of employees’ promotion and rotations,
5) the principles of vacation policy,
6) the procedure of appraisal of employees’ performance,

7) job descriptions of professional employees,

8) professional ethic's guide.

21. All employees of the bank are informed in written form at least about the risks, related to their job responsibilities, their role in the internal control system, the requirements to their behavior at workplace and out of it, the consequences of their abuses and gaps.

22. The remuneration policy, approved by the Board, meets at least the following requirements:

1) does not stimulate the unreasoned risk-taking by the bank's employees, as well as unfair treatment towards the clients,

2) is consistent with the risk appetite and long-term goals of the bank, approved by the Board,

3) at least applies to the bank's management and all those employees, whose activities can have significant impact on the risk level of the bank,

4) at least possible cases and areas of conflict of interests are being disclosed and controlled during designing, implementing and monitoring of remuneration policy. To exclude possible cases of conflict of interests, which can hinder effective work of employees, involved in oversight functions, the mechanisms of floating remuneration can be used when defining the remuneration of oversight function employees, based on their work performance. The remuneration of employees, involved in oversight functions, can be derived from the results of the oversight function to meet its goals.

5) when using floating elements of remuneration, an effective combination of fixed and floating elements of remuneration is being ensured

23. In case of defining a floating element of remuneration, based on the results of activities,

1) it is ensured, that the criteria to assess the results of activities are clear and objectively measurable,

2) the assessment of the results of activities can be based on both financial and non-financial criteria,

3) not only the results of activities of the separate individual are being taken into consideration, but also the results of activities of the appropriate business unit, as well as the total results of bank's activity (if applicable),

4) when implementing a growth of remuneration, based on the results of activities, both current and future risks, connected with the activity, are being taken into consideration. Taking into consideration the probability of change of results of activity and

risks, connected with them, during the time, the assessment of the results of the activity is being done for a long-time period, if applicable,

5) the limits of floating elements of remuneration are being defined, which are consistent with the bank's capital management strategy and bank's ability to maintain an effective level of capital, taking into consideration the internal targets of capital and legal requirements.

PART 4. RISK MANAGEMENT

Chapter 4. Risk management system

24. Risks, to which the bank is imposed or can be imposed, include internal or external circumstances, which can threaten the continuity of the bank's activity and have a negative impact on the bank's capital and/or earnings, as well as its reputation.

25. Bank ensures the existence of effective system of risk management, approved by the Board, which is consistent with the risk nature of bank's activity, volume and complexity of business processes.

26. Risk management system of the bank at least includes:

1) risk management strategy, which defines bank's general approaches/goals, concerning risk management. During the development of risk management strategy, at least business program and business processes of the bank (including the processes outsourced by the bank), approved by the Board of the bank, are being taken into consideration,

2) risk appetite of the bank, approved by the Board, i.e. the part of risks, that the bank is able and wiling to accept without threatening its financial stability and normal activity,

3) individual risks management policies, which at least define:

a. reasonably predictable and significant risks, inherent to the bank's activity, by types. At least, the risks, set in point 27 of this regulation, as well as any additional risks arising from being a member of a group (if applicable), should be reviewed by the bank,

b. acceptable limits of the risk for each type of risk, cases and sizes of allowed deviations from the defined limits,

c. implementation of mechanisms of risk reduction (for example, insurance, hedging, etc.),

4) processes and tools (including models (if applicable)) of identification, assessment, mitigation, monitoring and reporting of individual risks,

5) duties and authorities of bank's individual business units and employees, involved in risk management process,

6) the policy of bank's internal capital adequacy assessment process (ICAAP), according to Chapter 5 of this Regulation:

27. Bank develops a valid risk assessment system for assessment of at least the following risks:

1) Credit risk
2) Market risk
3) Liquidity risk
4) Operational risk
5) Reputational risk
6) Strategic (business model) risk
7) Country risk

(Point 27 was supplemented by Resolution No. 38-N dated 30.03.18)

28. ***Credit risk*** is the probability, that the counterpart will violate the provisions of the contract, signed with the bank, which will have a negative impact on the bank's earnings and/or capital, despite the fact if the transaction was reflected in the bank's balance sheet or was acted as an off-balance sheet item. Credit risk occurs at any time, when the resources are being provided, invested or anyhow acceptable to the borrower (counterpart) and/or a right of claim occurs at the bank and/or the bank gets liability to provide resources.

29. Bank should have a developed methodology, which will allow assessing credit risk both for a single borrower/counterpart and the whole credit portfolio.

29.1. In case of unhedged borrowers, the bank should assess also the credit risk, arising from the change of exchange rates. Meanwhile, the borrower should be considered as unhedged, if his/her inflows in the currency of claim (loan, credit, leasing, factoring) during the last year were less or, according to the bank's projections, can be less in the upcoming one year, than the money outflows (including all the payments, made on the claim), reflected in the same currency, and the FX risk is not hedged at the given bank.

(Point 29.1 was added by Resolution No. 38-N dated 30.03.18)

30. When using internal rating systems as a credit risk assessment tool by the bank, such systems should give opportunity to detect and assess the credit risk of individual

tools/borrowers. Internal ratings should be applied not only to problematic, but also to all assets.

31. Bank should implement a credit risk analysis for individual portfolios, identifying portfolio problems, including risk concentrations. Special attention should be paid to large exposures. The analysis should be documented.

32. Bank should have a methodology to identify, measure, monitor and manage credit risk concentrations. The methodology should cover different types of credit risk concentrations, including:

1) credit risk concentrations by a single economic area,
2) credit risk concentrations by a single geographical area,
3) credit risk concentrations among the people, whose financial conditions are depending on the price of the same product/service, or who provide similar activity/act in the same market/adopt similar investment policy,
4) large exposure provided to a concrete individual or affiliated individuals,
5) indirect concentrations of credit risk, for example, by a same type of collateral, concentration by a single guarantor, etc.

33. The approaches of credit risk concentrations management should be clearly documented, and the definition of credit risk concentration, their limits and their calculation procedure should be provided by these documents. Limits can be applied to the bank's capital, total assets or credit portfolio.

34. Bank reviews the used amounts of credit lines, provided by the bank, on a daily basis. Based on that, the bank regularly assesses its existing total and net risks (taking into consideration the existence of collateral and guarantees).

35. Bank develops a methodology and processes to manage other risks (in particular, impossibility to timely realize the collateral, avoidance/postponement by the guarantor to meet his/her obligations, imperfection of documents, certifying the pledge, or existing of documents, consisting legal problems) occurred by using credit risk mitigation mechanisms (financial collateral (according to point 26 of Appendix 3 "Credit risk calculation" of "Regulation of banks' activities, prudential ratios of banking activities" Regulation 2 adopted by Resolution No 39-N of the Board of the Central Bank of the Republic of Armenia on February 9, 2007), guarantees/warranties). The effectiveness of such methodology and processes should be regularly assessed.

36. ***Market risk*** is the probability that fluctuations of market prices (interest rates, FX rates, prices of equity instruments, etc.) will have a negative impact on the bank's capital and/or earnings.

37. Depending on the level of bank's exposure to market risk, the internal process of risk assessment can be based on Value-at-Risk or other models and/or results of stress-tests, including the assessment of risk concentrations and the risk of liquidity problems in the stressful market conditions. The implemented models should give an opportunity to identify and measure the risks, arising from all commercial transactions. In the case of changes of bank's trading instruments, as well as the strategy of commercial transactions implementation, the methodologies under the risk measurement models and/or stress tests should also be appropriately changed.

38. ***Interest rate risk*** is the probability, that undesirable fluctuations of market interest rates will have a negative impact on the bank's capital and/or earnings. It can be reflected by a general risk and/or a specific risk. General risk refers to such fluctuations of values of instruments, sensitive to interest rate risk, which are connected with general movements in the market, for example, changes of profitability curve. Specific risk refers to a concrete instrument, whose interest rates fluctuations deviate from the market level, due to individual factors, for example, credibility of the securities issuer.

39. Bank ensures the existence of a methodology, developed for measurement and management of the interest rate risk of the financial instruments, held to maturity, as well as for assessment and maintenance of capital requirement, necessary for such risk.

40. The concentrations in the bank's trading book should be measured and effectively managed, and the information about bank's positions, generating the concentration, should be regularly presented to the executive body and the Board. Special attention should be paid to the portfolios, consisting of non-diversified and low-liquid instruments.

41. ***Foreign exchange risk*** is the probability, that FX rates fluctuations will have a negative impact on the bank's capital and/or earnings. It refers to both commercial and credit operations.

42. Taking into consideration the low predictability of FX risk, the bank should have necessary resources (appropriately specialized staff, database, information processing systems, etc.) for measuring and managing the FX risk, whose adequacy and effectiveness should be regularly assessed.

43. Depending on the nature and complexity of FX operations, appropriate processes should be implemented in the bank, which should be addressed to manage both the general FX risk of the bank, and the FX risk of the concrete instrument or specific customers.

44. Bank should have appropriate processes for identification and management of the FX risk of implementation of new instruments or operations in new markets (in the existence of plans to implement new instruments or operations in new markets). The toolkit of FX risk management/hedging should be beforehand approved by the Board or appropriate committee, before implementation of new instruments/operations in new markets.

45. Bank's documents, concerning the management of FX risk, should at least define all possible main sources of FX risk and the assessment of the impact of fluctuations of FX rates on the bank's operations, as well as the results of bank's activity. The assumptions under the risk assessment system should be clear and understandable for risk managers and the bank's management.

46. Bank's documents, concerning the management of FX risk, describe the internal control system of the FX risk management process and the frequency of assessment of adequacy and effectiveness of that system, duties and authorities of appropriate people or divisions, responsible for the assessment of internal control processes.

47. ***Liquidity risk*** is the probability, that the bank will not have enough liquid resources to meet its obligations when they come due. It can appear in two ways: **impossibility to attract resources** and **assets liquidation risk**. The first assumes that the bank will not have an opportunity to attract resources from market in time with such cost, which is available to other market participants (for example, in case of decrease of the bank's rating or reputation). In the second case, the bank is not able to sell its assets in market without price losses (in case of low-capacity and non-liquid market conditions, when there are significant price fluctuations, or in case of insufficient demand in the market towards the assets of the concrete bank).

48. Bank assesses the liquidity of those markets, where it provides activity, as well as provides and maintains capital, adequate to its liquidity level, taking into consideration, that the size of bank's capital can impact on the ability of the bank to attract liquidity in stressful conditions.

49. Bank implements an effective valid assets-liabilities management system.

50. Bank assesses inflows and outflows of its cash on a monthly basis, including the share of those term liabilities, whose repayment requirements can be presented at any time.

51. ***Operational risk*** is the probability of loss, occurring as a result of insufficient or failed internal processes, systems and human factor or external factors, which can have a negative impact on the bank's capital and/or earnings. Operational risk includes also the legal risk.

52. ***Legal risk*** is the probability that the provisions of contracts, court procedures, court decisions, decrees or other legal processes will interrupt or have a negative impact on the bank's activities.

53. Bank's sensitivity to operational risk, including the possibility and level of transferring out the operational risk (for example, by outsourcing, insurance) is defined by the bank's policy.

54. ***Reputational risk*** is the probability that the negative public opinion (true or false) about the bank will bring to a reduction of number of clients, reduction of the size of transactions with counterparts/clients, costly judicial processes and reduction of profitability. Reputational risk can incur also liquidity problems, fall of equity prices, etc.

55. ***Strategic (business model) risk*** occurs in case of choosing an inappropriate business strategy or in case of negative changes in assumptions, indicators, goals or other factors under the strategy.

55.1. ***Country risk*** is the probability that economic, social and (or) political conditions or event, taking place in another country, will have a negative impact on the bank's risk profile, liquidity, capital and (or) earnings.

(Point 55.1 was added by Resolution No. 38-N dated 30.03.18)

55.2. The bank should develop respective rating systems for those countries, with the residents of which the bank or the bank's customers conduct such financial operations, which are material for the bank from perspective of country risk.

(Point 55.2 was added by Resolution No. 38-N dated 30.03.18)

55.3. The bank should set respective limits for the countries, specified by point 55.2 of this Regulation, and the operations, conducted with such countries. Meanwhile, the limits, specified in this point, should be revised at least annually.

(Point 55.3 was added by Resolution No. 38-N dated 30.03.18)

55.4. The requirements, specified by points 55.2-55.3 of this Regulation, might be applied not only to solo countries, but to the whole region, if, according to the justified opinion of the bank, the countries of the region are exposed to the same or similar country risk.

(Point 55.4 was added by Resolution No. 38-N dated 30.03.18)

56. Any operation that can bring to an unauthorized deviation from the risk management strategy, risk appetite and/or risk limits, approved by the bank's Board, should be discussed in details and presented to the Board's approval.

57. In case of implementation of new operations or tools by the bank, the bank assesses their possible impact on the riskiness level of the bank's activity, if necessary, making changes in risk management and internal control systems.

57.1. In case the bank uses internal models in the process of risk management (definition of risk appetite, risk measure, internal assessment of capital adequacy, projection of financial indicators), the bank should disclose and minimize the risk, arising from wrong description of the parameters, used in the model, wrong assessments, incomplete hypothesis and (or) assumptions, inaccurate mathematical calculations, wrong or incomplete data, wrong or incomplete implementation, insufficient monitoring and (or) control.

(Point 57.1 was added by Resolution No. 38-N dated 30.03.18)

57.2. For each internal model, used by the bank in the process of its risk management, the bank should have internal acts and procedures, which describe the whole lifecycle of development and implementation of the model, including:

1) assessment of necessity of model implementation,

2) model development,

3) model assessment,

4) model approval,

5) conduction of regular monitoring of the model, including its back testing (at least annually),

6) conduction of changes and adjustments of the model (if necessary).

(Point 57.2 was added by Resolution No. 38-N dated 30.03.18)

57.3. Each internal model, used by the bank in the process of its risk management, should pass an assessment before its approval, in case of which the bank should ensure the independence and impartiality of the assessment process.

(Point 57.3 was added by Resolution No. 38-N dated 30.03.18)

57.4. The requirements of points 57.2 (except for the requirements, specified by sub-points 5 and 6 of point 57.2 of this Regulation) and 57.3 of this Regulation are not mandatory for those banks, which use the internal models, developed by their parent organizations, provided that there are enough justifications, that the parent organizations have implemented adequate mechanisms of model development, assessment and approval.

(Point 57.4 was added by Resolution No. 38-N dated 30.03.18)

58. Risk management process is being reviewed and, if necessary, revised with the frequency, defined by the Board of the bank, to ensure promptness and validity of the process. The justifications of absence of necessity to revise the risk management process

should be properly documented. The main areas, subject to review/revision, at least include:

1) adequacy of bank's internal capital adequacy assessment processes (ICAAP) to the nature, volume and complexity of the operations, provided by the bank,

2) disclosure of large exposures and risk concentrations,

3) validity and completeness of input data, used during the assessment of bank's level of risk,

4) justification and effectiveness of the methods and scenarios, used during the assessment of the bank's level of risk,

5) testing and analysis of assumptions and used input data.

59. The bank's Board is responsible for developing, functioning and ensuring the continuous monitoring of the effectiveness of risk management system. The executive body is responsible for effective implementation of risk management system, as well as ensuring the effective circulation of procedures and other internal legal acts, approved by the Board, within the whole bank.

Chapter 5. Internal capital adequacy assessment process (ICAAP)

60. Bank ensures the existence of capital, adequate to its risks, as well as develops and uses effective mechanisms of risk monitoring and management.

61. Bank's executive body is responsible for developing the internal capital adequacy assessment process (ICAAP), defining a benchmark level for capital, adequate to the bank's riskiness profile and risk management environment, as well as implementing a system for matching the bank's capital level with its risks.

62. Bank's executive body and the Board consider the capital planning as a required element to achieve the bank's strategic goals. Bank's development programs clearly define the bank's capital requirement, planned capital investments, desirable level of capital as well as possible sources of capital replenishment.

63. As a part of the bank's risk management system, the bank implements an internal capital adequacy assessment process at least on a quarterly basis, which should be consistent with the nature, volume and complexity of risks of the bank's activities.

64. The main elements of the internal capital adequacy assessment process are:

1) appropriate policies and procedures that define the criteria to consider the risks as significant, ensure the identification, measurement of all significant risks by the bank and the flow of information about them (during the assessment of capital adequacy, all

significant risks, taken by the bank, are being taken into consideration. The impact of external factors, such as business cycles and macroeconomic environment, on capital requirement is also being assessed),

2) process of complying the capital level with the level of risks undertaken,

3) process of assessment of adequacy of capital to existing and potential risks, based on the bank's strategy and business program,

4) implementation of internal control and internal audit reviews of capital management process.

65. The Board of the bank approves the ICAAP policy, which at least includes:

1) description of necessary procedures for implementation of ICAAP. ICAAP implementation procedures should be consistent with the bank's organizational structure and risk management system,

2) procedures of collection, protection, checking the validity of information, used during the calculations, made during the ICAAP, as well as the bank's requirements towards the quality (completeness, validity, etc.) of used data,

3) the circumstances, under which an additional ICAAP should be implemented,

4) the main responsible people for ICAAP implementation,

5) the methods of usage of ICAAP results during the managerial decision making as well as the risk management processes,

6) the procedures to make ICAAP results available to the interested divisions.

66. Bank develops an appropriate risk monitoring and reporting system, which will allow assessing how the change of the bank's risk level impacts its capital requirement. With a defined frequency, the bank's executive body and the Board get a report from the people, responsible for risk management, about the bank's risk level and adequate capital requirement. The content of the report should allow the management bodies:

1) to assess the level of significant risks, their trends and impact on the bank's capital level,

2) to assess justification of assumptions under the internal capital adequacy assessment processes,

3) to decide, whether the bank ensures enough capital level to withstand the risks and whether it complies with capital adequacy targets, defined by the bank,

4) based on the reports, to assess the future capital requirement and, if necessary, to make appropriate changes in the bank's strategic program.

67. Banks uses ICAAP results to detect whether the bank's existing capital is enough to withstand the bank's risks. If the existing amount of capital is not enough, then the bank

decreases the level of its risk or increases the amount of its capital/reserves to meet both capital adequacy requirement and the additional requirement of capital under ICAAP results.

68. Bank ensures a capital adequacy level above the regulatory minimum requirement, based on the following circumstances:

1) during the normal activity of the bank, the amounts and types of operations, provided by the bank, are changing, which generates new risks or increases the existing ones, bringing to the necessity of capital replenishment,

2) if the bank has to replenish capital in a short-time period or in adverse market conditions, then the capital replenishment can be costly for the bank,

3) some risks (macroeconomic or inherent to the bank's activity) occur during the bank's activity, which are not included in the regulatory requirement of capital adequacy,

4) violation of the regulatory requirement of capital adequacy by the bank can bring to implementation of sanctions by the supervisor,

5) if the bank intends to get a high rating from international rating agencies, it should have capital above the minimum requirement of capital adequacy.

69. Ensuring capital above the minimum capital level, defined by normative legal acts of the Central Bank, should not be considered as the only technique to withstand the bank's increasing risks. The problems of non-adequate internal control system or ineffective risk management processes should not be solved by establishing excessive capital.

Chapter 6. Stress testing
(Chapter was edited by Resolution No. 148-N dated 11.10.19)

70. Stress testing system forms a part of the bank's risk management process. The banks conducts stress-testing as a primary method of risk assessment or, at least, as a parallel method in addition to statistical, econometrical and predictive models of risk assessment.

71. The results of stress tests have practical usage. In particular, stress tests are used when defining the bank's risk appetite (the limits on separate risks and their components); and if no quantitative limits are defined, the results of stress-tests are used to make concrete decisions on necessity to accept the risk or mitigate it (its impact). The results of stress tests are also used during developing long-term business programs, developing recovery programs, as well as during capital and liquidity planning.

72. The Board of the bank is responsible for ensuring necessary conditions for implementing an effective process of stress testing, and the executive body is responsible for consistent implementation of stress tests; in particular, the Board and executive body of the bank ensure, that stress-tests are regularly revised and the applied assumptions and conditions are adequate.

73. The bank conducts:

1) one-factor stress-tests - sensitivity analysis, the purpose of which is to assess the impact of the changes of a separate or limited risk factors on the bank or a separate portfolio, without taking into consideration other factors,

2) scenario stress-tests, the purpose of which is to assess the impact of the changes of a number of risk factors on the bank or a separate portfolio, in case of which the results of interaction of different risk factors (including systemic) are taken into account,

3) reverse stress-tests, the purpose of which is to assess and disclose the scenarios or risk factors, in case of which the potential loss, used as an input factor, will happen. Meanwhile, the input factor is being defined by the bank respective to its portfolio, scale, complexity and riskiness of its activity.

73.1. Stress tests include:

1) bank-specific stress indicators,

2) financial market stress indicators,

3) consolidated – macroeconomic stress indicators.

73.2. Bank performs stress testing for all material risks, which at least include the following risks:

1) credit risk,

2) liquidity risk,

3) operational risk (due to the influence of both internal and external factors),

4) market risk by separate components, in particular:

a. FX risk,

b. interest rate risk in banking book,

c. market risk in trading book,

d. price risk, if the sum of assets, containing price risk, exceeds 3 percent of total balance sheet assets of the bank,

5) contagion risk (potential negative impact of financial problems of other bank/financial organization on the bank's capital and/or earnings),

6) country risk.

74. The scenarios ensure a complex assessment of the risk and comply with the complexity and riskiness of the bank, in particular:

1) scenarios are forward-looking, extreme but probable,

2) scenarios are developed taking into considerations both hypothetic and historically considered stress situations (taking into consideration also the last stress happened in the market). The use of hypothetic scenarios is necessary, in particular, in cases, when no any stress situation has been considered on any specific risk (portfolio, product, including a newly implemented one), or the material shocks on risk factors, impacting the bank, have been considered in different periods, but their simultaneous happening is also probable,

3) scenarios are developed sufficiently detailed, by risk factors, as well as by portfolios, currencies, products, adequate to the bank's complexity and riskiness.

75. The time horizon and scenario of conducted stress-tests should comply with the time horizon and results of the ICAAP. Meanwhile, stress-tests are conducted at least for the upcoming 12-month time horizon.

76. Stress testing is being performed, based on the main scenario, based on the bank's assumptions, which is subject to market shocks, reflecting at least two levels (moderate and severe) of extreme but probable conditions.

77. If the situation under the stress testing for one type of the risk can also have an impact on other risks of the bank, then the bank should assess the impact on each type of risk separately, as well as their total impact.

78. Stress testing for credit risk, operational risk, interest rate risk in banking book, price, contagion and country risks is being performed at least on a quarterly basis, and stress testing for liquidity, FX risks and market risk in trading book is being performed at least on a monthly basis. Stress testing for interest rate risk in banking book, including the assessment of conduct factors/parameters (assessment update) may be performed on a annual basis, if it is justified, that from perspective of the risk assessment no material changes have taken place in the bank's balance structure.

79. The bank regularly (at least annually) reviews its stress-tests, in particular it performs:

1) an assessment of efficiency and applicability of the stress-testing process,

2) a review of stress-scenarios, including the list of risk factors, considered in the scenarios,

3) assessment of the models, assessing the impact of the stress on the bank's financial indicators, the actuality of the assumptions, laid under the models, compliance of qualitative and quantitative justifications; and their review (if necessary):

80. The banks ensure internal regulation of the process of stress-testing, in particular:

1) The bank's internal legal acts at least define:

a. the types (sensitivity, scenario or reverse) and purpose of performed stress-tests,

b. the principles of selecting stress tests scenarios, including also the justification for the scenario of being extreme but probable,

c. the methodology of the models (including, financial instruments pricing, assessment of conduct factors), used in order to assess the impact of risk factors on the financial indicators,

d. the process and principles of model validation,

e. the methodology of selection of the time horizon,

f. the procedure of reviewing the stress-testing process,

g. the main responsible parties of the process,

h. the ways of usage of the results of stress tests in the managerial decision making and risk management processes,

i. the procedures of making the results of stress tests available to the decision-makers, interested divisions and providing them to the Central Bank.

2) The main assumptions under the stress tests, the main scenarios, the main judgments, used for assessment of stress tests results should be documented and circulated among the people, responsible for the process.

81. The bank takes measures to prevent potential stress situations in its internal environment or to mitigate the potential negative impact, arising due to them.

Chapter 6.1. Recovery plan
(Chapter was added by Resolution No. 148-N dated 11.10.19)

81.1. The bank should have a recovery plan (hereinafter referred to as recovery plan), aimed at the improvement of its financial situation in case of material worsening of the financial situation. The recovery plan should be consistent with the peculiarities of the bank's activity, nature of the risks, size and complexity.

81.2. The recovery plan should at last include:

1) the description of probable scenarios, in case of occurrence of which the bank's financial condition would materially deteriorate,

2) the impact of the probable scenarios on the main directions, sectors of the bank's activity,

3) the benchmark limits/indicators, in case of violation of which the bank would apply the measures, defined by the recovery plan,

4) the description of measures aimed at recovery of the bank's financial situation in case of occurrence of the probable scenarios.

81.3. The scenarios, described in the recovery plan:

1) the scenarios, included in the recovery plan, should be forward-looking, extreme but probable, and reflect at least two levels (moderate and severe) of probable scenarios,

2) the recovery plan should at least include:

a. two scenarios, which, if occur, will have a negative impact on a particular given bank,

b. two scenarios, which, if occur, will have a negative impact on the whole financial system and/or economy, which in turn will have a negative impact on the bank,

c. two scenarios, which will combine the occurrence of the abovementioned two scenarios,

3) the described scenarios should reflect the events, which may have an impact on the bank, taking into consideration the bank's risk structure, nature of activity, size, level of affiliation with the other participants of the banking system, etc.

81.4. The recovery plan should present the description of main directions, sectors of the bank's activity, as well as their impact on the latter in case of occurrence of the scenarios, described in the recovery plan.

81.5. Definition of benchmark limits/indicators:

1) the recovery plan should clearly define the benchmark limits/indicators, in case of violation of which the bank would use the measures, specified by the recovery plan,

2) the benchmark limits/indicators should be both quantitative and qualitative, which will reflect the bank's financial situation, and it will be possible to monitor them,

3) the benchmark limits/indicators should at least apply to the bank's:

a. capital,

b. liquidity,

c. profitability,

d. assets quality,

4) the recovery plan should also include benchmark limits/indicators, reflecting the situation on the financial market, as well as macroeconomic benchmark limits/indicators.

81.6. The measures, aimed at recovery of the financial situation:

1) the recovery plan should include the description of the measures that the bank will take in case of occurrence of the scenarios, described in the recovery plan, and (or) violation of the benchmark limits, as well as the sequence of their implementation, the reasonable terms, required for their implementation, the scope of units/employees, responsible for implementation of the measures aimed at recovery, as well as the description of the procedure of performance of effective communication among the latter,

2) the possible risks, arising from the implementation of each measure, specified by the recovery plan, should be disclosed in the recovery plan,

3) the recovery plan is being approved by the Board of the bank,

4) the recovery plan should be reviewed at least annually or more frequently in cases, when, e.g. the bank's organizational structure, operations, the level of the taken risk, strategy are being changed, there is a change in the financial situation, if the latter may have a material impact on the measures, specified by the recovery plan,

5) the banks should regularly explore (review) the external and internal factors, which may impact on the bank's activity, and should comply their recovery plans with the respective changes,

6) the bank should submit its recovery plan to the Central Bank on an annual basis before March 15 of each year, as well as within 10 working days after making any change,

7) the measures, specified by the recovery plan, should be tested at least on an annual basis in order to find out the effectiveness and should be updated, if necessary. The results of the testing should be documented by the bank and submitted to the Central Bank of the Republic of Armenia before October 15 of each year.

PART 5. OTHER ELEMENTS OF INTERNAL CONTROL SYSTEM

Chapter 7. Cash desk operations, investment activity, loans management

82. Bank's internal control system, concerning cash desk operations, at least includes:

1) maximum limits of cash under disposal of cashiers,

2) periodicity of cash funds inventory,

3) internal procedures, control mechanisms of implementation of cash operations,

4) mechanisms of ensuring the security of maintenance and transportation of cash funds.

83. Bank's internal control system, concerning its investment activity, at least includes:

1) investment policy,

2) targeted (benchmark) structure, profitability and maturity of investment portfolio (separate groups of investment instruments),

3) internal procedures, necessary minimum information for investment decision making,

4) structure, duties and authorities of the investment committee or other responsible division, and in the absence of such division, duties and authorities of the person, responsible for investments,

5) investment limitations (for example, by borrowers or by ratings of financial instruments),

6) limits of permissible concentrations (for example, by investment instruments, by counterparties/securities issuers/borrowers, by sectors of economy, by related parties, etc.),

7) principles of investments diversification,

8) principles of opening and closing of bank's corresponding accounts, periodicity of monitoring and comparison of accounts balances in other banks,

9) acceptable types of collateral for loans,

10) requirement of assessment of credibility of bought securities' issuers and borrowers; procedure, terms and periodicity of implementation of such assessment, responsible persons and their duties,

11) types and permissible maximum size/limits of a transaction (transactions) that can be performed by a dealer (employee who has authority to perform investment transactions) without verification of the appropriate manager,

12) principles and procedures of investments classification and provisioning against not-performing assets; scope and duties of people, responsible for its measurement and regular monitoring, as well as procedures of recovering the bank's overdue assets,

13) positions (parties) responsible for implementing monitoring and comparison of accounts balances in other banks, frequency of implementation,

14) procedures to ensure the compliance of the bank's investment activity to the structure and nature of the bank's liabilities, as well as to manage the risks, occurred as a result of existing non-compliances,

15) policy of implementing operations with derivatives, internal procedures of the implementation, including:

a. existence of an effective system of identification, measurement and management of risks, occurring from operations with derivative instruments,

b. methods of measurement of prices of derivative instruments, in case of performing operations with derivatives in over-the-counter market.

84. Reports, submitted to the bank's Board and executive body, concerning the bank's investment activity, at least include:

1) structure of investments,

2) schedule of repayments,

3) profitability of investments,

4) analysis of quality of investments,

5) problematic investments and implemented actions for their recovery,

6) pledged securities expressed in value, as well as percentage of investment portfolio,

7) implemented derivative operations.

85. Bank's internal control system, concerning its lending activity (credits, loans, overdrafts, credit lines, credit cards, guarantees, factoring and financial renting (leasing) activities, hereinafter loans), at least includes:

1) bank's target markets, acceptable types of lending (in case of providing leasing operations, also the types of property, which leasing the bank is intending to provide),

2) targeted (benchmark) structure, profitability and maturity of loan portfolio,

3) the members of credit committee, authorities and duties of credit committee, procedures of activity and decision-making,

4) limits of credit concentrations, including, by those countries, with whom or with residents of which the bank is implementing operations,

5) principles of loan portfolio diversification,

6) principles of granting, monitoring and recovering (including judicial and extrajudicial) loans,

7) principles of pricing (formation of lending interest rates, factoring discount rates) in the bank: meanwhile, in case of an unhedged borrower, during the pricing the bank should take into account also the credit risk, arising from the change of exchange rates.

8) acceptable types of pledge (collateral, guarantee),

9) "loan to value" ratios for different types of loan instruments (types of loans), expressed as a percentage,

10) types of control over the collateral (particularly in case of mortgage lending) and other requirements (for example, insurance of the pledged building),

11) cases or basis of possible exceptions from the approved policies and/or limits,

12) lending limits by loan value, maturity, those countries with whom or with the residents of which the bank is implementing operations; interest rates and types,

13) minimum documents and information, required for loan granting and maintaining in loan books,

14) principles of lending to related parties,

15) procedure of maintaining the information about applications, rejected by the bank, as well as studying the proof for rejections,

16) procedure of classification of loans and receivables and formation of provisions for possible losses, basis and cases of granting loans without security,

17) procedure and limits of providing loans to affiliated parties.

(Point 85 was edited by Resolution No. 38-N dated 30.03.18)

86. Internal control system of assessment and control of the collateral at least includes:

1) principles of selection and control of work of employees, implementing valuation of collateral,

2) principles of selection of persons, performing independent valuation,

3) procedure and frequency of implementing collateral revaluation,

4) procedure and frequency of control of collateral and its insurance, especially for collaterals which are physically out of the bank's control (under use of pledger),

5) requirement that the persons, assessing the collateral, are not interested in granting the loan.

87. In case of pledge of golden items (if the golden items are maintained by pledgee), the internal control system of valuation and maintenance of pledged items includes:

1) requirement, that the maintenance of the pledged items in the bank's storage should be implemented in closed transparent pockets, which should be stamped (with signature or other means of identification) by the bank's employee and the pledger,

2) requirement that will ensure that the opening of the transparent pocket should be done only with presence of the pledger and the bank's employee, whose has stamped the pocket. In case, if the pledgers presence during the opening of the pocket is impossible, with the presence of the pledger's agreement, the pocket is being opened with a special procedure (to protect the pledger's interests) without the pledge's presence,

3) requirement that description of each collateral should be maintained in the bank, signed by the bank's employee and the pledger,

4) requirement of signing the receipt, verifying the date and time of opening the transparent pocket, by the customer.

88. Deviations from internal legal acts, regulating the bank's lending activity, are properly justified, documented and stored in the loan book.

89. Loan books at least include the following documents:

1) loan application,
2) decision of credit committee or other competent body or person,
3) loan contract,
4) borrowers rating (if available),
5) documents, proofing borrower's legal capacity or capability,
6) documents, proofing requests, received from the credit registry or bureaus (if available),
7) contract of collateral or other type of pledge (in existence of a pledge),
8) other documents about collateral or other types of pledge (if applicable),
9) borrower's business plan or other information, proofing the repayment of the loan,
10) borrower's financial statements (if applicable),
11) analysis of the borrower's financial statements (if applicable),
12) correspondence with the borrower (if applicable),
13) records about phone conversations and meetings with the borrower, verified by the responsible person (If applicable),
14) loan monitoring report/ all other documents, concerning the monitoring (if available)

90. Documents, available in the loan book, should at least include the following information (either in electronic or in paper form):

1) borrower's name, surname and occupation (in case of legal person, name and type of activity), pledgers, guarantors, persons providing other types of security (if available),

2) date of granting the loan and the repayment date,

3) amount of the loan (initial amount and current balance),

4) purpose of the loan – consumer or commercial, and for large loans – documents, proofing the purpose of the loan,

5) interest rate of the loan and repayment schedule,

6) type and assessed value of collateral (in case of availability of collateral),

7) loan status – current or overdue (how long),

8) loan restructurings or prolonging, description of reasons of loan contract revisions,

9) results of internal and external examinations, related to the loan,

10) classification of the loan, reasons of classification (in case of classification),

11) information about the steps undertaken to recover the non-performing loans,

12) information about any other borrowing received by the borrower or other related parties from the bank.

91. Loan monitoring process at least includes:

1) examination of objectivity of use of the loan before each tranche distribution (except for the first one) (in case of large amounts), except for loan limits of credit lines,

2) recording of payments and loan repayments,

3) regular revaluation of collateral,

4) regularly receiving and analyzing financial and operational information about the borrower, in case of an unhedged borrower – also assessment of the risk, arising from the changes of interest rate, and, if necessary, its discussion with the borrower,

5) keeping in touch with the borrower through phone conversations,

6) if necessary, conversation with the borrower's suppliers, other counterparts and customers,

7) recording of all information, related to the loan,

8) if necessary, undertaking measures to support the borrower (to ensure the recovery of the loan),

9) special attention to those credit lines, which:

a. exceed the limits defined by the bank's internal legal acts (exceptions),

b. have no moves,

c. are repaid through funds, received by a new tranche of the loan.

(Point 91 was edited by Resolution No. 38-N dated 30.03.18)

92. Reports, submitted to the bank's Board and executive body with the periodicity, approved by the Board of the bank, concerning lending activity of the bank, at least include:

1) structure of loan portfolio,
2) quality of loan portfolio,
3) main directions of loans,
4) credit concentrations,
5) large exposures,
6) loans, provided to related parties,
7) problematic (overdue) loans, information proofing classification of such loans, measures undertaken to recover (repay) the overdue loans.

Chapter 8. Management of bank's fixed assets

93. Bank's internal control system, concerning the management of fixed assets, at least includes:

1) rules of buying, selling and writing off fixed assets,
2) criteria to define the reasonability of buying/selling fixed assets,
3) principles, terms and procedures of buying or using fixed assets, which have become the property of the bank as a result of confiscation or on other basis,
4) internal procedures of maintenance and accounting of fixed assets,
5) frequency and internal procedures of inventory,
6) principles and forms of disposal of written-off fixed assets,
7) periodicity, procedure of revaluation of fixed assets, principles of defining the necessity of revaluation.

Chapter 9. Management of bank's deposits and liquidity

94. Bank's internal control system, concerning the management of bank's existing deposits (deposit base) and banking accounts, at least includes:

1) targeted (benchmark) structure (share of demand and term deposits, taking into consideration seasonality and other possible factors) of deposit base,
2) principles of attracting deposit,

3) principles, procedure and processes of opening, operating, oversight and closing accounts for the bank's clients (separately for the related parties). Moreover, closing procedures should at least include:

a. information about the reasons of closing,
b. in case of payment cards accounts – the procedures of return of the payment card as a result of closing of the account,
c. in case of payment cards accounts – the procedures of suspension or termination of the transactions with the given account, including the online and offline transactions.

4) principles for defining interest rates, calculated on accounts balances.

(Point 94 was edited by Resolution No. 256-N dated 08.12.15)

95. Bank's internal control system, concerning liquidity (assets and liabilities) management, at least includes:

1) sources to meet the bank's liquidity requirements and channels of its use,

2) mechanisms of pricing of bank's assets (determining the interest rate) (taking into consideration the bank's cost of funds, overhead expenses, credit risk and payable dividends),

3) desirable or targeted structure and maturity limits of the bank's liabilities (for example, the bank can define, that the deposit certificates, issued by the bank should not exceed a certain percentage of the bank's total liabilities, and the maturity of those deposit certificates should not be less than a certain period),

4) limits of amounts of loans (gross and by types), given to the bank, as well as limits on gross interest expenses,

5) limits of concentrations of funding sources, used to meet the bank's liquidity requirements (for example, the bank is becoming dependent on actions of one person (natural or legal person), whose deposits form a big portion of the bank's liabilities),

6) requirement to diversify loans by repayment periods,

7) limitations of attracting borrowings from related parties (organizations) to improve liquidity requirements of the bank,

8) criteria for selecting alternative sources of liquid funds, in case when the primary sources are wiped out, the ways of finding such sources,

9) principles and methods of limiting interest rate risk, including the interest rate risk related to off-balance sheet items,

10) targeted level of interest margin,

11) limits of off-balance sheet items, sensitive to interest rate changes,

12) list of members of assets and liabilities management committee (if available), procedure of their appointment, their duties and authorities, as well as the division, responsible for assets and liabilities management, its duties and authorities,

13) mechanisms and procedures of decision making about the interest rates of attracting and distributing of funds,

14) permissible limits of maturity gap of the bank's assets and liabilities,

15) permissible maximum size/limits of a transaction (transactions) that can be performed by the employees, who have authority to perform transactions of attracting funds on behalf of the bank, without verification of the appropriate manager,

16) ways of coordination of work of those divisions of the bank, which can affect the level of the bank's liquidity by their actions,

17) program to meet additional requirements of liquidity (which can arise from decrease of income, increase of non-performing assets, concentration of deposits),

18) approaches of diversification of attracted and distributed funds, by individual currencies,

19) requirement to perform current analysis of sensitivity of collateral prices, in order to decrease liquidity risk,

20) requirement to regularly perform liquidity risk stress-tests: short-term and permanent, specific to the bank and broad market stress scenarios. Frequency of stress testing should be consistent with the structure of the bank's assets and exposure to liquidity risk,

21) requirement for availability and regular revision of an action plan in liquidity crisis (unexpected) situations, including requirement for availability of funding program in emergency situations.

96. Reports, submitted to the bank's Board and executive body at least once in two months, include the following information:

1) liquidity requirement of the bank, formulated during the reporting period,
2) current liquidity,
3) expected/forecasted requirement of funds,
4) sources of attracting funds,
5) current and expected quality of assets,
6) current and expected cash flows,
7) current and expected level of capital,
8) "price" of attracting and distributing funds (for example, interest rates of deposits, possible losses from assets' sale, etc.),

9) quality of assets and liabilities management of the bank,

10) information about the profitability of the bank's assets,

11) interest margin, analysis of the reasons of changes/fluctuations of interest margin,

12) concentrations of instruments, sensitive to interest rate,

13) structure of the deposit base by the reporting period and the trends of its change,

14) trends of changes of structure of assets, liabilities and off-balance sheet,

15) market forecasts,

16) purpose of loans, provided by the bank, sources of their funding, amounts, maturity, receivable and received interest payments.

Chapter 10. Business continuity management

97. Bank identifies, assesses, manages and decreases risks, which endanger the bank's business continuity.

98. The goal of business continuity management is to decrease or prevent the possible negative impact of emergency situation on the bank's operations, reputation, profitability, depositors and other debtors, financial system and/or other interested parties.

99. Those operations, that are not performed directly by the bank and are outsourced to other parties, are also included in the business continuity management system.

100. Business continuity management (hereinafter BCM) is a complex and complete process, which includes all those measures and actions, that are aimed at ensuring and/or recovering the continuity of key business processes in emergency situations during a predefined periods and amounts.

101. By means of this chapter, ***emergency situation*** is the situation, whose occurrence is possible but hardly forecasted (having low probability), and which imposes or can impose significant material losses or other negative impact on the bank, its depositors or other debtors. Emergency situations include both external disasters (for example, natural disasters, technical accidents, war (military actions), ruffian attacks, mass activity, epidemic, sabotage, protest strikes) and internal disasters, which occur as a result of intentional (malware) or unintentional (negligent, rash) actions or inactivity of the bank's employees, including the results of making non-professional or wrong decisions during formation and operation of security systems.

102. By means of this chapter, key processes are those operations, processes, resources and infrastructures of the bank, whose failure, interruption or absence (hereinafter, failure) will have a significant negative impact on the bank's operations, reputation, profitability, depositors and other debtors; and/or which were recognized as such by the Board of the Central Bank.

103. Bank's business continuity management system at least includes:

1) bank's business continuity management policy, approved by the Board of the bank,

2) analysis of the bank's business processes, including assessment of risks,

3) goals and strategy of recovery of business processes,

4) action plan, ensuring business continuity, including the plan of managing and recovering emergency situations,

5) program of organizing seminars for the bank's employees and raising the level of awareness,

6) plan of regular testing and updating the action plan ensuring business continuity.

104. Bank's business continuity management system is being adapted to the nature, size and complexity of the bank's activity.

105. Bank's business continuity management policy is the main document, which describes the principles and directions of implementation of BCM system. The policy should at least contain:

1) goals and objectives of the BCM and the bank's approach of implementation of BCM system,

2) list of persons, teams and/or committees, responsible for implementation of BCM, their clear rights, duties and authorities.

106. The purpose of analysis of bank's business processes is to disclose all those business processes, that have high importance, assess the impact of their failure on the bank and to decide the priorities of recovery.

107. During the analysis of business processes, the following are taken into consideration:

1) probable emergency situations (scenarios),

2) possible negative impact of failure of business processes on the bank's depositors or other debtors, as well as the assessment of the impact from financial, legal or reputational point of view,

3) maximum permissible time of failure of business processes.

108. During assessment of risks, those possible factors (reasons) are being disclosed, which can bring to a failure of a key business processes. For those risks, the probability of emerging and the possible impact in case of emerging are being taken into consideration.

109. The goals of recovery are the predefined levels (volumes) of implementation of the bank's key business processes, according to which those business processes should be recovered after occurring of an emergency situation, within predefined recovery terms.

110. Bank defines and documents the goals of recovery of business processes and the strategy to achieve that, based on the results of analysis of the bank's business processes, the nature, size and complexity of the bank's activity.

111. Bank ensures compliance of the action plan, ensuring business continuity, with the bank's business continuity management policy.

112. All those actions and required information, which will allow the bank to effectively manage the emergency situation in initial phase, as well as recover key business processes afterwards, are being mentioned in the action plan, ensuring business continuity.

113. The action plan, ensuring business continuity, at least includes:

1) list of key business processes,
2) recovery level and terms of each key business process,
3) strategy, required actions and their coherence for recovery of each key business process,
4) description of resources and infrastructures, required for the actions, ensuring business continuity,
5) rights, duties and authorities of the bank's employees and teams during emergency situation and after it,
6) communication plans.

114. Bank's action plan, ensuring business continuity, is being tested at least once a year or more frequently, in cases of significant changes, connected with the list, structure or nature of business processes. The results of testing of the action plan, ensuring business continuity, are being documented and submitted to the Board of the bank.

115. Singularities, connected with ensuring and managing the bank's IT systems continuity, are defined by another normative legal act of the Central Bank.

Chapter 11. Payment system, off-balance sheet operations, management of branches, information concerning related parties, AML/CFT

116. Objectives of implementation of internal control during provision of payment services by banks are: disclosure, analysis and management of risks, inherent to payment services, as well as implementation of actions in order to increase effectiveness of work.

117. Internal control system, concerning payment systems, at least includes:

1) provision of short description of activity when signing a contract with an operator or an agent,

2) description of possible failures in the system and measures, aimed to eliminate them.

118. Bank's internal control system, concerning payment instruments (payment order, direct debit, order of regular payments, direct debiting (hereinafter, order)), at least includes:

1) defining procedures for implementation of transactions, particularly, accepting, processing, making and rejecting of transactions,

2) defining procedures to apply for preventing possible risks during implementation of transactions,

3) defining procedures for submitting information about volumes of transactions, performed through bank accounts and by cash,

4) defining procedures for storing (archiving) documents,

5) defining procedures for submitting information about not clarified, rejected and delayed transactions, as well as procedures of measures, aimed at to disclose the not clarified transactions.

119. Bank's internal control system, concerning documentary letters of credit, documentary encashment, guarantees and other documentary transactions, at least includes:

1) procedures of performing the transactions,

2) description of each instrument,

3) mechanisms of risk management.

120. Bank's internal control system, concerning operations with checks, at least includes:

1) procedures of check issuing, servicing and making payments by the bank,

2) clients' identification data input and maintenance in the database, during the provision of the check-book,

3) defining procedures about servicing the checks (including, by types), written to other bank,

4) defining the conditions of rejecting the payments with checks,

5) defining procedures of detecting fake checks and undertaking appropriate measures.

121. Internal control system, concerning acquiring, keeping and servicing payment cards, at least includes the following requirements:

1) The procedures of acquiring, keeping the payments cards and their provision to the cardholder, including:
   a. The procedures of transportation from the territorial units of the bank and keeping within the bank of the payment cards, issued/acquired but not yet provided to the cardholder, and the envelops with the PIN-code,
   b. The security mechanisms of minimizing the possibility of access of the third parties, including the employees of the issuer, to the cardholder's data when providing the payment cards and the PIN-codes,
   c. The professional adequacy criteria for the employee, responsible for the process of implementation of the monitoring.
2) The procedures of servicing the payment cards, including:
   a. The procedures, ensuring the non-cash servicing of the payment cards (acquiring) by the bank for trading and/or service shops (hereinafter, servicers),
   b. In case of performing of withdrawal transactions by the bank - the procedures, ensuring the given function,
   c. In case of performing of cash-in transactions by the bank – the procedures, ensuring the given function.
3) The procedures of monitoring and controlling of the transactions, performed with payment cards, including:
   a. The procedures of monitoring of the servicers' behavior,
   b. The procedure of monitoring of the cardholders' behavior,
   c. The procedures of sending of an SMS to the cardholders about performance of each transaction (at least, outflows from the card account), performed with the payment card,
   d. The procedures of on-line responding to the cardholders' alarms in case of occurrence of incidents (loss, block, non-servicing of the card, capture of the card by the ATM, etc.),
   e. The procedures of ensuring the continuity and accessibility of round-the-clock servicing of the system of monitoring of the transactions, performed with the payment card of the bank,

f. The procedures of ensuring the continuity and accessibility of round-the-clock servicing of the bank's alarming system of fast reaction of the incidents occurred.

4) The procedures of control over the suspicious transactions as a result of the monitoring, including:

a. Effective self-working systems of separation of suspicious transactions from other ones and their identification,
b. The professional adequacy criteria for the specialists, responsible for identification of suspicious transactions,
c. The mechanisms of contacting the cardholder or the servicer in case of identification of suspicious transactions,
d. The procedures, describing the bank's actions in case of absence of possibility to contact the cardholder or the services in case of identification of suspicious transactions,
e. The procedures of initiating the funds chargeback process, based on the claim-applications, submitted by the cardholder,
f. The professional adequacy criteria for the employee, responsible for the funds chargeback process.

5) Appropriate criteria, ensuring the secure implementation of transactions within the virtual (internet) environment, and effective control mechanisms, including:

a. As the issuer – the procedures, related to existence of systems, ensuring the information security of the transactions, performed by the cardholders: by sharing encoded close keys (for example, 3 d secure), providing an SMS to the cardholder and/or generating and providing a one-time code by the bank,
b. As a provider of servicing – the procedures, related to existence of systems, ensuring the information security of the transactions, performed by the servicers: by sharing encoded close keys (for example, 3 d secure) and/or generating and providing a one-time code by the bank.

6) The procedures of performing the accreditation by the bank,

7) The procedures of identification of the cardholder by the bank,

8) In case of loss of the payment card, provided by the issuer to the cardholder - the procedures, aimed at management of potential risks, applied by the issuer prior to disclosure about the loss by the cardholder and informing the issuer about the loss:

a. In case of transactions, performed contactless, and not requiring identification of the cardholder (despite the fact of performing the transaction online or offline),
b. In case of transactions, performed with identification of the cardholder by the issuer (despite the fact of performing the transaction online or offline),
c. In case of transactions, performed offline, and occurrence of possible fines against the negative balance due to those transactions.

9) The procedures, aimed at management of the cardholder's risk due to performance of payments with fake cards, prepared as a result of grab, illegal reading of payment cards data; or illegal use of data:

a. In case of transactions, performed contactless, and not requiring identification of the cardholder (despite the fact of performing the transaction online or offline),
b. In case of transactions, performed with identification of the cardholder by the issuer (despite the fact of performing the transaction online or offline),
c. In case of transactions, performed offline, and occurrence of possible fines against the negative balance due to those transactions.

10) The procedures about ensuring physical and technical security of installed ATMs and other self-servicing equipment (selection of location, security measures, appropriate contracts, etc.), as well as procedures, aimed at disclosing and eliminating of reasons of fraud and failures, made through ATMs and other self-servicing equipment,

11) procedures to ensure normal operation of ATMs and other self-servicing equipment during working and non-working days, including:

a. mechanisms to manage and mitigate the risks (for example, violation of charging terms, connection failure, expiration of the paper, proofing the transaction, crash of the equipment, including the cameras, violation of consumers' interest because of crash, etc.), related to installation and servicing of ATMs and other self-servicing equipment,
b. criteria of charging the ATMs and other self-servicing equipment (taking into consideration the results of monitoring of previous transactions, days of salary payment, cash demand for upcoming non-working days and holidays and other factors),

c. procedures of eliminating the technical problems (“capturing” of banknotes, capturing of the payment card, etc.) during the work of ATMs and other self-servicing equipment,

d. procedures of returning (informing, the maximum period of return, etc.) the cards, captured by ATMs, to the cardholders,

e. cases and maximum terms of termination of work of ATMs and other self-servicing equipment,

f. procedures of implementing monitoring of current working conditions of self-servicing equipment.

(Point 121 was edited by Resolution No. 256-N dated 08.12.15)

122. **(Point 122 was repealed by Resolution No. 256-N dated 08.12.15)**

123. Bank’s internal control system, concerning servicing of bank and depot accounts, at least includes the following requirements:

1) definition of procedures of opening and servicing accounts in the bank and performing transactions with them,

2) definition of procedures of data identification of natural and legal persons while servicing the customers.

124. Bank’s internal control system, concerning off-balance sheet operations, at least includes:

1) conditions of providing applications for credit lines, overdrafts, credit cards, letters of credit and guarantees, the list of minimum required documents, procedure of their processing and examination,

2) conditions of renting of personal deposit boxes, as well as the requirement of sign a contract for the personal deposit box, which shall at least include the following provisions:

a. cases and procedure of using the same deposit box by affiliated persons,

b. list of those items (drugs, weapon, etc.), which are prohibited to keep in deposit boxes,

c. requirement to provide a separate room (other from the room of deposit boxes) to the customer after each time opening the deposit box with presence of the bank’s employee,

d. requirement of signing a receipt by the customer, proofing the date and time of entering the room of deposit boxes.

3) services, provided by the bank, concerning trust management.

125. Provisions/requirements of internal legal acts, regulating off-balance sheet operations which are exposed to credit risk, should be consistent with the requirements of internal acts, regulating credit operations.

126. Internal control system, concerning the bank's branch management, at least includes:

1) minimum/maximum number of branch employees and requirements to them,

2) assessment of professional competency of branch employees, trainings,

3) distribution of duties of submitting reports to the bank's head office,

4) principles of applying a unified system of accounting and internal reporting by the bank's all branches,

5) limit of cash funds in a branch, limits of lending by branch employees (by types of loans), permissible maximum size/limits of a transaction (transactions) that can be performed by the employee, who has authority to perform borrowing transactions, without verification of the appropriate manager,

6) measures, undertaken by the bank, in case of big flows of funds and performing large transactions.

127. Internal control system supposes existence of effective procedures of collecting, maintenance (archiving) and regular update of information about related parties, as well as effective procedures of performing transactions with related parties.

128. Procedures of performing transactions with related parties at least disclose and oversee possible cases and areas of conflict of interests.

129. Bank ensures getting and examination of reports (information) about major shareholders, affiliated parties of the bank, as well as parties affiliated with the affiliated parties, which are being regularly submitted to the Central Bank, according to Regulation 1 on "Registration and licensing of banks and branches of foreign banks, registration of banks' branches and representative offices, qualification and registration of managers of banks and branches of foreign banks", approved by Decision of the Board of the Central Bank of the Republic of Armenia No 145-N, on April 12, 2005.

130. Information about related parties with banks, at least include:

1) name and address of the party (for legal persons, name and location),

2) occupation (for legal persons, type of activity),

3) form of relationship,

4) all kinds of loans, borrowings, investments, collateral, contingent and other liabilities, deposits from the bank (if possible, also from other banks), borrowings given to the bank, etc.

131. Bank's internal control system, concerning anti-money laundering and combating financing of terrorism, at least include:

1) those mandatory procedures, that should be maintained by the bank while performing financial and/or other operations with customers, creditors and other parties,

2) necessary information, provided while performing financial or other operations,

3) riskiness criteria of the bank's customers (high risky customers), requirements, defined for customers involved in each group of risk,

4) collecting of minimum information about the real beneficiary and minimum procedures, necessary for identification of customers,

5) procedure of recording and maintaining information about customers, as well as collecting, registering and maintaining information about suspicious transactions.

132. Bank's internal monitoring body at least examines the compliance of the bank's financial operations, activities of bank's structural and territorial divisions and employees, with the requirements of the law of the Republic of Armenia on "Combating money laundering and financing of terrorism", other normative legal acts, adopted on the basis of the law, and the bank's internal legal acts.

133. Bank's internal legal acts at least include procedures and conditions of performing oversight over maintaining of procedures and requirements, specified by internal legal acts; sanctions, specified by legislation of the Republic of Armenia; procedure and conditions of applying those sanctions over the bank's managers, employees, structural division or the employee, responsible for combating money laundering and financing of terrorism, in case of violations of procedures and/or requirements.

PART 6. INFORMATION AND REPORTING SYSTEMS

Chapter 12. Information and reporting systems

134. Internal control system provides for existence of valid and effective information and reporting systems.

135. Bank's accounting and other recordings, used information should be valid, complete, timely and protected from unauthorized use.

136. Interbank information flows and system of circulation of documents are used in all levels of bank's management for performing different operations/procedures and implementing monitoring over them.

137. Bank’s internal legal acts define the forms of reports, submitted to the bank’s Board and executive body, procedure and frequency of submission, the division/person, responsible for submission. At least, reports about the areas, mentioned in parts 4 and 5 of this regulation, are being submitted to the bank’s Board and executive body, and should comply with the minimum requirements, defined by this regulation, and allow the bank’s Board and executive body:

1) to assess the current situation of the area, trend of changes, their impact on the bank’s activity and level of riskiness,

2) to react timely and adequately and, if necessary, to undertake appropriate measures to solve the problems, identified in the area,

3) to assess the quality of work done by the division/person, responsible for the specific area, as well as the effectiveness of their activity,

4) to increase the effectiveness of decision-making process of the bank’s Board and executive body by submitting the information, necessary for decision-making, to the bank’s Board and executive body.

138. Bank’s internal acts define the information (reports, references, etc.), necessary for decision-making, procedure and periodicity of providing the information.

139. Bank ensures the security and continuity of electronic systems of information storage and processing.

140. Bank clearly regulates the procedures of collecting information from appropriate divisions and bank’s branches, accounting, preparing reports and submitting them to the Central Bank.

141. Information, submitted to the bank’s Board and executive body with defined periodicity, concerning each branch of the bank, at least includes:

1) analysis of the branch’s activity, including the branch’s credit portfolio, structure of deposit base, concentrations and trends of their change,

2) economic analysis of the region, serviced by the branch,

3) claims represented by customers,

4) dynamics of change of number of customers.

142. Bank provides for such procedures that will allow the bank to ensure the validity of reports, submitted to the Central Bank. Such procedures at least include:

1) checking of existing data by a person, who has not performed those transactions, has not made the decision to perform them and has no way participated in the process of performing the transactions, before implementing the accounting of the bank’s transactions,

2) checking of reports by a person, who has not prepared them, has not performed the transactions, has not made the decision to perform them and has no way participated in the process of performing the transactions, before submitting the reports to the Central Bank,

3) recording of differences, identified as a result of checking, examination of their reasons and proposing and implementing measures to eliminate such cases in future.

143. Validity of information, reflected in reports, which form a part of internal reporting system, is being proved and, if possible, checked by the head of division, providing the report, and in case of absence of such division, by the employee, responsible for submitting the report.

144. Bank ensures existence of effective system of storage of the bank's more important documents (including loan, deposit contracts, etc.), which allows to ensure the protection of those documents from loss, unauthorized removal or usage. Bank's internal legal acts define also the form, terms and procedures of storage (archiving) of the bank's more important documents.

PART 7. OVERSIGHT FUNCTIONS

Chapter 13. General provisions

145. As an element of risk management and internal control system, bank should have at least the following oversight functions:

1) risk management function,
2) compliance function,
3) internal audit function.

146. Appointment of people, responsible for implementation of oversight functions (except for internal audit function), early termination of their authorities, approving the conditions of compensation, regular assessment of their activity, applying stimulation measures and disciplinary sanctions against them is implemented by the bank's executive body, with the consent of the Board.

147. Existence of oversight functions does not exempt the bank's Board and executive body from meeting their responsibilities.

148. The bank integrates its oversight functions and appropriate reporting system in its organizational structure in such a way, which gives opportunity to effectively implement the abovementioned functions.

149. Authorities and duties of a person/persons, responsible for implementation of each oversight function, are defined by the Board. The person, responsible for implementation of each oversight function, regularly reviews those documents and, if necessary, provides his/her suggestions to change them to the executive body or the Board.

150. Possible cases of conflict of interests should be brought to minimum for each oversight function. If, nevertheless, there is a case of conflict of interests, which can not be regulated by the bank's executive body, then the problem should be brought to the discussion and solution by the Board.

151. Bank ensures enough authority, independence and resources for each oversight function to effectively meet the responsibilities and reach the goals, defined for the function.

152. The person, responsible for implementation of each oversight function, must:

1) have opportunity to express independent and objective opinion about the problems under his responsibility, actual and possible violations,

2) have opportunity, if necessary, to implement oversight over the taken remedial measures and implementation of given suggestions,

3) have opportunity to talk to any employee with his/her own initiative and to get necessary documents and information for meeting his/her responsibilities,

4) have opportunity to directly talk and regularly meet (without the presence of the executive body) with the Chairman of the Board,

5) have opportunity to involve employees, having necessary qualification and knowledge, to properly implement the function,

6) have opportunity to effectively use appropriate information systems, as well as management information systems (MIS).

153. The person, responsible for implementation of each oversight function, regularly discusses with the bank's CEO the adequacy of the function's resources and, if necessary, asks for corrections. If the person, responsible for implementation of the function, does not come to agreement with the CEO about the necessary resources, then the problem is being brought to the discussion and solution by the Board.

154. The person, responsible for implementation of each oversight function, regularly assesses the effectiveness of the function; if necessary, initiates the necessary reforms and implements monitoring over them. The results of the mentioned assessment are being submitted to the Board, according to the procedure, defined by the Board.

155. Effectiveness of implementation of each oversight function is being regularly assessed by the Board, according to criteria, defined by the Board. To perform the

assessment, the Board of the bank defines the contest, format, frequency of reports, submitted to the Board by the persons, responsible for implementation of oversight functions. Reports, submitted to the Board by the persons, responsible for implementation of oversight functions, at least give opportunity to the Board to:

1) assess the current situation of the areas of responsibility of the persons, responsible for implementation of oversight functions, the trends of change, their impact on the bank's activity and level of riskiness,

2) timely and adequately respond and, if necessary, undertake appropriate measures to solve the problems, identified by the persons, responsible for implementation of the oversight functions,

3) assess the quality of work, done by the persons, responsible for implementation of oversight functions, effectiveness of their activity from the point of view of reaching the goals, defined for oversight functions,

4) increase the effectiveness of decision-making process of the Board, by submitting the information, necessary for decision-making, to the Board.

Chapter 14. Risk management function

156. Bank must have an effective risk management function, which should support the bank in procedure of timely identification, measurement, control, monitoring and communication of its risks.

157. The person/persons, responsible for implementation of risk management function:

1) support the bank's Board and executive body in meeting their responsibilities, by implementation of professional analysis, risk reviews and other means,

2) identify the risks, inherent to the bank's activity,

3) assess, monitor, help to effectively manage the identified risks. The latter includes the assessment of the bank's ability to absorb risks, taking into consideration the nature, probability of emerging, correlation and the level of possible negative impact of the risks,

4) give the general description of the bank's risk both by solo and group levels, if the bank is a member of a group,

5) regularly assess internal and external environment for early identification and assessment of potential risks,

6) monitor the risks, arising as a result of the bank's remuneration policy, regularly send signals to the Board about incentives, created as a result of the bank's remuneration policy, as well as the impact of the remuneration policy on the risk-taking behavior,

7) develop the risk management strategy, risk appetite, as well as policies of management of individual risks, subject to approval by the bank's Board,

8) according to the procedures, approved by the Board, participate in the bank's internal capital adequacy assessment process, regularly perform stress-tests, within their functions,

9) regularly submit reports to the Board, executive body, if necessary – also to the persons, implementing oversight functions, about the bank's risk profile and risk management processes,

10) document and submit to the Board the significant changes, which have affected or can affect the bank's risk management system, providing suggestions to keep and improve the effectiveness of risk management system.

158. At least on a quarterly basis, the person, responsible for implementation of risk management function, submits reports to the Board at least about the following:

1) assessment of bank's risks and measures undertaken to manage the risks,

2) assessment of changes of description of the bank's risks,

3) assessment of predefined limits of risks (if applicable),

4) problems, concerning risk management, related to large programs and investments (if applicable),

5) assessment of risky events and undertaking of necessary preventive/remedial measures.

159. The person, responsible for implementation of risk management function, properly and in timely manner informs the Board and the executive body about all those circumstances, which can have significant negative impact on the bank's risk management system.

Chapter 15. Compliance function

160. Bank ensures existence of effective compliance function, which should support the bank to deal in compliance with the requirements of legislation, as well as encourage and save the corporate culture of ensuring compliance.

161. The person/persons, responsible for implementation of compliance function, at least perform:

1) encouragement and support of formation of ethical corporate culture in the bank, which values responsible behavior and compliance of employee's activity with requirements of laws and other legal acts, including the bank's internal legal acts. This includes regular organization of seminars and discussions about rules of behavior, presenting the bank's corporate values, intended to encourage high professionalism and define the behavior, expected from the employees,

2) identification, assessment, management of risks, related to general legal and supervisory requirements and ensuring their compliance with the bank's activity; and ensuring appropriate circulation,

3) assessment of impact of possible changes of legal system on the bank's activity and its related risks,

4) ensuring existence of proper policy, processes and oversight mechanisms in the main areas of legal, supervisory and ethical responsibilities, and implementation of proper monitoring,

5) regular organization of seminars about main legal and supervisory liabilities for employees, bearing high responsibility as well as dealing with high risky activity,

6) identification of shortcomings and violations, concerning compliance of the bank's activity, and, if necessary, undertaking of preventive measures.

162. The person/persons, responsible for implementation of compliance function, submits reports to the Board at least on a quarterly basis, which at least include:

1) assessment of risks, related to the bank's compliance function, and the measures, undertaken for risk management,

2) assessment of compliance of activity of the bank's different units (divisions, business units, etc.) from point of view of following internal standards and goals,

3) any issue, related to compliance, concerning managers and other responsible positions in the bank; results of investigation, related to them, and steps undertaken,

4) significant violations and issues, related to compliance, concerning the bank's other employees of organizational units; results of investigation, related to them, and steps undertaken,

5) Fines or other sanctions, applied against the bank or any employee by the regulatory or supervisory body.

163. The person, responsible for implementation of compliance function, must have authority and duty to properly and directly inform the Chairman of the Board about the

cases of significant incompliance by the bank's managers, as well as the cases of significant incompliance in part of the bank's liabilities.

Chapter 16. Internal audit function

164. Bank must have an effective internal audit function, which at least assumes provision of independent and impartial assurance, aimed at increasing effectiveness of bank's management, internal control and risk management systems and processes and ensuring targeting.

165. Bank's internal control system, concerning internal audit activity, at least includes:

1) objective, role, authorities and responsibilities, principles of activity of internal audit,
2) minimum work that shall be done by internal audit,
3) scope of activities of internal audit, nature of assurance services, provided by internal audit,
4) procedure and terms of performing internal audit, preparing and submitting audit reports,
5) procedure of selecting and appointing the head and employees of internal audit,
6) procedure of long-term planning of internal audit work, terms of developing the annual working plan, the methodology of risk assessment while doing the planning.

166. Bank ensures that the head and members of internal audit division follow the following principles when performing their functions:

1) Principle of independence, for ensuring of which, along with other requirements, defined by legislation, the head and members of internal audit division:
    a. are free of intervention of third parties in matters of planning and performing auditing, summarizing and circulating the results,
    b. refrain from assessment of those functions, for performing of which they have been the responsible person during the year preceding the audit review,

c. exclude other cases of conflict of interests during performing their work (for example, conflict of interest can occur as a result of being a large borrower or providing consulting services about the area, subject to auditing).

2) Principle of integrity, for ensuring of which the head and members of internal audit division:

a. perform their activity, showing integrity, diligence and high responsibility to the work,

b. are not involved in illegal activity or do not become a participant of such actions, that can harm the reputation of auditing profession or the bank.

3) Principle of objectivity, which assumes, that while collecting, processing and circulating the information about the examined activity or process, the head or members of internal audit division use high professional objectivity (impartiality). The head and members of internal audit division perform balanced assessment of all material circumstances and are not pushed by their personal or other parties' interests while making judgments. To ensure the principle of objectivity, the head and members of internal audit division:

a. are not involved in any activity, action or relation, which can harm their impartial assessments, bringing to violation of the bank's interests and/or decrease of quality of the auditors' professional judgments,

b. disclose all significant facts, they are aware of, in case of non-disclosure of which, the reports, concerning the activity under auditing, will be false.

4) Principle of confidentiality, which assumes that the head and members of internal audit division ensure the confidentiality of information, got by them, and do not disclose it without appropriate authority due to legal or professional obligation for the disclosure. To ensure the principle of confidentiality, the head and members of internal audit division:

a. exercise caution in using and storing the information, received while performing their duties,

b. do not use information for their personal interests of any other way, which will contradict the laws or the bank's objectives and ethic norms (if there is no any legal requirement to provide confidential information).

5) Principle of competency, which assumes, that the head and members of internal audit division have appropriate knowledge, skills and experience, that are necessary for effectively performing the functions of internal audit. To ensure the principle of competency, the head and members of internal audit division:

a. are involved only in those areas, for which they have necessary knowledge, skills and experience,

b. continuously improve (upgrade) their abilities and effectiveness and quality of their work.

167. Planning of work of internal audit is done on the basis of risk assessment, results of which are being properly documented. The head of internal audit division is responsible for long-term planning of risk-based audit work, as well as for developing risk-based annual working program. The head of internal audit regularly assesses and, if necessary, revises the results of long-term planning of work, as well as the annual working program. Each revision (including grounds of revision) is being properly documented.

168. While setting the priorities of work, when planning the work of internal audit, at least the followings are taken into consideration:

1) bank's risk management system, including risk management strategy, risk appetite, risk management policies for specific risks,

2) results of assessment of riskiness of the bank's operations and processes,

3) importance of the bank's operations and processes from the point of view of reaching the bank's objectives; complexity, volumes, the level of professional competency of employees of the area,

4) results of similar audit examination in the past.

169. Each year the Board approves the annual working program of internal audit division, which at least includes:

1) the areas, subject to auditing,

2) description of auditing work in each area,

3) scope of the program (including the schedule of performing the audit).

170. Internal audit work at least include:

1) monitoring and assessment of adequacy and effectiveness of the bank's policy, processes, their documentation and implementation of control mechanisms, from the point of view of the bank, group (if the bank is a member of a group), bank's branches (if available), business unit, business area, as well as division or other organizational unit,

2) regular assessment of effectiveness of risk management and compliance functions,

3) assessment of processes of bank management and decision-making in different levels, assessment of credibility of information, used in decision-making process

4) assessment of undertaking of effective and timely steps for risk identification and management,

5) assessment of completeness and adequacy of working documents and records, as well as proper accounting of transactions,

6) assessment of proper representation of the bank's assets in financial statements, and, if necessary, assessment of physical existence and ways of maintenance of assets (for example, cash) and assessment of liabilities to be fully disclosed and reasoned,

7) assessment of proper assessment, accounting and security of collateral and other off-balance sheet items, including by on-site inspections,

8) assessment of compliance of activity of the bank and its managers with requirements of laws, normative and other legal acts, including the bank's procedures (regulations, procedures, orders, guidelines, etc.),

9) assessment of compliance of operations of the bank's employees and organizational units with the bank's internal policies and procedures (regulations, procedures, orders, guidelines),

10) assessment of justification of income accounting and expenses, from the point of view of their compliance with legislation and the bank's internal regulations (selective examinations of credit discounts, deposit payments, penalties for overdue repayments, fees for services and overdue loans, in order to assess their accuracy),

11) assessment of effectiveness of the bank's internal control system and its adequacy to the bank's risks,

12) assessment of performing each employee's functions within his/her authorities in internal control system,

13) assessment of internal information and reporting system,

14) examination of implementation of the bank's internal capital adequacy assessment process (ICAAP) and its effectiveness,

15) assessment of authorities (for example, granting loans, signing of letters of attorney, contracts, transfers and other types of legal or accounting documents), given to the bank's employees to exclude possible abuses,

16) examination of lending processes, process of loan classification, loan losses, writing off and reversion of loans,

17) assessment of effectiveness and adequacy of business continuity management system, implemented in the bank; assessment of compliance of plan of measures, ensuring business continuity, with the bank's business continuity management policy; assessment of effectiveness of testing and updating the plan of measures, ensuring business continuity,

18) assessment of effectiveness of functions, outsources by the bank.

171. Internal audit function ensures, that the bank's all significant risky areas and liabilities are audited in reasonable terms and frequency.

172. For each auditing, the internal auditors develop a program, which defines the objective, scope, duration, resource allocation of the audit, as well as other necessary details.

173. During planning of the audit, the internal auditors take into consideration:

1) the objectives of functions, subject to auditing, control mechanisms of performing those functions,

2) significant risks, connected with functions, objectives, resources, operations, subject to auditing, and those measures, which are being used to keep the possible impact of the risks within its permissible levels,

3) adequacy and effectiveness of management of functions, subject to auditing, risk management and internal control,

4) possibilities of significant improvement of management of functions, subject to auditing, risk management and control functions.

174. During planning of the audit, the internal auditors perform a preliminary assessment of risks, inherent to the functions under auditing, as well as assessment of probability of occurrence of significant errors, frauds, mismatches and other risky factors, related to the functions, subject to auditing. Objectives of the audit should be consistent with the results of assessment.

175. Scope of audit should be adequate for reaching the objectives of the audit.

176. Internal auditors should perform effective allocation of resources for reaching the defined objectives of the audit, taking into consideration the nature and complexity of the functions under auditing, maturity limitations and available resources.

177. Internal audit rejects the requirement of the executive body of the bank to perform audit or other actions, if it does not comply with the objectives of functions of internal audit, defined by the Board, or can hinder the effective implementation of annual plan of the audit.

178. During planning of the audit, the internal auditors also develop work implementation program, defining the procedures of disclosure, analysis, assessment and documentation of information. The working plan is being approved before beginning of the audit, and any change in it is being approved in reasonable term.

179. Internal auditors disclose, analyze, assess and document enough information for reaching the objectives of audit.

180. The employees of internal audit are given enough authorities to achieve their responsibilities. They should be authorized to receive all necessary documents (information), and enter the examined division and other areas, where documents (archives), cash, other values (bunker), computer processing of information are kept, with mandatory attraction of the head of the examined division or an employee, authorized by him.

181. Internal auditors summarize the results of each audit, performed in the bank, in a report, which at least should include:

1) description of performed audit work,

2) violations and shortcomings, disclosed as a result of the audit, and proposed measure for their elimination,

3) internal audit's conclusion about elimination of disclosed violations and shortcomings.

182. The report, mentioned in point 181 of this regulation, is being submitted to the head of examined unit. The latter provides a written opinion about the report, expressing his/her consent or disagreement, with appropriate grounds, which is being signed by the head of the examined unit and forms an inseparable part of the report.

183. Internal audit performs a follow-up control of implementation of at least those measures of the bank's unit, which were recommended as a result of internal and external audit and were approved by the Board, or were recommended as a result of examinations, performed by the Central Bank.

184. Based on the results of the follow-up control, within the defined terms, and in case of absence of such terms – at least quarterly, reports are being prepared and submitted to the Board by appropriate responsible persons about implementation of suggestions and/or recommendations, made as a result of internal and external audit, as well as examinations of the Central Bank. Reports, submitted to the Board, describe the significant risks, existing in the bank, control mechanisms, issues of corporate governance (if such exist).

185. The internal audit properly documents and stores all main documents, concerning the audit, performed by him, including results of monitoring and analysis, justifying internal audit's conclusions, methodology of the audit's selection, ground of choosing that methodology. Working documents of internal audit contain information about all stages and processes of internal audit, including planning and implementation of the audit work, summarizing of results, implementation of follow-up control.

PART 7. BUSINESS CONDUCT, PROTECTION OF CONSUMER RIGHTS

Chapter 17. Business conduct, protection of consumer rights

186. Ensuring proper processes in the bank, related to business conduct, aims to ensure sufficient level of protection of the bank's customers (consumers) rights.

187. Bank' internal control system, concerning business conduct and protection of consumer rights, at least includes:

1) concerning internal legal acts, describing the services, provided by the bank, and the policy of their provision:
   a. detailed description of the service, including:
      1. conditions (rules) of service provision, samples of contracts of services,
      2. prices of services provided (including fees and other payments, their list), conditions and procedure of changing them,
      3. list of documents (information), required from consumers for providing the service,
   b. procedures, describing the process of defining the prices (including fees and other payments) of provided services,
   c. policy of providing additional services along with the main services,
   d. all conditions, limiting availability of services, provided by the bank, to the customer,
   e. criteria and procedures of rejecting transactions (refusing to provide the service) by the bank,
   f. procedures of correcting the mistakes, made during the provision of service,
   g. procedures of interrupting provision of the bank's services by the bank's initiative for the concrete customer, as well as generally,
   h. procedures, performed by the bank in case of meeting the obligation, set by the contract, before the deadline by a customer (including also description of penalties or any other means deteriorating the customer's condition),
   i. procedures of providing services with conditions, other than the defined general conditions (signing contracts with more/less favorable conditions), including the criteria, based on which the bank's competent body will make similar decisions,

2) concerning internal legal acts, describing prevention and regulation of conflict of interests:

a. measures and procedures of regulation of prevention of conflict of interests on the bank, bank's managers and employees,

b. procedures aimed at disclosing and excluding cases of possible conflict of interests while servicing customers,

3) concerning internal legal acts, describing processes of examining claims:

a. procedures of accepting, discussing customers' claims, decision-making, answering, performing monitoring over that process,

b. process of examining customer's oral claims, procedures of performing monitoring over that process (function of acceptance and examination of customers' written or oral claim can not be implemented by the employee, who has been directly involved in providing the services to customers).

4) concerning internal legal acts, defining policy of information disclosure by the bank:

a. list of information, subject to disclosure, about the bank and services, provided by the bank

b. description of forms, means (media, internet, bulletin board, informational bulletin, etc.), procedures of information disclosure by the bank about itself,

c. description of forms, means (media, internet, bulletin board, informational bulletin, etc.), procedures of making the information about the services, provided by the bank, available to the customers,

d. procedures, describing the process of performing advertising by the bank, procedure of assessment of advertising and other disclosed materials from the point of view of protection of customer rights,

e. internal procedures, ensuring timely updating, reliability and consistency of information, disclosed in different forms and means (media, internet, informational bulletins, leaflets, brochures, booklets, etc.) about the bank and the services, provided by the bank,

5) concerning internal legal acts, defining policy of customer service by the bank:

a. principles, procedure and forms of communication between the bank and customer,

b. list of information (including the list of minimum information, concerning oral information), provided to the customer before signing the contract, during signing the contract and during the term of contract, forms and procedure of providing that information,

c. policy, defining appropriate skills, quality criteria and norms of conduct for the bank's staff, servicing customers, and employees, directly consulting customers.

188. Adoption of internal legal acts, describing the procedures, defined by sub-point 1 of point 187 of this regulation, is not mandatory, if the procedure, by its nature, is not applicable to the provided service.

189. Processes and procedures, developed by the bank, concerning business conduct and protection of consumer rights, ensure fair treatment to customers, which at least assumes:

1) monitoring of customers' needs and interests while developing and providing banking services,

2) providing clear, reliable and timely information, adequate to the customer's needs, before signing the contract with the customer and during the term of the contract,

3) avoidance from providing servicing, not matching the customer's needs,

4) ensuring high quality of consultation, provided to the customer,

5) fair and timely examination of customers' claims and/or requests,

6) protection of information about customers, containing bank secrecy,

7) justification of customers' reasonable expectations,

8) provision of services with conditions other than generally defined conditions (signing contracts with more/less favorable conditions) only in case of existence of appropriate criteria.

190. Fair treatment to customers must be defined as an objective by the bank's business program and it should be taken into consideration in decision-making procedures.

191. Bank must ensure following the developed processes and procedures, concerning business conduct and protection of consumer rights, as well as rules of high professionalism and behavior, by the bank's employees.

192. Bank ensures existence of appropriate mechanisms of assessment of the process of developing and providing services from the point of view of consumer rights protection; and procedures of informing the executive body and the Board about the assessments, received as a result of application of those mechanisms.