Ordinance No 10*
of the BNB
of 24 April 2019
on the Organisation, Governance and Internal Control of Banks

(Published in the Darjaven Vestnik, issue 40 of 17 May 2019)

Chapter One
SUBJECT

Article 1. (1) This Ordinance shall determine the requirements to organisation, governance and internal control of banks.

(2) The provisions of this Ordinance shall also apply to:

1. third-country bank branches;
2. companies included within the scope of supervision on a consolidated basis.

Chapter Two
ORGANISATION AND GOVERNANCE

Section I
General Requirements

Article 2. (1) The organisation, governance and internal rules of banks shall be consistent with the size, nature, scale and complexity of the activities performed by them and the risks to which they are exposed.

(2) For the purposes of paragraph 1, the banks shall take into account the criteria set out in item 19 of the Guidelines of Internal Governance (EBA/GL/2017/11) issued by the European Banking Authority (EBA).

Article 3. (1) Management and controlling bodies of the bank, in line with their competence, shall create a suitable and transparent organisational and operational structure, which shall ensure effective and prudent management of the bank.

(2) The structure of the bank shall be consistent with its risk strategy and risk appetite and shall not impede the ability of the management and controlling bodies to manage and oversee the risks it faces and the ability of the Bulgarian National Bank to effectively supervise its activity.

(3) Banks shall not set up unduly complex and non-transparent structures, that have no clear economic justification and may be used for illegal purposes.

* Unofficial translation provided for information purposes only. The Bulgarian National Bank bears no responsibility whatsoever as to the accuracy of the translation and is not bound by its contents.

Section II

Internal Rules

Article 4. (1) The management body of the bank shall adopt and implement rules on bank's organisation and governance, which shall include at least:

1. a detailed description of bank's management and organisational structure, including clear allocation of functions and responsibilities among structural units, relationships between them and a decision-making procedure;

2. an exhaustive definition of powers and responsibilities of administrators and key function holders in the bank, as well as a description of requirements for holding such positions in order to ensure knowledge, skills and professional experience necessary for the performance of their duties;

3. the bank's strategy and plan of activities that take into account its long-term financial interests and solvency;

4. the policy and structure of risk management and control, including determination of bank's risk appetite;

5. the procedure for preparing and the scope of management information;

6. appropriate and reliable accounting and financial reporting systems, including efficient organisation of financial and operational controls;

7. an effective internal control framework that includes independent risk management, legal compliance and internal audit functions;

8. the policy to establish, manage and prevent conflicts of interest;

9. the procedure for reporting by employees breaches committed within the bank;

10. the code of ethics of administrators and employees, that includes high ethical and professional standards consistent with bank's specific needs and characteristics;

11. the system for providing training, evaluation and incentives to senior management and employees with supervisory functions.

(2) The management body of the bank shall periodically review and assess the rules under paragraph 1 and in case of identified deficiencies, weaknesses and/or need of improvements it shall amend them. The conclusions of the assessment and the measures undertaken shall be included in the meeting minutes.

(3) Upon assuming office, the members of management and controlling bodies, and the employees to whom the rules under paragraph 1 apply shall acquaint themselves with these rules, which shall be certified in writing or in other appropriate manner. The requirement under the previous sentence shall apply to any subsequent amendment to the rules.

(4) The supervisory board of the bank, respectively the non-executive members of the board of directors shall oversee the implementation of policies, rules and procedures for the organisation and management of the bank in relation to:

1. bank's risk culture;

2. accounting and financial reporting;

3. the internal control framework;

4. the policy for identifying, managing and preventing conflicts of interest;

5. the annual internal audit unit plan;

6. the code of ethics;

7. other issues provided for in the bank's Statute and internal acts.

Article 5. (1) The management body of the bank shall develop a sound and consistent risk culture, taking into account the risks to which the bank is exposed, and its risk appetite.

(2) The risk culture shall include at least:

1. management and controlling bodies' core principles, values and expectations concerning risk-taking and risk management;

2. the responsibility of employees at all levels to be aware of and understand the main risks to which the bank is exposed, its risk appetite and risk capacity;

3. open and effective communication between the employees;

4. appropriate incentives in making decisions concerning risk-taking aligned with bank's risk profile and its long-term objectives.

(3) The supervisory board of the bank, respectively the non-executive members of the board of directors shall monitor that the risk culture is implemented consistently.

Section III

Conflict of interest

Article 6. (1) Each bank shall segregate duties and establish appropriate information barriers in all cases where a conflict of interest may occur, and shall prevent the combination of functions related to authorisation, performance and reporting of operations.

(2) The management body of the bank shall adopt and implement an effective policy to identify, manage and prevent actual and potential conflicts of interest between the interests of the bank and the private interests of employees, including members of the management and controlling bodies, which could adversely influence the performance of their duties and responsibilities. The policy shall include:

1. identification of cases or relationships where conflicts of interest may arise, such as financial interests (holding shares or interests in companies, which are customers of the bank), relationships with the owners of qualifying holdings in the bank, employees of the bank or entities included within the scope of prudential consolidation, consultancy, audit and other companies with which the bank has contractual relationships, and the cases of potential political influence;

2. the procedure for reporting any case that may result or has already resulted in conflict of interest, including the unit to which it should be reported and bank employees' specific duties to promptly disclose it;

3. procedures, measures, documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking actions to address them.

Section IV

Reporting Procedure

Article 7. (1) Each bank shall adopt and implement appropriate and effective written procedures for reporting by its employees of actual or potential breaches within the bank.

(2) The procedures shall ensure:

1. an independent and autonomous reporting channel accessible to all bank's employees;

2. protection of the personal data of both the person who reports the breach and the person who is allegedly responsible for the breach;

3. providing information on reports received from employees to the bank's management and/or controlling body and other persons entrusted with such functions;

4. that the reports are taken into account by the bank and, where necessary, are sent to the Bulgarian National Bank or other competent authorities or persons;

5. protection of persons reporting breaches from unfair treatment;

6. confidentiality of reported information unless disclosure is required by law in the cases of criminal or administrative proceedings;

7. record keeping of reports and tracking of the outcome of investigations into each report.

(3) The bank shall provide for a whistle blowing procedure under paragraph 2, item 3, where requested by the employee who has reported the breach.

Chapter Three

INTERNAL CONTROL FRAMEWORK

Section I

General Provisions

Article 8. (1) The internal control framework shall include:

1. the operational control organisation;

2. the risk management function;

3. compliance function;

4. the internal audit system.

(2) The internal control framework shall cover the entire internal organisation, as well as the responsibilities of bank's management and controlling bodies, the activities of all business lines and structural units, including the internal control functions and outsourcing.

(3) Each bank shall ensure a clear, transparent and documented decision-making process and a clear allocation of responsibilities and powers within its internal control framework.

(4) The internal control framework shall ensure:

1. effective and efficient operations;

2. prudent conduct of business;

3. adequate identification, measurement and mitigation of risks;

4. reliability of financial and non-financial information and reporting;

5. sound administrative and accounting procedures;

6. compliance with laws and regulations, supervisory requirements and bank's internal policies, processes, rules and decisions.

Section II

Reporting and Information

Article 9. Each bank shall maintain a reliable reporting and information system, which shall at least allow timely access to information according to officials' powers, and its movement:

1. upward, to inform the management of the operations, business risks and current bank status;

2. downward, to inform the staff of bank's objectives and tasks, as well as of the policy, rules and decisions approved by the management; and

3. horizontally across the organisation, to provide and exchange the relevant information between the structural and functional units of the bank.

Article 10. (1) All bank transactions and operations shall be registered in due time and comprehensively in a chronological order.

(2) Banks shall maintain electronic and/or paper files of all transactions by type of operation, customer and other criteria selected by them.

Article 11. Bank files shall contain:

1. an inventory of the documents in the file;

2. internal bank documents, minutes, agreements, contracts, *etc.*;

3. financial and other information about the customers and the market;

4. other documents and information essential for the bank.

Article 12. (1) To protect the information when using information and communication technologies (ICT), the management body shall ensure the segregation of:

1. duties associated with ICT development, implementation and modification, including ICT administration and maintenance;

2. rights of access to information.

(2) The management body of the bank shall put in place and implement appropriate control mechanisms for operational risk evaluation and management related to ICT reliability and security.

Article 13. (1) The management body shall adopt internal rules for using ICT which shall limit:

1. errors in software development and modification, database administration and use;

2. interruption of operation due to internal and/or external factors;

3. fraud and unauthorised access to information.

(2) Banks shall update their internal rules and procedures for using ICT in line with the technologies they apply and associated risks.

Section III

Risk Management Function

Article 14. (1) Each bank shall maintain an adequate risk management function which shall include:

1. identifying, assessing and measuring all risks to which the bank is exposed, as well as external and internal sources of risk;

2. risk measurement and monitoring and risk assessment models;

3. monitoring and periodical assessment for compliance with risk management internal rules taking into account market conditions and best banking practices;

4. policies and procedures for risk assessment, determination and compliance with risk limits, as well as for allowing exceptions in case of emergencies;

5. the scope, structure and frequency of risk reporting;

6. the risk culture.

(2) Requirements to the risk management function shall be governed by Ordinance No 7 of the BNB on Organisation and Risk Management of Banks (Darjaven Vestnik, issue 40 of 2014).

Section IV

Compliance

Article 15. (1) Each bank shall establish a compliance function to ensure an adequate identification, measurement and management of the compliance risk.

(2) The compliance function shall be independent of the business lines and internal units falling within the scope of the activities it oversees.

(3) The compliance function shall be headed by a reputable person, who holds a higher education degree in law or economics and has professional experience of at least five years in the banking or finance sector.

(4) The compliance function shall have an adequate stature and sufficient authority and resources to perform its duties, including access to any information that is necessary to carry out its activities.

(5) The compliance function shall:

1. identify and measure the compliance risk to which the bank is exposed or might be exposed;

2. regularly assess the changes in the laws and regulations applicable to the bank and their impact on its activities;

3. advise bank's management and controlling body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards and shall assess the impact of any changes in the legal and regulatory requirements on bank's activities;

4. verify that all new products and new procedures comply with the law and the applicable regulations;

5. report to the management and controlling bodies on the compliance risk;

6. cooperate and exchange information with the risk management function on risk compliance and its management.

(6) The management body of the bank shall adopt internal rules and an annual plan of the compliance function's activities.

Section V

Internal Audit. Internal Audit Unit

Sub-section I

General Requirements

Article 16. (1) Internal auditing is an independent and objective appraisal function to review bank transactions and operations, and control systems to provide assurance and consultations, intended to improve bank's operations.

(2) Internal audit helps the bank to achieve its objectives by applying a systematic and disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

(3) All activities, including outsourcing, each structural unit and each process in the bank shall be subject to internal audit.

(4) The internal audit of the bank shall be exercised by an internal audit unit, which shall assist the management bodies in taking decisions and conduct follow-up reviews on their execution.

Article 17. (1) In performing its function, the internal audit unit shall examine and evaluate:

1. the reporting and information system, usefulness of the analyses prepared, ICT and data quality;

2. compliance of operations with law, observance of internal rules and procedures, and whether objectives set by the management have been met;

3. compliance of internal control policies and procedures with statutory and regulatory requirements, as well as with decisions of management and controlling bodies;

4. the accuracy and effectiveness of applied internal policies and procedures;

5. the risk management systems, risk and capital adequacy assessment methodologies;

6. the adequacy, quality and effectiveness of the controls performed by the units responsible for operational controls exercised over business units conducting transactions and operations, the risk management function and the compliance function;

7. reliability and timely submission of reports to the Bulgarian National Bank;

8. whether the bank's assets are properly safeguarded from mismanagement and fraud;

9. adherence to contracts and commitments;

10. staff recruitment and training, as well as consistency of job descriptions with duties.

(2) In carrying out their activities, internal audit officers (internal auditors) shall be empowered to:

1. unlimited access to:

a) the bank's premises and assets;

b) the decisions of management bodies, committees and other officials and structures;

c) accountancy and ICT;

2. require and collect information, statements and other documents in relation to the assigned tasks;

3. recruit experts in carrying out specific control actions.

(3) Internal auditors may not be authorised or held liable for the activities and subjects of examination, and their position may not combine with other positions in the bank.

(4) Administrators and employees of the bank shall assist the internal auditors in performing their activity.

(5) Reviews and control actions initiated by administrators and other persons of the management staff within their powers may not substitute the internal audit functions.

Article 18. (1) Internal auditors shall have:

1. professional skills in applying international standards for the professional practice of internal auditing, procedures and techniques of auditing;

2. knowledge and experience in applying accounting standards;

3. knowledge of management principles and prudential banking.

(2) Internal auditors shall follow the prescribed principles and best practices of ethical conduct, they shall be honest, impartial, diligent, loyal and outgoing in their contacts with people.

Article 19. (1) A head of the internal audit unit shall be elected a person with high ethical and professional reputation, and appropriate qualification in auditing and accounting, and experience of at least five years in financial auditing.

(2) The head of the internal audit unit may not hold more than one office in the bank.

(3) The head of the internal audit unit shall ensure and oversee the application of international standards for the professional practice of internal auditing and the efficiency of internal audit activities.

Article 20. (1) The management body of the bank shall approve internal rules and an annual plan of the internal audit's activities.

(2) The annual plan under paragraph 1 shall be adopted on a motion by the head of the internal audit unit following the risk-based approach.

Article 21. (1) The internal rules shall regulate the powers of internal auditors, the procedure for taking control actions, their documentation and reporting results.

(2) Internal rules shall ensure:

1. independence and discretion to the head of the internal audit unit in planning and assigning examinations;

2. unlimited access to the assets and information;

3. direct contacts of the head of the internal audit unit with management bodies;

4. the right of the head of the internal audit unit to recruit internal auditors in compliance with the professional qualification required;

5. avoidance of any conflict of interests in executing the tasks by the internal auditors;

6. conditions for recruitment of experts in taking specific control actions.

Article 22. (1) The head of the internal audit unit shall estimate resources and approve programmes on execution of detailed control tasks with a view to implementing the annual plan.

(2) All processes, objects and internal audit systems shall be covered within an audit period of up to three years. The frequency of internal audits concerning individual processes, objects and control systems shall be determined according to their significance and potential risk for the bank.

Sub-section II

Documentation of Control Actions and Reporting Results

Article 23. Any examination or other control actions of internal auditors shall finish with preparing a report containing findings and recommendations for measures to be taken against violations of law and internal rules, and for removing malpractices in the bank's operations.

Article 24. (1) The head of the internal audit unit, in compliance with international standards for the professional practice of internal auditing, shall approve requirements for the reports and documents prepared and collected by internal auditors.

(2) Information collected in the process of auditing shall base the findings, evaluations and recommendations made.

Article 25. (1) The report under Article 23 shall be submitted to the head in charge of the examined unit, to the head of the structural unit involved in the audit processes and to the head of the internal audit unit.

(2) Within the terms set by the internal rules, the head of the examined unit shall submit explanations and/or lay claims concerning the findings and recommendations addressed.

(3) Internal auditors shall draw a conclusion on the written explanations or claims submitted by the head of the examined unit.

(4) Upon implementing procedures under the previous paragraphs, the head of the internal audit unit shall submit the report and the documents under paragraphs 2 and 3 to the executive directors.

(5) The management body and the administrators shall impose remedial measures and notify the head of the internal audit thereby.

Article 26. (1) In case of significant violations and malpractices or where insufficient remedial measures have been taken, as well as if violations and breaches on the part of executive directors or procurators have been identified, the report shall be submitted to the competent management body.

(2) In case of identified violations and breaches on the part of the management bodies or if in cases under paragraph 1 insufficient measures have been taken by these bodies, the report shall be submitted to the superior body in compliance with the bank's Articles of Association, as well as to the Bulgarian National Bank.

Sub-section III

Annual Performance Report

Article 27. (1) The head of the internal audit unit shall present an annual report of the internal audit unit to the shareholders' general meeting and the board of directors, the supervisory board and the management board respectively.

(2) The annual report shall inform about main results of internal auditors' actions, measures taken and their execution. It shall include organisational issues and underlying tasks to be fulfilled in the following year and in the future.

Chapter Four

ORGANISATION, GOVERNANCE AND INTERNAL CONTROL ON A CONSOLIDATED BASIS

Article 28. Management bodies of banks, financial holding companies, mixed financial holding companies and mixed-activity holding companies which are subject to supervision on a consolidated basis by the Bulgarian National Bank shall ensure:

1. adoption and implementation of effective and reliable policies, rules and procedures for organisation and governance;

2. maintenance of control systems and application of procedures in compliance with the requirements of this Ordinance relating to directly and/or jointly controlled companies, including those which are not covered by the Law on Credit Institutions;

3. compatibility and coordination of systems for risk management on a consolidated basis, and

4. the required scope of management information.

Article 29. Management bodies of banks, financial holding companies, mixed financial holding companies and mixed-activity holding companies shall maintain internal rules and risk management systems adequate to the organisation of the group and the specificity of enterprises controlled.

Chapter Five
RELATIONSHIP WITH THE BANKING SUPERVISION

Article 30. (1) The Bulgarian National Bank shall assess the organisation, governance, internal rules and effectiveness of internal control in banks on an individual and consolidated basis.

(2) The Deputy Governor heading the Banking Supervision Department or persons authorised by him and the head of the internal audit unit shall periodically hold discussions and consultations on the banking risks inherent, the measures to be taken and the relations with audit companies conducting an independent financial audit of the bank under Article 76, paragraph 1 of the Law on Credit Institutions.

Article 31. (1) The head of the internal audit unit shall immediately notify the Bulgarian National Bank of established violations or malpractices in the bank's management that have led or may lead to material damages.

(2) Management bodies of banks, financial holding companies, mixed financial holding companies and mixed-activity holding companies shall submit to the banking supervision bodies the annual reports of the internal audit, and by request, reports on conducted examinations and other control actions.

ADDITIONAL PROVISION

§ 1. Within the meaning of this Ordinance:

1. International Standards for the Professional Practice of Internal Auditing shall be the International Standards for the Professional Practice of Internal Auditing issued by the Global Institute of Internal Auditors, USA and their translation in Bulgarian published by the Institute of Internal Auditors in Bulgaria.

2. Risk appetite shall be the aggregate level and types of risk an institution is willing to assume or maintain within its risk capacity, in line with its business model, to achieve its strategic objectives.

3. Risk culture shall be norms, attitudes and behaviours of the bank's management bodies and employees related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks.

4. Compliance risk shall be the risk of legal measures and sanctions, the risk of material financial loss, or loss to reputation the bank may suffer as a result of its failure to comply with laws, standards, codes of conduct, and internal rules applicable to bank's activities.

TRANSITIONAL AND FINAL PROVISIONS

§ 2. Banks shall bring their activity in line with the requirements of this Ordinance within three months after its enforcement.

§ 3. This Ordinance is issued on the grounds of Article 11a, paragraph 1, Article 73, paragraph 6 and Article 74, paragraphs 3 and 4 in relation to § 13 of the

Transitional and Final Provisions of the Law on Credit Institutions and is adopted by Resolution No 149 of 24 April 2019 of the Governing Council of the Bulgarian National Bank.

§ 4. This Ordinance repeals Ordinance No 10 of 2003 on the Internal Control in Banks (published in the Darjaven Vestnik, issue 108 in 2003; amended, issue 102 of 2006).