

Pursuant to Article 83, paragraph 7 of the Law on Banks (RS Official Gazette, Nos 107/2005, 91/2010, 14/2015 and 19/2025) and Article 15, paragraph 1 of the Law on the National Bank of Serbia (RS Official Gazette, Nos 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – CC decision, 44/2018 and 19/2025), the Executive Board of the National Bank of Serbia issues the following

D E C I S I O N
ON TERMS AND CONDITIONS OF IDENTIFICATION, MONITORING AND
MANAGEMENT OF BANK COMPLIANCE RISK

1. This Decision sets out detailed terms and conditions of identification, monitoring and management of bank compliance risk.

2. A bank's compliance risk is the risk of regulatory sanctions, financial loss or reputational damage due to the bank's non-conformance with the law and other regulations, internal acts of the bank, business standards, anti-money laundering and terrorism financing procedures, and other acts regulating the bank's operations.

The risk of regulatory sanctions from paragraph 1 hereof arises if a bank's conduct specified in that paragraph results in the regulatory authority taking measures against and/or imposing fines on the bank.

The risk of financial loss from paragraph 1 hereof arises if a bank's conduct specified in that paragraph results in negative consequences to the bank's financial operations.

The reputational damage from paragraph 1 hereof arises if a bank's conduct specified in that paragraph results in a loss to business reputation of the bank and client trust.

3. The bank shall set up an organisational unit in charge of compliance risk control, including advisory activities pertaining to bank's compliance, whose main tasks shall be to identify, monitor and manage the bank's compliance risk (hereinafter: Organisational Unit).

4. The bank shall regulate by its internal acts:

1) the position of the Organisational Unit in the organisational structure of the bank that ensures the functional and organisational separation of the Organisational Unit from other organisational units of the bank, preventing a conflict of interest;

- 2) responsibility for implementing the bank's compliance function;
- 3) responsibility of the Organisational Unit, or the scope of the bank's operations whose compliance with the law, other regulation, the bank's internal acts, professional rules, good business practice and the bank's business ethics the Organisational Unit controls in such a way as to ensure a clear separation of tasks and duties of the Organisational Unit from business lines and other functions of the bank's internal controls system;
- 4) the manner which ensures the independence of the Organisational Unit;
- 5) the manner of cooperation and communication of the Organisational Unit with all organisational units and employees of the bank (hereinafter: employees);
- 6) the relationship between the Organisational Unit and organisational units of the bank whose scope of activity includes risk management and internal audit;
- 7) right of access to information necessary for the exercise of the compliance function and the corresponding duty of bank staff to cooperate in providing this information;
- 8) right of the head of the Organisational Unit to present the compliance control findings to the bank's executive board, committee for monitoring the bank's operations and managing board, as well as the obligation to notify the executive board and monitoring committee about the identified omissions within the shortest possible term;
- 9) right of the head of the Organisational Unit to propose to bank bodies the engagement of adequate experts in order to investigate possible breaches of compliance;
- 10) obligation for the bank's subordinated companies abroad, as well as its branches and other organisational forms abroad, to notify the bank and the National Bank of Serbia about the discrepancy between the regulations and standards of the country in which they operate relative to the regulations of the Republic of Serbia. The notification also needs to contain the information that the regulations and standards of the country in which other organisational forms or subordinated companies of the bank operate – hamper or prevent the publication or exchange of information between the group members.

5. In setting up the Organisational Unit, the bank shall take care that its size, organisational and qualifications structure are commensurate with the bank's size, or the scope and type of the bank's activities, and that the number and profile of employees in the Organisational Unit enable effective and efficient compliance risk management.

For performing compliance tasks, the bank shall ensure a sufficient number of employees with appropriate qualifications, knowledge and experience, as well as professional and personal qualities, who are familiar

with and keep abreast of any changes to the law, secondary legislation and the bank's internal acts, are familiar with the professional rules, good business practices and the bank's ethical code, and have the skills and expertise to assess their mutual compliance and impact on the bank's operations.

The bank shall ensure that the employees from paragraph 2 hereof regularly attend training and development programmes.

6. The head of the Organisational Unit must have good business reputation and appropriate qualifications and experience in accordance with the provisions of the decision governing the detailed terms and manner of appointing key function holders in a bank.

The head of the Organisational Unit shall be appointed and relieved of duty by the bank's managing board.

The National Bank of Serbia shall give prior consent to the appointment of the head of the Organisational Unit in accordance with the decision governing the granting of the preliminary bank founding permit, bank operating licence and consents and approvals by the National Bank of Serbia.

The bank shall notify the National Bank of Serbia about the appointment, relief of duty or resignation of the head of the Organisational Unit, in line with the provisions of the decision from paragraph 1 hereof.

7. The head of the Organisational Unit and members of staff shall be independent in their work and shall only perform activities under their remit, bearing in mind the potential conflict of interest with other members of the bank staff and their activities.

With a view to performing their activities, the Organisational Unit's staff shall have the right of access to all organisational parts of the bank, as well as the right to obtain all required documents and/or information they need. They shall also have the right to demand that appropriate explanation and information are provided by all members of bank staff within a reasonable period of time.

For the purpose of conducting compliance control, timely provision of accurate and complete data, and their subsequent electronic processing, the bank shall ensure that the Organisational Unit has access to the bank's information system containing data about bank operations.

8. The Organisational Unit shall identify and assess the bank's key compliance risks and propose an annual plan of managing these risks, which also contains a staff training plan.

The annual plan from paragraph 1 hereof shall also contain the planned activities in executing the advisory role of the Organisational Unit, the planned compliance control in areas within the remit of the Organisational Unit, activities aimed at improving the ethical and professional standards of employee conduct, and the dynamics and deadlines for conducting all planned activities.

The annual plan from paragraph 1 hereof shall be adopted by the bank's managing board.

9. The Organisational Unit shall compose a quarterly report on its activities, including in particular a report on the implementation of the compliance risk management plan from Section 8, paragraph 1 of this Decision.

The Organisational Unit shall submit the report from paragraph 1 hereof to the bank's executive board, monitoring committee and the managing board for consideration.

The Organisational Unit shall also compose the annual report on compliance risk which it shall submit to the bank's executive board, monitoring committee and the managing board.

In addition to the report on the implementation of the compliance risk management plan, the reports from paragraphs 1 and 3 hereof shall also contain the key identified compliance risks, including risks identified in controls of the Organisational Unit and the implementation status of the proposed measures for managing these risks.

10. The Organisational Unit shall prepare a compliance monitoring programme, specifying in particular the Unit's methodology of work, manner and deadlines for preparing reports, and the compliance verification method.

The programme referred to in paragraph 1 hereof shall also stipulate the manner of establishing adequate and up-to-date procedures at the level of all organisational units of the bank, in compliance with the law, secondary legislation and the bank's internal acts, as well as with professional rules, good business practices and the bank's ethical code, enabling ongoing monitoring and measuring of the bank compliance risk.

The Organisational Unit's methodology of work refers to the formulation and conduct of adequate ongoing and efficient compliance control to enable identification and management of current and potential compliance risks, thereby ensuring the highest standards of bank performance.

The programme shall be adopted by the bank's managing board.

11. The Organisational Unit shall regularly and timely notify the bank's governing bodies about changes in laws and secondary legislation, and provide them with information on their content, deadlines for compliance with these changes, bank's internal acts that need to be amended and/or adopted to align with these changes, as well as the effects they may have on the bank's operations.

The Organisational Unit shall regularly and timely notify the organisational units to which amendments to the laws and secondary legislation from paragraph 1 hereof pertain about the said amendments and provide them with the information from that paragraph.

For the purpose of identifying, monitoring and managing the bank's compliance risk, the Organisational Unit shall, among other things:

1) develop and implement procedures and standards in the field of compliance function, as well as provide guidelines, advice, opinions, and recommendations on the application of these acts;

2) provide opinions on the compliance of the bank's internal acts with the law and other regulations, as well as on the bank's adherence to laws, other regulations, and internal acts;

3) issue opinions about the mutual compliance and proper application of the bank's internal acts;

4) conduct compliance controls, including monitoring and assessing the bank's compliance risk in relation to regulatory requirements;

5) perform controls of individual actions found to be non-compliant with the law, other regulations, or the bank's internal acts;

6) continuously monitor compliance risk, particularly by assessing its potential consequences;

7) conduct employee training to raise awareness of business ethics, integrity, and adherence to the bank's code of conduct.

12. The head of the Organisational Unit shall be responsible for efficient, ongoing, regular and quality performance of the compliance function and efficient implementation of the compliance risk management plan, timely drafting and submission of reports from Section 9, paragraphs 1 and 3 of this Decision, and implementation of the compliance programme from Section 10 of this Decision.

The head of the Organisational Unit shall promptly notify the bank's executive board and monitoring committee of any omissions established in the course of compliance control.

The head of the Organisational Unit shall have the right to directly approach the bank's managing board, when necessary.

13. The bank is required to perform and develop its compliance control function in a manner that enables the timely assessment of compliance risk at all organisational levels, including evaluating the emergence of such risk due to the introduction of new products, new business practices, or the outsourcing of bank activities to a third party, i.e. the bank must minimise the adverse impact of these risks on its operations.

14. Banks shall bring their internal acts in compliance with the provisions of this Decision by no later than 1 October 2025.

15. As of the application date of this Decision, the Decision on Terms and Conditions of Identification, Monitoring and Management of Bank Compliance Risk (RS Official Gazette, Nos 86/2007 and 89/2007 – correction) shall cease to be valid.

16. This Decision shall come into effect on the eighth day after its publication in the RS Official Gazette and shall apply as of 1 October 2025.

NBS EB No 32
12 June 2025
B e l g r a d e

Chair
of the NBS Executive Board
G o v e r n o r
National Bank of Serbia

Dr Jorgovanka Tabaković, sign.