

Pursuant to Article 89, paragraph 4, Article 93, paragraph 8, Article 129 and Article 133, paragraph 1 of the Law on Payment Services (RS Official Gazette, No 139/2014), and Article 15, paragraph 1 of the Law on the National Bank of Serbia (RS Official Gazette, No 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015 and 40/2015 – CC decision), the Executive Board of the National Bank of Serbia hereby issues the

D E C I S I O N

ON GOVERNANCE AND INTERNAL CONTROLS SYSTEMS OF PAYMENT AND ELECTRONIC MONEY INSTITUTIONS AND ON SAFEGUARDING FUNDS OF PAYMENT SERVICE USERS AND ELECTRONIC MONEY HOLDERS

1. This Decision sets out detailed terms and conditions for the establishment, maintenance and upgrading of the governance and internal controls systems in payment and electronic money institutions, specifies liquid and low-risk types of assets in which payment and electronic money institutions may invest funds in accordance with Articles 93 and 133 of the Law on Payment Services (hereinafter: the Law), and lays down the terms and conditions of investment into these types of assets by payment institutions and electronic money institutions with a view to safeguarding the funds of payment service users and electronic money holders.

For the purpose of this Decision, institution shall imply both a payment institution and an electronic money institution, unless they are specifically designated.

Governance and internal controls systems

2. The institution shall establish, maintain and improve reliable, efficient and comprehensive governance and internal control systems that ensure responsible and reliable management of a payment institution.

The systems referred to in paragraph 1 hereof shall be proportionate to the nature, scope and complexity of services provided by the institution.

The systems referred to in paragraph 1 hereof shall be considered reliable, efficient and comprehensive if they enable the

institution to manage risks it is or may be exposed to in connection with its business activities relating to the provision of payment services and/or electronic money issuance.

Business activities referred to in paragraph 3 hereof shall also imply operational activities that the institution has outsourced to another party, as well as activities that the bank has outsourced to the institution pursuant to the decision governing risk management by banks and this Decision.

The institution shall put in place procedures for the assessment and review of acts, actions and procedures establishing the systems referred to in paragraph 1 hereof, shall regularly review whether these systems are adequate and efficient and proportionate to the nature, scope and complexity of services provided by the institution, and shall amend and supplement them as necessary.

Governance system

3. Governance system of an institution shall encompass:

– organisational structure with precisely and clearly defined, transparent and consistent division and distinction between tasks, as well as responsibilities and duties relating to the provision of payment services and/or electronic money issuance, including the provision of these services through branches and/or agents, or outsourcing of certain operational activities relating to the provision of these services;

– effective and efficient procedures for identifying, measuring and monitoring risks to which the institution is or might be exposed, and for managing these risks and/or reporting on these risks;

– appropriate information system.

Organisational structure

4. The institution shall, in accordance with the legal form in which it operates and the services it provides, establish such organisational structure and/or internal organisation that ensures clear division of duties and responsibilities between the management bodies of the institution, and between members of these bodies, the person who is directly managing the provision of payment services and/or electronic money issuing in the institution and other employees (hereinafter: employees) in a manner that

prevents concentration of mutually incompatible offices, ensures clear line of responsibility, prevents conflict of interests, and ensures an adequate system of internal controls and efficient control of operational risks of the institution.

The institution shall ensure:

- that employees' tasks, duties and responsibilities are identified unequivocally in the institution's internal regulations on the organisation of its operation;

- that all employees are aware of their tasks, duties and responsibilities;

- efficient communication and cooperation at all organisational levels, as well as provision of timely and reliable information necessary for decision-making to managing bodies and the director of the institution;

- that the process of decision-making and implementation of decisions is transparent, documented and based on the principles of safe and sound management of the institution.

5. In accordance with the legal form in which it operates and the services it provides, the institution shall define and implement business strategy which contains clearly set business objectives whose accomplishment can be easily monitored, and shall put in place the procedures for monitoring the accomplishment of these objectives.

6. In accordance with the scope, type and complexity of the activities it performs, the institution shall define and implement human resources management policy based on the principles that ensure hiring of staff with adequate knowledge, expertise and professional experience, as well as define the policy of employee promotion and reward which implies the assessment of employee performance and encourages reasonable and prudent risk-taking.

7. To ensure the implementation of business strategy, risk management strategy and policies and smooth functioning of internal controls systems, the institution shall enable adequate communication, exchange of information and cooperation at all organisational levels.

The institution shall ensure that members of the managing bodies of the institution have continuous access to all data and information relevant for the operation of the institution, and particularly:

- data and information on liquidity and capital position of the institution and/or potential deterioration of that position,
- data on compliance of the institution's operations with the rules laid down in regulations and internal regulations, as well as on major deviation from these rules in practice.

Risk identification, measurement and monitoring

8. The institution shall ensure that the risks that the institution is or may be exposed to in its operation are identified, measured and monitored, on a long-term basis, in a uniform and consistent manner, and shall provide for the management of and reporting on such risks.

9. The institution shall adopt the risk management strategy which shall include in particular:

- summary and definitions of all risks the institution is or may be exposed to;
- long-term business objectives determined by the institution's business strategy, as well as risk propensity consistent with these objectives;
- main principles of risk taking and management;
- basic principles for the management of the institution's capital.

Risk management strategy should be consistent with the institution's business strategy, and with the nature, scope and complexity of the activities it performs.

The institution shall review the risk management strategy periodically and amend it as necessary, particularly in the case of significant changes of the institution's business strategy and/or changes in macroeconomic environment in which the institution operates.

10. To identify, measure and monitor risks and to define its risk profile, the institution shall adopt policies and/or risk management procedures which shall regulate in particular:

- manner of organising risk management process in the institution and clear division between employees' responsibilities in all stages of that process;

- manner (methodology) of risk identification and assessment and the methodology for assessment of individual types of risk;

- measures for mitigation of individual types of risk, rules for their implementation and monitoring;

- manner of monitoring and control of individual types of risk and establishment of the system of acceptable levels (limits) of the institution's exposure to these risks;

- manner of decision-making on business transactions resulting in overrun of the set limits, and definition of exceptional circumstances where these overruns may be permitted within the bounds of the law.

11. The institution shall make sure in particular that its policies and procedures for risk identification provide for timely and comprehensive risk identification and envisage the analysis of causes that lead to the occurrence of risks.

Policies and procedures for risk measurement shall in particular contain quantitative and/or qualitative methods on the basis of which the institution shall define its risk profile and/or the type and level of risks that it is exposed to in its operation, as well as risk propensity, i.e. the risks it may accept in pursuance of its business objectives, and on the basis of which it may detect on time any change in its risk profile, including emergence of new risks.

Risk management policies and procedures shall in particular contain a description of risk mitigation procedures, as well as a description of risk monitoring and control procedures.

An institution shall review its risk management policies and procedures at least once a year or more frequently in case of significant changes in the institution's risk profile, and amend them as necessary.

Information system

12. In accordance with the legal form, nature, scope and complexity of its operations, the institution shall establish an adequate information system which meets the conditions prescribed by the decision of the National Bank of Serbia setting minimum standards for information system management in a financial institution.

13. The institution shall be required to establish such a reporting system which shall, at all levels in the institution, ensure timely, accurate and sufficiently detailed information necessary for business decision-making and efficient risk management, as well as for safe and sound operation of the institution.

Reporting on the emergence of risks that have not been previously identified and on unusual intensity of risks that have been previously identified shall be included in the risk reporting system in due time.

Internal controls systems

14. The institution shall establish and implement, in accordance with its legal form, nature, scope and complexity of operations, an efficient and reliable system of internal controls, which shall be included in all its business activities and which shall ensure continuous monitoring of the risks the institution is or may be exposed to in its operation, as well as the safety and soundness of the institution's operation.

The system of internal controls shall represent a set of processes and procedures laid down in this Decision which relate to risk management, compliance and internal audit, established for the purposes of efficient and effective management of the institution, adequate risk management and control, monitoring of effectiveness and efficiency of operation, reliability of financial and other data and information of the institution and for the purposes of ensuring compliance of the institution's operation with regulations governing the prevention of money laundering and financing of terrorism, as well as with other regulations, internal regulations and business standards.

The institution shall organise the processes and procedures referred to in paragraph 2 hereof in accordance with its legal form and the nature, scope and complexity of the services it provides;

however it shall be required to ensure functional and organisational separation between risk management activities and compliance and internal audit activities.

15. The internal controls system of the institution shall ensure provision of timely information on any detected deficiencies to the institution's competent officers, as well as application of measures to eliminate such deficiencies and making changes to the internal controls system when necessary.

The institution shall be required to ensure that internal controls are an integral part of all day-to-day activities of its employees and that the employees understand, in conformity with good business practices, professional and ethical standards, the purpose and the importance of these controls and their own contribution to their effective implementation.

Using the system of internal controls, the institution shall establish, where applicable, controls that restrict access to the institution's physical property and/or ensure its safety. These controls shall include various forms of restriction of access to the institution's physical property (e.g. multiple verifications or joint verifications by several persons), as well as taking periodic inventories of this property.

Risk management

16. The institution shall establish comprehensive and reliable risk management processes and procedures, integrated in all its business activities, which ensure that its risk profile is always in line with already established risk propensity.

Risk management processes and procedures within the meaning of paragraph 1 hereof shall be considered comprehensive and reliable if they enable the institution to manage the risks it is or may be exposed to in connection with its business activities.

Risk management processes and procedures within the meaning of paragraph 1 hereof shall be considered integrated in all business activities of the institution if every business decision whereby the institution assumes certain risks (including outsourcing of operational activities to another party, deciding on introduction of new products, and the conditions under which certain transactions are negotiated) is made by taking into

consideration prior assessment of the employees in charge of risk management.

17. The institution shall be required to establish, on the basis of strategies, policies and procedures referred to in Sections 9 and 10 hereof, an effective and efficient risk management process which encompasses mitigation, monitoring and control of risks that the institution is or may be exposed to and which it has identified and measured and/or assessed.

Risk mitigation shall imply risk diversification, transfer, reduction and/or avoidance and the institution shall implement it having regard to its risk profile and risk propensity.

Monitoring and control of risks shall imply frequency and manner of monitoring risks which the institution is exposed to, as well as monitoring and control of limits within the established system of limits.

Compliance

18. The institution shall establish adequate mechanisms and procedures for identification and monitoring of compliance risk of the institution and for management of that risk, which shall in particular encompass the investigation of compliance of internal regulations of the institution with relevant regulations, mutual compliance between different internal regulations and compliance of the business practice of the institution with relevant regulations and its internal regulations.

Compliance risk is the possibility of adverse effects on the institution's financial result and capital as a consequence of failure to comply with the law and other regulation, operating standards, procedures for prevention of money laundering and financing of terrorism and other rules governing operation of the institution; it includes in particular the risk of sanctions by the regulatory authority, risk of financial losses and reputational risk.

19. The supervisory board of the institution or another competent body shall adopt relevant procedures that enable continuous monitoring and measuring of compliance risk at the level of all organisational units, which particularly imply appropriate accounting procedures and procedures for assessing compliance with regulations governing the prevention of money laundering and terrorism financing.

Internal audit

20. The institution shall organise internal audit activities in the manner that ensures autonomy and independence of internal audit, and shall make sure that these activities are carried out in accordance with the law governing auditing, this Decision and other legal, professional and internal regulations.

The institution shall enable continuous implementation of comprehensive audit of all activities of the institution, in particular:

- assessment of adequacy, reliability and efficiency of the established governance and internal controls systems of the institution;

- assessment of adequacy and reliability of established procedures for risk identification and measurement, and/or risk assessment and management, including procedures for compliance risk monitoring and measurement;

- assessment of adequacy and reliability of accounting policies and procedures of the institution;

- assessment of reliability, accuracy and promptness of the reporting system within the institution, as well as system of reporting to the National Bank of Serbia;

- issuing of appropriate recommendations for eliminating the observed irregularities and deficiencies and for improving the internal regulations applied in the institution.

The institution shall ensure that the internal audit plan is adopted annually and that it encompasses at least activities referred to in paragraph 2, indents one and two of this Section.

The institution shall ensure that the reports on conducted audits are made regularly and that they are submitted to the supervisory board or another competent body of the institution, which has the obligation to review these reports.

The institution shall establish and implement adequate mechanisms for monitoring the implementation of activities specified in the recommendations which are issued on the basis of findings contained in the reports referred to in paragraph 4 hereof.

Performance of activities outsourced by banks and reporting on these activities

20a Under the governance and internal controls system the institution shall clearly and unambiguously ascertain and distinguish between operational activities it performs on its behalf and for its account and operational activities it performs on behalf of and for the account of the bank by which it was outsourced to perform these activities.

The institution intending to perform certain activities on behalf of and for the account of the bank as outsourced activities shall establish the following in its internal acts:

- the process of decision-making on the performance of outsourced activities and the criteria for making the decision, so as to ensure that the performance of outsourced activities does not jeopardise regular business of the institution, efficient risk management by the institution and its internal controls system;

- manner of integrating those activities in the risk management process and in the system for internal reporting on risks;

- manner of informing payment service users that the institution shall perform payment service provision/electronic money issuance activities for which it was outsourced, on behalf of the bank and for its account, and on the fees charged to payment service users for the provision of these services.

Before the adoption of the decision on every individual performance of outsourced activities, the institution shall obtain a substantiated opinion of the organisational unit responsible for risk management on the impact of the performance of outsourced activities on the risk profile of the institution.

When adopting the decision on every individual performance of outsourced activities, the institution shall particularly assess the impact of the performance of outsourced activities on the risk profile of the institution, the quality of services provided by the institution to users, costs and financial result of the institution.

The institution can perform a certain activity of a bank as outsourced only if it informs the National Bank of Serbia thereof not later than 30 days before signing the contract on outsourcing that

activity and provides the following documents and information along with that notification:

- 1) decision of the competent management body of the institution on the performance of outsourced activities, containing the assessment referred to in paragraph 4 of this Section;
- 2) main information on the bank (business name and head office) whose activities are outsourced to the institution;
- 3) the description of the activities outsourced by the bank to the institution, information on the addresses where those activities will be performed – in the event of outsourcing the provision of payment services/issuance of electronic money activities, and the outsourcing period;
- 4) draft contract with the bank whose activities are outsourced to the institution;
- 5) opinion from paragraph 3 of this Section.

If there is an intention to amend the contract on outsourcing signed by the institution and the bank, the institution shall inform the National Bank of Serbia thereof not later than 15 days before signing of the annex to the contract, and submit the draft annex and other documents and information from paragraph 5 of this Section along with the notification depending on the scope and significance of intended amendments in performing the outsourced activities.

In the event of the cancellation of the contract on outsourcing the activities signed by the institution and the bank, the institution shall immediately inform the National Bank of Serbia thereof.

The institution can subcontract another party to perform the activities for which it was outsourced by the bank only with the prior consent of the bank, provided in each individual case in accordance with the provisions of the decision governing risk management by banks.

20b The institution shall establish and maintain the single records of all the activities it was outsourced to perform pursuant to Section 20a hereof.

The institution shall submit to the National Bank of Serbia the information from the records referred to in paragraph 1 of this

Section in the form defined in Schedule 1, printed along with this Decision and is integral part thereof, on a semi-annual basis within the following deadlines:

1) information on the balance as at 30 June of the current year – by 31 July of the current year;

2) information on the balance as at 31 December of the current year – by 31 January of the next year.

Information from paragraph 2 of this Section shall be submitted to the National Bank of Serbia in accordance with the guidelines of the National Bank of Serbia governing electronic submission of the information in question, published on the website of the National Bank of Serbia.

Liquid and low-risk types of assets in which the institution may invest funds and the terms and conditions of investment in such types of assets

21. The institution shall be required to safeguard funds received from payment service users and/or funds received in exchange for issued electronic money by investing them into liquid and low-risk types of assets, in accordance with Articles 93 and 133 of the Law.

Assets referred to in paragraph 1 hereof shall include:

1) debt financial instruments issued by the Republic of Serbia or by the National Bank of Serbia, and/or guaranteed by the Republic of Serbia;

2) debt financial instruments issued or guaranteed by the European Central Bank, a Member State of the European union (or its central bank) which has been assigned credit rating corresponding to at least credit quality step 3 (investment rank) within the meaning of the decision of the National Bank of Serbia governing capital adequacy of banks, and which are denominated and settled in the currency of any Member State;

3) debt financial instruments issued and/or guaranteed by an international development bank and/or an international organisation within the meaning of decision referred to in point 2) of this paragraph;

4) debt financial instruments issued or guaranteed by a state, central bank, territorial autonomy or local self-government, public

administrative body, financial sector entity or a company which in accordance with the decision referred to in point 2) of this paragraph would be assigned credit risk weight of no more than 50%;

5) units of investment funds which invest only in instruments referred to in points 1) through 4) of this paragraph.

The institution shall be required to determine its policy of investment in types of assets referred to in paragraph 2 hereof and to lay down in this policy the limits on investment into each individual type of assets, as well as to review this policy at least every three years or more often in case of significant changes in investment terms.

22. If the funds received for the purposes of exchange for issued electronic money are transferred to an electronic money institution by means of a payment instrument, that institution shall not be required to safeguard these funds until they are credited to the electronic money institution's payment account or are otherwise made available to the electronic money institution in accordance with the Law.

In any event, the electronic money institution shall safeguard the funds referred to in paragraph 1 above within five business days from the issuance of electronic money.

23. If the electronic money institution provides payment services that are not directly linked to the issuance of electronic money, it shall safeguard the funds received from payment service users or other payment service providers in relation to the execution of a payment transaction in accordance with Articles 93 and 94 of the Law and Section 21 of this Decision.

24. This Decision shall enter into force on the eighth day from its publication in the RS Official Gazette and shall apply as of 1 October 2015.

NBS Executive Board No 55
19 June 2015
B e l g r a d e

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

Jorgovanka Tabaković, PhD