RS Official Gazette, Nos 23/2013, 113/2013, 2/2017, 88/2019 and 37/2021

Pursuant to Article 15, paragraph 1 and Article 63, paragraph 2 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 and 106/2012), the Executive Board of the National Bank of Serbia issues the following

DECISION
ON MINIMUM INFORMATION SYSTEM MANAGEMENT STANDARDS FOR FINANCIAL INSTITUTIONS

I. INTRODUCTORY PROVISIONS

1. This Decision lays down minimum standards and requirements for safe and sound information system management in banks, insurance undertakings, financial leasing providers, voluntary pension fund management companies, as well as in payment institutions, electronic money institutions and the public postal operator in the part of their activities regarding the provision of payment services and/or issuance of electronic money (hereinafter: a financial institution).

This Decision also lays down minimum standards for business continuity management and disaster recovery in a financial institution.

This Decision applies to all financial institutions, unless stipulated otherwise.

2. For the purpose of this Decision:

1) *information system* means a comprehensive set of technological infrastructure (hardware and software assets), organisation, people and procedures for the collection, processing, storage, transfer, presentation and use of data and information;

2) *information system resources* means software assets, hardware assets and information assets;

3) *software assets* means all types of system and application software, software development tools and other software;

4) *hardware assets* means computer equipment, communication equipment, data storage media, and other technical equipment supporting the functioning of the information system;

5) *information assets* means data in files and databases, program code, configuration of hardware assets, technical and user documentation, internal regulations, procedures etc;

6) *information system users* means all persons authorised to use the information system (employees in a financial institution, employees in other entities accessing the information system of a financial institution, clients of a financial institution accessing the institution's information system through electronic interactive communication channels etc);

7) *information system risk* means the possibility of negative effects on the financial result and capital, achievement of business objectives, operation in accordance with regulations, and reputation of a financial institution due to inadequate information system management or other system weaknesses which negatively affect the system functionality or security, and/or jeopardise the business continuity of the financial institution;

8) *controls* means policies, procedures, practices, technologies and organisational structures relating to the information system and established to reasonably ensure that business objectives of a financial institution will be achieved and that undesired events will be prevented or detected. Controls may differ by the implementation method (administrative, technical and physical) and purpose (preventive, detective and corrective);

9) *administrative controls* means the adoption and implementation of policies, standards, plans, procedures and other internal acts, and the establishment of an adequate organisational structure, for the purpose of achieving and maintaining the adequate level of information system functionality and security;

10) *technical controls* means controls implemented in hardware and software assets of the information system;

11) *physical controls* are controls protecting the information system resources from unauthorised physical access, theft, physical damage or destruction;

12) *preventive controls* means controls aimed at the prevention of problems and incidents;

13) *detective controls* means controls aimed at the detection and recognition of problems and incidents, and the identification of problems and incidents which occurred;

14) *corrective controls* means controls aimed at the limitation and elimination of problems and consequences of incidents;

15) *incident* means every unplanned and undesired event that may jeopardise the information system security or functionality;

16) *information system security* means upholding the principles of confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability;

17) *confidentiality* means that data and information are not disclosed or made available to unauthorised persons;

18) *integrity* means that data, information and processes are protected from unauthorised or unforeseen modifications, or that any such modifications do not remain undetected;

19) *availability* means that data, information and processes are available and usable on request of the authorised party;

20) *authenticity* means that parties involved are who they claim they are;

21) *accountability* means that each activity in the information system may be traced uniquely to its source;

22) *non-repudiation* means that an activity performed in the information system or receipt of information cannot be denied;

23) *reliability* means that the information system consistently and expectedly performs the anticipated functions and provides correct information;

24) *authorisation* means granting access rights to information system users;

25) *identification* means user identity presentation upon login and in the course of activity in the information system;

26) *authentication* means user identity verification and confirmation by using one of the following elements or their combination:

– something that only the user knows (e.g. the password, personal identification number etc),

– something that only the user possesses (e.g. magnet card, chip card, token, cryptographic key etc),

– something that only the user is (biometric characteristics such as the fingerprint, iris, voice, handwriting etc);

27) *privileged access to the information system* means access to information system resources which enables authorised users (administrators of system software, network, databases etc) to override technical controls;

28) *remote access to the information system* means access to information system resources from a remote location by using the telecommunication infrastructure over which a financial institution does not have full control;

29) *operational and system logs* means chronological logs about events and activities on information system resources (logs of operating systems, application software, databases, network devices etc);

30) *malware* means any type of program code created with the intention to gain unauthorised access to information system resources, collect information, cause unexpected behaviour or interruption in functioning of this system, and/or to otherwise potentially jeopardise the confidentiality, integrity or availability of these resources (e.g. computer viruses, worms, Trojan horses etc);

31) *critical/key business processes* means business processes or functions whose inadequate functioning may significantly jeopardise the operation of a financial institution;

32) *maximum acceptable outage (MAO)* means the maximum acceptable period of unavailability of a business process, and/or the critical time for process recovery;

33) *service delivery objective (SDO)* means the adequate level of business process recovery which should be achieved within the recovery time objective;

34) *recovery time objective (RTO)* means a period, and/or phases in the period during which the adequate level of business process recovery is to be achieved;

35) *recovery point objective (RPO*) means the longest acceptable period from the last backup copy until the occurrence of unavailability of a business process;

36) *backup copy* means the copy of at least those source data (software assets and information assets) which are needed for the recovery and/or reestablishment of business processes;

37) *electronic services* means services which clients of a bank, payment institution, electronic money institution and the public postal operator use remotely through the internet, and which include accessing a payment and another account, initiating payment transactions and other activities which involve accessing data in relation to the services of these financial institutions which could be subject to fraudulent activities or other abuse.

II. INFORMATION SYSTEM MANAGEMENT FRAMEWORK

3. In accordance with the nature, volume and complexity of operation, a financial institution shall establish an adequate information system which meets the following minimum conditions:

1) possesses functionalities, capacity and performances enabling the provision of suitable support to business processes;

2) provides timely, accurate and complete information important for making business decisions, efficient performance of business activities and risk management, and/or for safe and stable operation of a financial institution;

3) is designed to include adequate controls for validation of data entering the system, data being processed and data exiting the system, in order to prevent inaccuracies and inconsistencies of data and information.

A financial institution shall ensure that all data processing systems important for business operation, including the reporting system, are an integral part of the information system.

4. In accordance with the nature, volume and complexity of operation and the complexity of the information system, a financial institution shall establish, supervise, regularly review and upgrade the process of managing this system, for the purpose of reducing the exposure to risks and preserving

the security and functionality of the system, and shall define by an internal regulation, in accordance with law, the authorisations and responsibilities of its management and supervision bodies relating to these activities.

5. In accordance with its business strategy and the nature, volume and complexity of operation, a financial institution shall adopt the information system development strategy.

In accordance with the information system development strategy, the financial institution shall adopt the appropriate strategic and operational plans.

When needed, the financial institution shall amend the information system development strategy, particularly if this is required by amendments and/or supplements to its business strategy.

The financial institution shall notify the National Bank of Serbia on any amendments and/or supplements to the information system development strategy, 15 days upon their adoption.

6. For the purpose of adequate information system management, a financial institution shall provide adequate organisational structure, with a clearly defined distribution of tasks and responsibilities of employees, and/or with established internal controls which prevent the conflict of interest.

As part of the distribution of tasks and responsibilities referred to in paragraph 1 hereof, the financial institution shall clearly define tasks and responsibilities of employees which are directly related to efficient and appropriate management of information system security.

7. A financial institution shall ensure the application of all internal regulation and procedures relating to the information system, and shall also ensure that all system users are familiar with the content of these regulations and procedures, in accordance with their authorisations, responsibilities and needs.

8. A financial institution shall adopt and document the adequate methodology to determine the criteria, manner and procedures of managing projects related to the information system.

9. A financial institution shall determine the criteria, manner and procedures of reporting to its competent body about relevant facts relating to the information system functionality and security.

III. INFORMATION SYSTEM RISK MANAGEMENT

10. Provisions of regulations on general terms and method of managing risks in operation of financial institutions shall also apply to information system risk management, unless stipulated otherwise by this Decision.

11. Within the comprehensive risk management system, a financial institution shall establish the information system risk management process which includes risk identification, measurement, assessment, mitigation, monitoring and control.

12. A financial institution shall manage the information system risk in order to ensure smooth management of the system security and business continuity of a financial institution.

Information system risk management must cover the entire information system of a financial institution and must be integrated in all phases of system development.

13. A financial institution shall adequately manage risks arising from contractual relations with legal and natural persons whose activities relate to its information system.

A financial institution shall continuously supervise the manner and quality of contracted activities referred to in paragraph 1 hereof.

IV. INTERNAL INFORMATION SYSTEM AUDIT

14. In accordance with the nature, volume and complexity of operation, and the complexity of the information system, a financial institution shall cover by its internal audit methodology the criteria, manner and procedures for the internal audit of this system based on the results of risk assessment.

15. Internal audit of the information system of a financial institution shall be performed in accordance with regulations on operation of financial institutions.

V. INFORMATION SYSTEM SECURITY

16. In accordance with complexity of the information system, a financial institution shall adopt an internal regulation to establish the framework for system security management (hereinafter: information system security policy).

The information system security policy shall define in particular the principles, manner and procedures of achieving and maintaining the

adequate level of system security, including the authorisations and responsibilities relating to system security and resources.

A financial institution shall harmonise the security policy with changes in the environment and the information system.

17. A financial institution shall establish the process of information system security management as a continuous process of identifying needs for such security and achieving and maintaining the adequate level of such security.

In accordance with the nature, scope and complexity of operations, as well as the information system complexity, the financial institution shall:

1) carry out the distribution of tasks related to the system security in such a way that the internal regulations governing the organisation of its operations may clearly define the tasks and responsibilities of employees related to the security;
2) nominate the key employees in charge of information system security, taking care of the fact that their position has a significant impact on activities and decisions taken in relation to that security;
3) involve a sufficient number of employees with appropriate expertise and professional experience in information system security management.

A financial institution shall identify and monitor the needs for information system security, at least based on the results of risk assessment and obligations arising from regulations, internal regulations, contractual relations etc.

18. For the purpose of achieving and maintaining the adequate level of information system security, a financial institution shall establish adequate controls.

19. A financial institution shall by its internal regulations determine in more detail the criteria, manner and procedures for the classification of information assets according to the degree of sensitivity and criticality – in light of possible consequences of jeopardising their confidentiality, integrity and availability, and shall consistently implement such classification and accordingly ensure the adequate level of protection of these assets.

A financial institution shall appoint a person and/or persons employed in that institution, who shall be responsible for the management, classification and protection of information assets.

20. A financial institution shall implement the adequate control of access to information system resources and, in relation to this, it shall establish an adequate system of managing user access rights.

The system of managing user access rights shall encompass in particular the processes of registering, authorisation, identification and authentication of information system users, including the supervision of user access rights.

A financial institution shall ensure that the authorisation of information system users be based on the principle of granting the minimum possible access rights to system resources, which enable the efficient performance of activities.

A financial institution shall periodically and when required, but at least once a year, revise user access rights.

When managing user access rights, a financial institution shall regulate in particular the privileged and remote access to the information system.

21. Based on the results of information system risk assessment, a financial institution shall establish an appropriate system of monitoring the information system and generating operational and system logs.

A financial institution shall ensure the adequate protection, and specify the retention period, as well as the frequency, scope and manner of monitoring logs referred to in paragraph 1 hereof.

The logs referred to in paragraph 1 hereof must contain a sufficient quantity of information to enable the identification of problems, reconstruction of events, detection of unauthorised access and activities relating to information system resources, as well as to enable the establishment of related responsibilities.

22. By applying appropriate controls, a financial institution shall protect information system resources and other systems supporting the functioning of the information system against unauthorised physical access, theft, physical damage or destruction caused by a human or natural factor.

A financial institution shall in particular ensure the integrity of payment transactions data during their processing and storage, and during any other activity relating to these data.

23. A financial institution shall protect information system resources against malware by applying appropriate controls.

VI. BUSINESS CONTINUITY MANAGEMENT AND INFORMATION SYSTEM DISASTER RECOVERY

24. In order to ensure smooth and continuous functioning of all its important systems and processes, and to limit losses in emergency situations, a financial institution shall establish the business continuity management process.

25. A financial institution shall ensure that business continuity management be based on the business impact analysis and risk assessment, which include in particular:

1) establishment of resources and systems needed for the performance of individual business processes, their interdependence and interrelatedness;
2) risk assessment relating to individual business processes, including the probability of occurrence of undesired events and their potential impact on business continuity, financial situation and reputation of the financial institution;
3) establishment of acceptable levels of risks and techniques for mitigation of identified risks;
4) establishment of the maximum acceptable outage (MAO) of individual business processes;
5) establishment of critical/key business processes and activities.

In accordance with implemented activities referred to in paragraph 1 hereof, a financial institution shall adopt the recovery strategy to be implemented in case of interruption of operation, which shall contain in particular:

1) priorities of recovery of business processes, as well as resources and systems needed for their implementation;
2) service delivery objectives (SDO);
3) recovery time objectives (RTO);
4) recovery point objectives (RPO).

26. Based on activities implemented in accordance with Section 25 of this Decision, the board of directors of a bank and a financial leasing provider, and/or the competent body of an insurance undertaking and a voluntary pension fund management company, payment institution, electronic money institution and the public postal operator shall adopt the business continuity plan and the disaster recovery plan which primarily determine the creation of

conditions for the recovery and availability of resources of the information system, needed for the performance of critical/key business processes.

The business continuity plan shall contain in particular:

1) description of procedures in case of interruption of operation;
2) updated list of all resources necessary for the reestablishment of business continuity;
3) data on teams to be responsible for the reestablishment of operation in case of occurrence of unforeseen events and data on appointed members of these teams, including their clearly stipulated duties and responsibilities, and the plan of internal and external lines of communication;
4) the alternate site – in case of interruption of operation and the inability to resume business processes on the primary site.

The disaster recovery plan shall contain in particular:

1) procedures for information system recovery in case of disasters;
2) priorities of recovery of information system resources;
3) data on teams to be responsible for information system recovery and on the appointed members of these teams, including their clearly defined duties and responsibilities;
4) alternate site for information system recovery, and/or location of the secondary data centre.

For the purpose of efficient implementation of plans referred to in paragraph 1 hereof, a financial institution shall ensure that all employees are familiar with their roles and responsibilities in case of emergency situations.

A financial institution shall take all necessary activities to harmonise plans referred to in paragraph 1 hereof with business changes, including changes in products, activities, processes and systems, with changes in the environment and the business policy and strategy.

A financial institution shall periodically and after the occurrence of significant changes, but at least once a year, test plans referred to in paragraph 1 hereof, and shall also document the results of these tests and ensure their incorporation in the reporting to the competent body of a financial institution.

The executive board of a bank and financial leasing provider, and/or the competent body of an insurance undertaking and a voluntary pension fund management company, payment institution, electronic money institution and the public postal operator which manages the company's activities in line

with law, shall be responsible for the implementation of plans referred to in paragraph 1 and paragraphs 4–6 hereof.

27. In managing business continuity, a financial institution shall also take into account the outsourced activities and the dependence on services of these persons.

28. In case of circumstances requiring the implementation of the business continuity plan and the disaster recovery plan, a financial institution shall inform thereof the National Bank of Serbia, by no later than the next day following the occurrence of these circumstances. The National Bank of Serbia may require additional documentation relating to relevant facts about these circumstances and may set the deadline for the submission of such documentation.

29. A financial institution shall establish the incident management process providing a timely and efficient response in the case of breach of security or functionality of information system resources.

In case of an incident which seriously jeopardised or disturbed its operation or which could seriously jeopardise or disturb its operation, a financial institution shall inform the National Bank of Serbia:

1) promptly upon learning of the circumstances of occurence of such incident – if such incident occured due to the distured functionality of the information system resources;
2) promptly upon learning of the incident – if such incident occured due to the disturbed security of the information system;
3) promptly upon learning of the circumstances of occurence of such incident or upon learning of the incident – if such incident occured at the service provider and materially impacted or could have materially impacted the information system of a financial institution.

Following the notification referred to in paragraph 2 hereof, if the incident is underway, the financial institution shall continuously inform the National Bank of Serbia on important events and other relevant information related to the incident (incident status), as well as of the activities taken to mitigate the incident and its consequences. This information shall contain a detailed description of the incident, information on the estimated number of users impacted by the incident, a rough time needed to address the incident, potential impact on other financial institutions, as well as the important events and other relevant information since the occurrence of the incident (e.g. information on whether the incident has escalated, whether new causes have been detected, and on the efficiency of implemented actions).

The financial institution shall submit to the National Bank of Serbia the final report on the incident which occurred 15 days upon the cessation of the incident, i.e. as of the day it estimates that the financial institution has resumed its regular operations and the information system is stable. This report shall contain the final information on the incident – dates of occurrence and cessation of the incident, length of the incident, type of the incident (inaccessibility of hardware components, problems in operation of software components or security incident), description of the incident, causes of occurrence and consequences of the incident, activities taken by the financial institution in the course of the incident, plan of preventative activities to preclude repeated occurrences of the same incident, the number of users affected by the incident, the incurred financial costs connected with the incident, impact on other financial institutions and other relevant information, as needed.

29a. A financial institution shall quarterly report to the National Bank of Serbia on incidents related to abuse of sensitive data of financial service consumers, unauthorised payment transactions, abuse, theft or loss of payment instruments, including technical manipulations on ATMs, frauds and abuses of financial service consumers, abuses of authentication factors and authentication system etc. which did not directly impact its information system.

The report from paragraph 1 hereof shall be submitted by no later than 10th day of the first month in the quarter and the National Bank of Serbia may regulate in more detail the manner of report submission.

30. A financial institution shall establish the backup management process, and shall for this purpose determine detailed procedures and responsibilities.

Backup management must include the procedures of backup copies creation, storage and testing, as well as the restoration of data and software assets, so as to enable the reestablishment of business processes within the recovery time objective.

A financial institution shall ensure that backup copies are up-to-date and adequately protected, and that recovery procedures are tested and successful.

At least one up-to-date and complete backup copy must be adequately stored at an appropriate distance from the source location, based on results of information system risk assessment and taking into account the need to avoid the impact of the same risks on both locations.

31. Based on the activities taken in accordance with Section 25 of this Decision, a financial institution shall ensure the availability of the secondary data centre with appropriate equipment, functionality and security level, at an appropriate distance from the primary data centre, taking into account the need to avoid the impact of the same risks on both locations.

VII. INFORMATION SYSTEM DEVELOPMENT AND MAINTENANCE

32. A financial institution shall establish the information system development process in line with relevant changes in the institution and in the environment, in order to ensure the continuous adequacy of the system.

33. A financial institution shall implement the information system development process in line with the adopted information system development strategy and the project management methodology, taking into account functional requirements and needs for security.

When developing the information system in-house, a financial institution shall establish and document the development process which shall cover the analysis and design, programming, testing and migrating into production use.

A financial institution shall appropriately separate the development, testing and production environment.

34. A financial institution shall establish the process of hardware and software asset management, in all phases of their life cycle – from the point of procurement or development until the withdrawal from use.

A financial institution shall ensure that hardware and software asset management includes, *inter alia*, the maintenance of detailed and up-to-date records of these assets, the appointment of a person and/or persons employed in that institution, who shall be responsible for the management and protection of such assets, as well as the definition of rules for their acceptable use and secure disposal upon the withdrawal from use.

35. A financial institution shall ensure the adequate maintenance of hardware and software assets of the information system in line with the manufacturer’s recommendations, keep records of such maintenance, and ensure that the system security or functionality are not thereby jeopardised.

36. A financial institution shall establish the change management process for hardware and software assets of the information system, so as to avoid unexpected and undesired behaviour of the system and/or to avoid jeopardising the system security or functionality.

The change management for software assets of the information system shall in particular include the following procedures:

1) identification of initial versions of these assets;
2) initiation, analysis and approval of change requests;
3) chronological documentation of all changes in these assets and database architecture together with the time when the changes occurred;
4) informing the information system users of the details of implemented changes.

A financial institution shall ensure that all changes in hardware and software assets, including new assets and systems, be tested and approved before becoming operational, and shall also define the plan for restoring the system to the previous state.

A financial institution shall regulate by an internal general act the process for managing urgent changes in hardware and software assets of the information system.

37. A financial institution planning data migration into the new core business application or other computer centre and/or which changes the location of the computer centre shall inform the National Bank of Serbia thereof at least 30 days before the planned start of the testing related to that migration.

The notification referred to in paragraph 1 hereof shall contain in particular:

1) detailed descriptions of systems among which data are being transferred;
2) plan, dynamics and description of the activities regarding data migration, including the testing methodology;
3) results of risk assessment and the description of controls to be applied during data migration, with the aim to preserve the confidentiality, integrity and availability of data;
4) plan for restoring the system to the state prior to data migration which includes the dynamic of such restoration and description of activities, as well as the criteria for making the decision to implement this plan.

Notwithstanding paragraph 1 hereof, if a financial institution plans data migration due to a status change in regard to which it shall obtain prior consent and/or license of the National Bank of Serbia, it shall also submit to the National Bank of Serbia, simultaneously with the request for obtaining this consent and/or license, the notification with data referred to in paragraph 2

hereof, and the bank shall also submit a request for enabling the functioning of an interim account of the legal successor (hereinafter: request for an interim account), which must be signed by the legal representative of the legal successor – so that National Bank of Serbia can act upon the request in the cases determined in this Section.

An interim account of a legal successor shall be an account of a bank which ceases to exist due to a status change, this account being opened at the National Bank of Serbia in accordance with the regulations, and/or rules of operation of the payment system in which that bank participates, which is, due to the status change, taken over by the legal successor, for the purpose of its interim functioning within the deadline set by this Decision.

A financial institution which decides to implement the plan of restoration to the status prior to data migration shall promptly inform the National Bank of Serbia thereof.

If it decides to implement the plan of restoration to the status prior to data migration due to a status change, the bank shall notify the National Bank of Serbia thereof not later than the next business day after the day when it started data migration and not later than one hour prior to the start of the period set by the Daily Time Schedule of the NBS RTGS payment system (hereinafter: NBS RTGS system) for executing transfer orders in that system.

The National Bank of Serbia shall enable the functioning of the interim account referred to in paragraph 4 hereof in the event that a bank decides to implement the plan of restoration to the status prior to data migration.

Notwithstanding paragraph 7 hereof, if there are objective circumstances that may jeopardise the interests of clients of the bank implementing data migration due to status change, the National Bank of Serbia may, on a reasoned requested submitted by the bank along with the documentation referred to in paragraph 3 hereof, separately determine the deadline for the implementation of the data migration process and enable the functioning of the interim account within that deadline.

The financial institution shall implement data migration due to status change no later than ten business days after the day it started to implement the plan, and/or within the deadline determined by the National Bank of Serbia in accordance with paragraph 8 hereof.

An interim account of a legal successor referred to in this Section, as well as the actions of the National Bank of Serbia in accordance with the request for an interim account shall be regulated in more detail by the Operating Rules of the NBS RTGS Payment System.

38. A financial institution shall ensure the drafting, keeping and regular maintenance of documentation relating to the information system so that the documentation is correct, complete and up-to-date at all times.

A financial institution shall provide all information system users with access to relevant documents in line with work requirements.

39. A financial institution shall ensure adequate and continuous professional development and training of employees to use the information system and preserve its security and functionality.

VIII. OUTSOURCING OF ACTIVITIES RELATING TO THE INFORMATION SYSTEM

40. The outsourcing of activities relating to the information system of a financial institution (hereinafter: outsourcing) shall be performed in line with regulations on operation of financial institutions, unless stipulated otherwise by this Decision.

The activities referred to in paragraph 1 hereof shall be all activities which include processing, storage and/or access to data which are in possession of a financial institution and which relate to its operation, as well as the activities of development and/or maintenance of core business applications.

Outsourcing also includes the outsourcing to parties related to a financial institution through ownership and management relations (persons with participation, members of the group of companies to which the institution belongs etc), which operate in the Republic of Serbia or abroad.

The use of standardised services (SWIFT, Bloomberg, Reuters etc) or telecommunication services, or the procurement of software which is available off-the-shelf etc. shall not be considered outsourcing.

Outsourcing shall be performed based on the contract concluded between a financial institution and the party to which activities are outsourced (hereinafter: service provider).

41. A financial institution intending to outsource shall regulate:

1) the decision-making process regarding outsourcing and the criteria for making such decision;
2) manner of including these activities in the risk management process and in the system of internal reporting on risks;
3) manner of ensuring the continuity of outsourced activities and measures to be taken in the event of termination of the contract with service providers, or temporary failure or discontinuation of their services;

4) manner of supervising outsourced activities, including the supervision of the compliance of such activities with regulations, good business practice and generally accepted standards in the corresponding area.

A bank intending to outsource to a third person activities whose implementation is relevant for ensuring the continuity of its critical functions, shall ensure the continuity of those functions in the case of implementing resolution instruments and/or measures, in one of the following ways:

1) by obliging such person to carry out the outsourced activities in all situations in which it is necessary to ensure the continuity of critical functions of a bank in resolution, and/or a bridge bank;

2) by a contract with an alternative supplier which could ensure the continuity of performance of critical functions of a bank in resolution and/or a bridge bank;

3) a detailed plan for ensuring the continuity of performance of critical functions by using internally available resources of the bank in resolution and/or a bridge bank.

42. Prior to making a decision on each outsourcing and/or on a change of the service provider, a financial institution shall:

1) perform a detailed analysis of a potential service provider relating to its capacity to provide services, its financial situation and business reputation;

2) determine whether regulations of the country or countries in which a potential service provider operates enable the National Bank of Serbia to smoothly perform on-site control of operations in the segment relating to the performance of outsourced activities or is connected to these activities;

3) assess possible difficulties and the time needed for the selection of another service provider, or the possibility to continue performing these activities within a financial institution in case of termination of the provision of contracted services and to adopt the appropriate exit strategy, which shall contain a list of measures and activities to be taken, and the schedule of their implementation from the moment of termination of the provision of contracted services until the selection of another service provider, or until the process for these activities within the financial institution has been fully set up.

When making the decision referred to in paragraph 1 hereof, a financial institution shall assess in particular the impact of outsourcing on:

1) business continuity and reputation of a financial institution;

2) costs, financial result, liquidity and solvency of a financial institution;

3) risk profile of a financial institution;

4) the quality of services that a financial institution provides to clients.

43. A financial institution shall ensure that the service provider grants to the financial institution, external auditor and the National Bank of Serbia timely and unlimited access to the documentation and data relating to outsourced activities.

A financial institution shall ensure that each contract concluded with a service provider contains the provision obliging the service provider to fulfil the obligation referred to in paragraph 1 hereof, as well as the provision enabling a financial institution to unilaterally terminate the contract if so ordered by the National Bank of Serbia and in accordance with that order.

A financial institution shall ensure that the National Bank of Serbia smoothly performs on-site supervision of outsourced activities on the premises of the service provider, or at the location where the outsourced activities are performed.

44. A financial institution shall ensure that the outsourcing does not jeopardise the information system security or functionality and that data of the financial institution remain in its possession.

A financial institution shall ensure that a service provider carries out outsourced activities in line with the information system security policy and other acts of the financial institution governing the security of its information system.

When outsourcing activities and/or performing the outsourced activities, the financial institution and the service provider shall act in compliance with the law on personal data protection and other regulations which govern the keeping of secrets arising from operation of financial institutions.

45. A financial institution may outsource particular activities and/or change the service provider only if it informs thereof the National Bank of Serbia by no later than 30 days before the conclusion of the outsourcing contract.

If the contract referred to in paragraph 1 hereof is amended without amending the outsourced activity and/or the service provider, or without impacting the results of the analysis from Section 42, paragraph 1, provision 1) of this Decision and/or the results of the assessment from Section 42, paragraph 2 of this Decision – the financial institution shall inform the National Bank of Serbia thereof minimum 15 days prior to concluding the Annex to the contract and submit to it the Draft Annex.

The notification referred to in paragraph 1 hereof shall contain in particular:

1) the decision on outsourcing and/or change of the service provider issued by the competent body managing a financial institution;

2) the description of activities that a financial institution intends to outsource, obligations and conditions that the service provider must fulfil, and the duration of outsourcing;

3) basic data on the service provider (business name, head office, registration and tax identification numbers, and/or other data in case of a foreign service provider);

4) results of the analysis referred to in Section 42, paragraph 1, subparagraph 1 of this Decision;

5) the exit strategy referred to in Section 42, paragraph 1, subparagraph 3 of this Decision;

6) results of the assessment referred to in Section 42, paragraph 2 of this Decision;

7) the draft outsourcing contract;

8) evidence that regulations of the country/countries where the service provider operates enable the National Bank of Serbia to smoothly perform the on-site control of operations in the segment relating to the performance of outsourced activities or is connected to these activities – if the service provider is headquartered outside of the Republic of Serbia or if it is envisaged by contract that it shall perform the outsourced activities outside of the Republic of Serbia.

The deadline referred to in paragraph 1 hereof shall run from the day of submission of duly completed documentation from that Section.

46. (*Deleted*)

47. A service provider may outsource to a third person the activities that a financial institution outsourced to such service provider, or other tasks relating to these activities, but only with the prior consent of the financial institution in each individual case, in accordance with Sections 41–44 of this Decision.

A financial institution may grant the consent referred to in paragraph 1 of this Section only if it informed the National Bank of Serbia of the intended outsourcing of activities or tasks referred to in that paragraph by no later than 30 days before granting the consent.

The notification referred to in paragraph 2 hereof shall contain in particular:

1) the draft decision of the competent body managing a financial institution on granting the consent referred to in paragraph 1 hereof;

2) the description of activities that a service provider intends to outsource, obligations and conditions that the third person referred to in paragraph 1 hereof must fulfil;

3) basic data on the third person referred to in paragraph 1 hereof (business name, head office, registration and tax identification numbers, and/or other data in case of a foreign person);

4) results of the analysis referred to in Section 42, paragraph 1, subparagraph 1 of this Decision;

5) the reviewed exit strategy referred to in Section 42, paragraph 1, subparagraph 3 of this Decision;

6) results of the assessment referred to in Section 42, paragraph 2 of this Decision;

7) the draft contract between a service provider and the third person referred to in paragraph 1 hereof on outsourcing of activities referred to in that paragraph;

8) evidence that regulations of the country/countries where the third party referred to in paragraph 1 hereof operates enable the National Bank of Serbia to smoothly perform the on-site control of operations in the segment relating to the performance of outsourced activities or is connected to these activities – if the third person is headquartered outside of the Republic of Serbia or if it is envisaged by contract that it shall perform the outsourced activities outside of the Republic of Serbia.

The deadline referred to in paragraph 2 hereof shall run from the day of submission of duly completed documentation from that Section.

48. A financial institution shall be fully responsible for the activities that it outsourced to service providers.

The financial institution shall continuously supervise the service provision and perform quality assurance of provided services related to outsourced activities.

If during the control and/or supervision the National Bank of Serbia determines that a financial institution, due to omissions in operation of the service provider or another party referred to in Section 47 of this Decision, does not act in accordance with this Decision and other regulations, it may order the financial institution to terminate the contract on outsourcing, concluded with the service provider.

48a. The financial institution shall submit to the National Bank of Serbia the contract from Section 40, paragraph 5 of this Decision, including Annexes to that contract – within 15 days from the date of conclusion of such contract and/or Annex.

In the event of termination of the contract referred to in paragraph 1 hereof, the financial institution shall promptly inform the National Bank of Serbia thereof.

IX. ELECTRONIC SERVICES

49. As an integral part of information system risk management, a bank, payment institution, electronic money institution and the public postal operator providing electronic services (hereinafter: electronic service provider) shall establish the process of managing risks arising from the provision of electronic services.

50. In providing electronic services, an electronic service provider shall apply secure and efficient methods for the verification and confirmation of the identity and authorisations of persons, processes and systems.

An electronic service provider shall ensure that user authentication is enabled during the use of these services, and that it consists of the combination of at least two mutually-independent elements for user identity confirmation.

By way of derogation from paragraph 2 hereof, an electronic service provider may apply user authentication containing a single element for user identity confirmation, in the case of:

1) low-value payments, in accordance with the payment services framework contract, provided that risks related to the total amount of these payments are managed accordingly (e.g. by setting a maximum amount for these transactions within a specified period after which authentication will take place, in line with paragraph 2 hereof, or additional protection measures will be applied),

2) payments to the payees pre-specified by the payer (e.g. introducing the so-called white list of payees),

3) the transfer of funds between two payment accounts of the same user held with the same electronic service provider,

4) the transfer of electronic money done with the same electronic service provider, based on risk analysis of these payment transactions,

5) other transactions and services assessed under the risk analysis as low-risk.

An electronic service provider may apply the user authentication referred to in paragraph 3 hereof only if it has notified the National Bank of Serbia thereof at least 30 days prior to the start of service provision and has provided, along with that notification, a comprehensive and in-depth risk

analysis and method to manage risks arising from the provision of services in the manner specified in items 1) to 5) of that paragraph and other relevant documentation pertaining to this analysis.

The analysis referred to in paragraph 4 hereof shall also include the analyses referred to in paragraph 3, items 4) and 5) hereof, if an electronic service provider intends to implement user authentication by using a single element for user identity confirmation in cases envisaged under those items.

The deadline referred to in paragraph 4 hereof shall be calculated from the day of submitting complete documentation referred to in that paragraph.

51. An electronic service provider shall adopt and implement rules that shall accordingly, in line with the market practice and risk assessment, limit the number of attempts to log into the electronic services system, i.e. the number of authentication attempts, to set the longest user idle time upon logging into the system, and to define the validity period of authentication parameters.

When using one time passwords for authentication (e.g. *One Time Password – OTP*), an electronic service provider shall ensure that the validity time of that password is restricted to the time required to perform authentication.

An electronic service provider shall set the maximum number of unsuccessful attempts to log into the electronic services system, after which that system will be permanently or temporarily blocked, and shall also set the procedures for safe re-activation of this system.

An electronic service provider shall set the longest possible user idle time on the electronic services system after logging into the system, upon which the user will be automatically logged out of the system (the so-called session timeout).

An electronic service provider shall make sure that appropriate confirmation of its identity is available on the electronic services distribution channel so that users can verify the authenticity of the electronic service provider.

An electronic service provider shall make sure that operational and system logs are available so as to ensure, to the extent applicable, the non-repudiation and accountability of actions relating to the provision of electronic services.

X. TRANSITIONAL AND FINAL PROVISIONS

52. An insurance undertaking, financial leasing provider and voluntary pension fund management company which outsource to a third person some of the activities referred to in Section 40 of this Decision until 30 June 2014 shall inform thereof the National Bank of Serbia by no later than 31 July 2014.

Along with the notification referred to in paragraph 1 hereof, an insurance undertaking, financial leasing provider and voluntary pension fund management company shall submit to the National Bank of Serbia the documentation and data determined in Section 45, paragraph 2 of this Decision.

A bank which outsources to a third person some of the activities referred to in Section 40 of this Decision until 31 December 2013, shall submit to the National Bank of Serbia, by no later than 31 January 2014, the exit strategy referred to in Section 42, paragraph 1, subparagraph 3 of this Decision.

If the third person referred to in paragraph 3 hereof is headquartered outside of the Republic of Serbia or it has been agreed that it shall perform the outsourced activities outside of the Republic of Serbia, a bank shall submit to the National Bank of Serbia, along with the exit strategy referred to in paragraph 3 hereof, the evidence referred to in Section 45, paragraph 2, subparagraph 8 of this Decision.

53. Sections 17 and 18 and Sections 68–72 of the Decision on Risk Management by Banks (RS Official Gazette, Nos 45/2011, 94/2011, 119/2012 and 123/2012) shall cease to be valid as of 1 January 2014.

Sections 6 and 8 of the Decision on Minimum Requirements Regarding Organisational and Technical Resources of Voluntary Pension Fund Management Company (RS Official Gazette, No 23/2006) shall cease to be valid as of 1 July 2014.

54. This Decision enters into force on the eighth day following its publication in the RS Official Gazette and shall apply as of 1 January 2014 to banks and as of 1 July 2014 to insurance undertakings, financial leasing providers and voluntary pension fund management companies.

NBS Executive Board No 7
12 March 2013
Belgrade

Chairman of
Executive Board of
the National Bank of Serbia

Governor of
the National Bank of Serbia

Jorgovanka Tabaković, PhD