Pursuant to Article 5, Paragraph 1, Item b), Article 20, Paragraph 2, Item b) and Article 37 of the Law on the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No. 59/13 and 4/17), Article 6, Paragraph 1, Item b) and Article 19, Paragraph 1, Item b) of the Statute of the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No. 63/17), the Management Board of the Banking Agency of Republika Srpska, at its 16th session held on 13 May 2025, adopted the

DECISION
ON MANAGING INFORMATION SYSTEM AND RISKS OF INFORMATION AND COMMUNICATION TECHNOLOGY IN BANK

I GENERAL PROVISIONS

Article 1

(1) This Decision shall define in more detail the obligations of the bank relating to information system management, information and communication technology risk management, including requirements relating to contracts and supervision of information and communication technology service providers by the bank, reporting on significant information and communication technology incidents, as well as cyber threats, testing of digital operational resilience and exchanging information on cyber threats.

(2) The provisions of this Decision shall apply to banks headquartered in Republika Srpska, to which the Banking Agency of Republika Srpska (hereinafter: the Agency) has issued an operating license.

(3) The bank shall apply the provisions of this Decision on an individual and consolidated basis.

(4) For issues related to information system management and information and communication technology risk management that are not regulated by this Decision but are regulated by law or other by-laws, the provisions of that law or other by-law shall apply.

Article 2

(1) Definitions used in this Decision shall have the following meaning:

1) **Information and communication technology** (hereinafter: ICT) – technology that enables the automated collection, processing, generating, storage, transmission, display, distribution, and disposal of information.
2) **Information system** (hereinafter: ICT system) - information and communication technology that is organized as part of a mechanism or interconnected network that supports the operations of a bank.
3) **Information asset** – a set of information in tangible and intangible form that is worth protecting.
4) **ICT asset** – software or hardware assets in network and information systems used by the bank.
5) **ICT system resources** – relate to information assets, ICT assets, human resources and processes.
6) **Software asset** – shall include application and system software, databases, development and testing tools, utilities and all other software products that are installed or licensed for use within the bank.
7) **Hardware asset** - physical components of an information system, which include: computers and computer equipment, communications equipment, data storage media, and other technical equipment that supports the operation of the information system.
8) **ICT system users** – all persons using the ICT system (bank employees, service providers, bank clients and others).
9) **ICT services** - services that ICT systems provide to users. Examples include data entry services, data storage and processing, as well as reporting, monitoring and operation and decision support services.
10) **ICT project** - any project in which ICT systems and/or services are changed, discontinued or implemented. ICT projects can be part of broader ICT programs or operation transformation programs.

11) **ICT product** - element or set of elements of the ICT system.
12) **ICT process** - a set of activities carried out to design, develop, implement or maintain an ICT product or ICT service.
13) **Critical functions** – in accordance with Article 2, Paragraph 1, Item 34) of the Banking Law of Republika Srpska (hereinafter: the Banking Law).
14) **Core business activities** – in accordance with Article 2, Paragraph 1, Item 35) of the Banking Law.
15) **Confidentiality -** a property that implies that data and information are not accessible or disclosed to unauthorized persons or processes.
16) **Integrity -** a property that implies that data, information and processes have not been altered in an unauthorized or unforeseen manner.
17) **Availability -** a property that ensures that data, information and processes are always available and usable at the request of an authorized person.
18) **Authenticity -** a property that ensures that a person's identity is truly which is claimed to be.
19) **Non-repudiation -** a property that ensures the impossibility of denying an activity performed in an information system or the receipt of information.
20) **Traceability -** a property that ensures that every activity in an ICT system can be unambiguously traced back to its source.
21) **Reliability –** shall mean that an ICT system consistently and as expected performs its intended functions and provides accurate information.
22) **Information security –** shall represent a set of measures required to preserve the confidentiality, availability and integrity of information and ICT systems.
23) **ICT system security -** the ability of ICT system to withstand, at a certain level of reliability, all events that may threaten the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services offered or accessed by these ICT systems.
24) **Risk -** the possibility of loss or disruption caused by an incident, expressed as a combination of the extent of that loss or disruption and the probability of the incident occurring.
25) **ICT risk –** shall represent the risk of loss due to breach of confidentiality, loss of integrity of systems and data, unsuitability or unavailability of systems and data or inability to change ICT within a reasonable period of time and at reasonable cost in the event of changing environmental or business requirements (adaptability feature). This risk also includes security risks arising from inadequate or failed internal procedures or external events, including cyber attacks or inadequate physical protection.
26) **Digital operational resilience** – shall mean the ability of a bank to build, secure and review its operational integrity and reliability so that, by using services provided by third parties, it directly or indirectly provides the full range of ICT capabilities required for the security of the ICT systems used by the bank and which support the continuous provision of financial services and their quality, including during disruptions.
27) **Vulnerability** – shall mean a weakness, vulnerability or deficiency in an ICT product or ICT service that a cyber threat can exploit.
28) **Controls –** shall include policies, procedures, practices, technologies and organizational structures related to the ICT system established to provide reasonable assurance that business objectives will be achieved and that undesirable events will be prevented or detected.
29) **Record –** a chronological record of activities on ICT assets (for example: records of operating systems, application software, databases, network devices, intrusion detection systems and activities on the ICT system, etc.).
30) **Operational or security incident (hereinafter: ICT incident) –** a single event or series of related events that were not planned by the bank, and that have or are likely to have a negative impact on the integrity, availability, confidentiality of data and/or authenticity of services.

31) **Avoided incident** – shall mean any event that could have compromised the integrity, availability, confidentiality of data and/or authenticity of services, but was successfully prevented from occurring or did not occur.
32) **Handling incident** - all operations and procedures aimed at preventing, detecting, analyzing, stopping or responding to an incident and recovering from an incident.
33) **Cyber security** - all activities necessary to protect ICT systems, users of those systems and other persons affected by them from cyber threats.
34) **Cyber attack** - malicious influence aimed at compromising information security that may cause an ICT incident.
35) **Cyber threat** - any possible circumstance, event or action that could damage, disrupt or otherwise negatively affect the ICT system, the users of the ICT system and other persons.
36) **Significant cyber threat** - a cyber threat that, based on its technical characteristics, can be assumed to have a serious impact on the bank's ICT systems or users of the bank's services by causing significant material or immaterial damage.
37) **Threat intelligence** - information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and to enable relevant and sufficient understanding in order to mitigate the impact of an ICT-related incident or of a cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations.
38) **Threat-led penetration testing (TLPT)** shall mean a framework that mimics the tactics, techniques and procedures of reallife threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the bank's critical live production systems.
39) **Chain of custody of related evidence** - the process that ensures that all information and materials collected as evidence are properly documented, stored, and transmitted in a manner that maintains their integrity, authenticity, and immutability. This process allows for the tracking of all movements and handling of evidence from the time it is collected to the time it is used in legal proceedings or other forms of audit.
40) **Outdated ICT system** – shall mean an ICT system that is at the end of its life cycle, which for technological or commercial reasons is not suitable for upgrade or repair or for which its supplier or ICT service provider no longer provides support, but is still in use and supporting the bank's functions.
41) **Backup data** - a copy of the original data required to re-establish the bank's business processes, and other data that the bank deems necessary to preserve.
42) **Business impact analyses BIA** – a process that includes the assessment of quantitative and qualitative effects that could occur in the event of unavailability of business processes and ICT system resources due to a specific incident, adverse event or breakdown. The goal of business impact analysis is to identify core business activities, processes and ICT system resources as part of the business continuity management process.
43) **Recovery time objective – RTO** - the longest acceptable time of unavailability of the bank's business process and the ICT system resources required for the business process performance, i.e. the time during which it is necessary to restore (recover) the business process.
44) **Recovery point objective – RPO** - the longest acceptable period from the last data backup to the occurrence of business process unavailability, i.e. the longest acceptable period of data loss in the event of an incident.
45) **Service delivery objective** – SDO – the level of service to be achieved during the alternative processing method until a return to normal operations is made.
46) **Change Request** – a request to change or modify any aspect of an ICT service, system, infrastructure, process or documentation.
47) **User Request** - a request from an ICT system user for access to certain ICT system resources or services, a request for information or advice, and other standard requests (e.g. password reset, equipment request, etc.) that do not fall into the category of incidents or changes.

48) **Third party** – a private individual or legal entity who/which has established a business relationship or concluded a contract with the bank for the purpose of providing a product or service, including providers of outsourced services.

49) **ICT third-party risk** - ICT risk that may arise in connection with the use of ICT services provided by third parties or their subcontractors in the ICT domain.

50) **ICT service provider** is a third party that performs a certain activity in the field of ICT, partially or entirely, based on a contract concluded with the bank.

51) **ICT service provider within a group** - an entity that is part of a financial group and that mainly provides ICT services to financial entities within the same group.

52) **General data** – data that falls into the category of personal or sensitive data.

53) **Bank governing bodies –** bank supervisory board and bank management.

(2) Definitions not defined in this Article, but used in this Decision, shall have the meaning in accordance with regulations and other by-laws.

II RESPONSIBILITIES

Article 3

(1) The bank shall be obliged to adopt and implement internal acts, in the form of strategies, policies, methodologies, procedures and work instructions, which regulate the management of the ICT system, including the use, monitoring and supervision of the ICT system.

(2) The internal acts referred to in Paragraph 1 of this Article shall be at least:

1) aligned with legal regulation and by-laws, standards and rules of the profession, requirements of the Agency, as well as with each other,

2) regularly, and at least once a year, reviewed and revised, and updated in the event of significant changes in the bank and the environment in which the bank operates, and

3) complete, detailed and applicable.

(3) The bank shall be obliged to ensure that all users of the ICT system are familiar with the content of internal acts relating to the ICT system, in accordance with their authorities, responsibilities and needs.

(4) Contracts, audit findings, reports reviewed by the bank's bodies, instructions and other documents should be drawn up, or translated, into one of the languages in official use in Republika Srpska.

Article 4

The bank supervisory board shall be obliged, as a minimum, to:

1) establish an adequate management system of the ICT system, as well as a system for measuring, monitoring, controlling and managing ICT risk, as part of the bank's comprehensive risk management system, in order to achieve a high level of digital operational resilience,

2) establish an adequate organizational structure with clearly defined and demarcated authorities, duties and responsibilities, professional qualifications and necessary competencies, including the roles and responsibilities of the Bank management members, taking into account that the number and necessary skills of employees are adequate to support the efficient and secure functioning of the ICT system and the management of ICT risks on a continuous basis,

3) ensure that information security management in its work and reporting line is independent from the management of the ICT system,

4) adopt a budget to meet the bank's needs for digital operational resilience, in terms of all types of resources, including relevant programs for raising awareness of information security and training in digital operational resilience, as well as acquiring knowledge and skills in the field of ICT for all employees in accordance with Article 21 of this Decision,

5) adopt an ICT system strategy, a digital operational resilience strategy and an information security policy, and ensure the conditions for their implementation, monitor their implementation and periodically review them, and at least once a year analyze and adapt to changes, taking into account the bank's business model, the complexity of the ICT system and the risk appetite,

6) stipulate the content and periodicity of reporting to the supervisory board and other relevant boards, bodies or persons in relation to:
   1. ICT system management, including reporting on the implementation of operational plans,
   2. ICT risk management, including a report on the level of digital operational resilience,
   3. significant ICT incidents, including a response plan, recovery activities and corrective measures,
   4. all contracts concluded with third parties in the ICT domain, and the risk assessment of third parties,
   5. all relevant changes to materially significant activities, the risk assessment, the potential impact of those changes on critical functions and/or core business activities, including the conclusions of the risk analysis and the impact assessment of those changes.

Article 5

(1) The Bank management shall be obliged, as a minimum, to:

1) prepare proposals for strategies and policies referred to in Article 4, Item 5) of this Decision adopted by the Supervisory Board, ensures their implementation at all decision-making levels and in business processes, and regularly report to the Supervisory Board on their implementation,
2) ensure an adequate framework for managing ICT risks, in order to achieve a high level of digital operational resilience, which needs to be reviewed at least annually,
3) ensure that all roles and responsibilities related to ICT system management, ICT risk, information security and business continuity, including management bodies, are adequately established, clearly defined and assigned, taking into account adequate segregation of duties, effective and timely communication, mutual cooperation and coordination,
4) ensure necessary and adequate resources for managing the ICT system and ICT risks, including ICT risks related to third parties. This implies:
   1. a sufficient number of employees with appropriate professional qualifications and skills to support ICT operational needs and ICT risk management processes on an ongoing basis, in order to ensure the implementation of the ICT system strategy and
   2. a sufficient budget for the above,
5) based on an assessment of the bank's risk profile, as well as the scope and complexity of its activities and services, regularly review the risks identified in connection with contracts for the use of ICT services that support critical functions and core business activities,
6) adopt and monitor the implementation of operational plans that support the implementation of the ICT system strategy, as well as significant changes to these plans,
7) periodically review the way in which the bank implements the business continuity policy in the area of ICT, and response and recovery plans,
8) establish an appropriate reporting system on the management of the ICT system, ICT risks and risks related to third parties,
9) prepare and periodically review the budget to meet the bank's needs in terms of digital operational resilience, for all types of assets, including relevant programs for raising awareness of information security and training in digital operational resilience, as well as acquiring knowledge and skills in the field of ICT for all employees in accordance with Article 21,
10) establish a function for monitoring contracts for the use of ICT services concluded with third parties or appoint a member of senior management who will be responsible for overseeing the associated risks and relevant documentation,
11) ensure that all employees, including key function holders, undergo appropriate training on ICT risks and information security, on an annual basis or more frequently if necessary, and

12) adopt and implement plans and procedures related to the management of ICT systems and information security, including, but not limited to, operational plans, procedures for managing ICT risks, managing ICT incidents, managing data backups, managing access to ICT systems, managing security patches and software updates, protecting against malicious software and other security threats, managing ICT assets, managing ICT projects, managing the procurement and maintenance of ICT systems, managing ICT changes, managing records, as well as business continuity plans in the area of ICT, response and recovery plans for ICT systems, business impact analysis and communication plans in crisis.

(2) Members of the Bank management responsible for managing the ICT system and ICT risks should possess an adequate level of knowledge and skills to understand and assess ICT risks and their impact on the bank's operations. They are also required to regularly participate in training in this domain, commensurate with the level of ICT risks they manage.

(3) The Bank management is required to establish an information security management function, including the appointment of a person responsible for information security and the definition of his or her powers, responsibilities and scope of work. In doing so, it is required to ensure the independence and objectivity of this function by ensuring that it is adequately separated from operational procedures related to ICT. Also, in accordance with the size, type, scope and complexity of the ICT system, as well as the nature, scope and complexity of its services, activities and operations, the Bank management shall be obliged to assess the required number of employees in the information security management function.

(4) The Bank management shall be obliged to appoint at least one person responsible for implementing communication plans in the event of an ICT incident, who will perform the function of communication with the public and the media for this purpose.

(5) The Bank management shall be obliged to consider the need to form a special body to coordinate activities related to the ICT system, taking into account the size of the bank, the nature, scope and complexity of its services, activities and operations, internal organization, and the size and complexity of the ICT system.

Article 6

(1) The person responsible for information security should be a competent person with appropriate professional qualifications, specialist knowledge and experience in the field of information security management and should hold relevant internationally recognized certificates in this field.

(2) The person referred to in Paragraph 1 of this Article shall supervise and coordinate activities related to information security, which shall include at least the following:

1) coordinates and implements internal controls in accordance with this Decision and relevant standards,
2) monitors and analyzes ICT systems, with the aim of detecting security threats and vulnerabilities,
3) participates in activities of identification and assessment of ICT risks and providing proposals for measures for managing ICT risks from Articles 15 to 19 of this Decision,
4) participates in the development of the information security policy from Article 17 of this Decision, and provides proposals for its improvement, in accordance with the development of ICT systems and ICT risks in the bank,
5) monitors changes implemented in ICT systems, including ICT projects and the development of new functionalities, and analyzes the impact of these changes on the existing level of information security and proposes protection measures and security controls,
6) participates in the development and implementing ICT incident response plans, including recovery,
7) ensures, monitors and coordinates activities related to the implementation of the digital operational resilience testing program, defined in Article 35 of this Decision,
8) ensures adequate and timely exchange of information on ICT incidents and cyber threats, in accordance with Articles 34 and 50 of this Decision,

9) participates in the assessment of ICT risks and proposes measures for the treatment of these risks in the case of engaging ICT service providers, as well as their compliance with the requirements of this Decision,
10) monitors security risks arising from the use of third-party services and products,
11) ensures, monitors and coordinates activities related to the implementation of information security awareness programs,
12) participates in the work of committees and working groups responsible for information security management.

(3) The person referred to in Paragraph 1 of this Article shall be obliged to report to the Bank management, at least quarterly, on the status and activities related to information security.

(4) The professional competence of the person referred to in Paragraph 1 of this Article shall be maintained through systematic and continuous training, whereby:
1) is educated in a timely manner about the risks of ICT systems and technologies used in the bank,
2) follows and is familiar with relevant international standards and guidelines related to the establishment and monitoring of information security,
3) is up to date with the latest ICT incident management practices, in order to be able to provide an effective response to current or new forms of cyber attacks,
4) follows relevant technological developments in order to better understand the potential impact that the introduction of new technologies could have on information security requirements.

Article 7

(1) The internal audit function shall, in accordance with the requirements stipulated by the Decision on the Bank Management System, conduct regular audits in the area of ICT, based on a defined internal audit work program.

(2) The frequency of the internal audit function activities in the area of ICT should be commensurate with the ICT risks in the bank, whereby all elements of the ICT risk management framework and all ICT processes must be reviewed in detail within the defined audit cycle.

(3) Persons conducting audits in the area of ICT should possess adequate professional knowledge and skills in this area.

Article 8

(1) The bank shall be obliged to conduct an external audit of the ICT system on an annual basis, in accordance with the Law and the Agency's bylaws regulating the field of external audit in banks, unless otherwise defined by the provisions of this Decision.

(2) If the Agency determines that the audit firm (hereinafter: the external auditor) has not performed an audit of the bank's ICT system or that the audit report is not in accordance with the law, by-laws adopted on the basis of the law, regulations in the field of audit and rules of the auditing profession, or if it is determined through the supervision of the bank's operations in this segment or in another manner that the audit assessment of the state of the ICT system and the adequacy of the management of the ICT system is not based on true and objective facts, it may reject the audit report and require the bank to have another audit firm to perform the audit at the bank's expense or, when it deems it necessary, directly appoint an audit firm at the bank's expense.

(3) The external auditor may not be a person whose report on the audit of the ICT system for the previous business year was not accepted by the Agency.

(4) The external auditor shall be obliged to submit to the Agency, at least 30 days before the start of the audit of the ICT system, an audit plan, which identifies the areas subject to the audit, the names of the persons who will perform the audit and their engagement, and the duration of the audit.

(5) When performing an audit of the ICT system, the external auditor shall take into account the outsourced services and their significance and impact on the ICT system, and accordingly develop an audit plan and an effective audit approach.

(6) The external auditor shall prepare an audit report on the conducted audit of the information system, and provide an assessment of the state of the ICT system and the adequacy of its management.

(7) The report on the conducted audit of the ICT system is a special report, which the bank shall submit to the Agency no later than 30 April of the current year.

(8) The Agency reserves the right to impose measures stipulated by the Banking Law and the Agency's by-laws governing external audits in banks.

III ICT SYSTEM MANAGEMENT

Article 9

(1) The bank shall be obliged to:

1) adopt an ICT system strategy,
2) define operational plans that support the implementation of the ICT system strategy and
3) establish procedures for monitoring and measuring the effectiveness of the ICT system strategy implementation.

(2) ICT system strategy referred to in Paragraph 1, Item 1) of this Article should:

1) define the connection and alignment of the strategic objectives of the ICT system with the bank's business objectives,
2) contain a description of the existing ICT architecture, as well as the way in which the bank's ICT system should be developed in order to effectively support and implement the bank's business strategy, including the development of the organizational structure, changes in ICT systems and key dependencies on third parties, and
3) define clear objectives in terms of information security, including key performance indicators and key risk parameters.

(3) The bank shall periodically update the ICT system strategy, especially in the event of changes in the bank's business strategy or significant changes in the risk management strategy, in order to ensure alignment between business objectives and ICT system objectives, as well as relevant plans and activities.

Article 10

(1) By means of the operational plans referred to in Article 9, Paragraph 1, Item 2) of this Decision, the bank shall define the activities to be undertaken in order to achieve the objectives of the strategy referred to in Article 9, Paragraph 2 of this Decision. The plans shall contain at least the following: a description of the activities and ICT projects, including activities for the implementation of corrective measures resulting from the ICT risk assessment, financial resources, human resources, deadlines and information on responsible persons.

(2) The bank shall regularly monitor and review the operational plans in order to ensure their relevance and appropriateness.

(3) The Bank management should be informed clearly, in detail and in a timely manner about the implementation and status of the activities defined in the operational plans, at least on a quarterly basis.

Article 11

(1) The bank shall establish, implement, monitor, maintain, regularly review and continuously improve the ICT system management process in accordance with relevant standards, regulatory requirements and internal policies.

(2) The bank shall use and maintain up-to-date ICT systems, protocols and tools that are:

1) appropriate to the scope of operations supporting the bank's business activities, in accordance with the principle of proportionality referred to in Article 13 of this Decision,

2) reliable,
3) equipped with sufficient capacity for:
   1. accurate and reliable processing of data necessary for the performance of business activities and the timely provision of services,
   2. periods of increased system load (processing the largest number of orders, messages or transactions),
   3. introduction of new technologies and
4) technologically resilient in order to adequately cope with additional data processing needs in stressed market conditions or other adverse situations.

(3) In addition to the internal documents referred to in Article 3 of this Decision, the bank shall obtain and store all relevant documentation (technical, functional, user and other), as well as information relating to the ICT system and its specific components. The aforementioned documentation shall be accurate, complete and up-to-date.

IV ICT RISK MANAGEMENT

Article 12

(1) The bank shall be obliged, in accordance with the Decision on the Management System, to establish a reliable, comprehensive and documented framework for managing ICT risks as part of its comprehensive risk management system.

(2) The framework referred to in Paragraph 1 of this Article should enable the bank to effectively manage ICT risks, which includes making adequate decisions on the treatment of ICT risks, implementing appropriate measures to manage that risk and ensuring a high level of digital operational resilience, with the aim of a rapid, efficient and comprehensive response to ICT risk.

Article 13

The bank shall apply the ICT risk management framework, as well as the rules set out in this Decision, in accordance with the principle of proportionality, taking into account the size and risk profile of the bank, as well as the type, scope and complexity of its services, activities and operations, internal organization, and the size and complexity of the ICT system.

Article 14

(1) The ICT risk management framework should include at least: strategies, policies, methodologies, programs, procedures and plans, and ICT protocols and tools necessary to adequately protect information assets and ICT assets, in order to minimize the impact of ICT risks.

(2) The bank shall be obliged to adopt a strategy for digital operational resilience, which includes methods of responding to ICT risk and achieving specific ICT objectives, and which:
   1) explains how the ICT risk management framework supports the bank's business strategy and its objectives,
   2) establishes the level of tolerance for ICT risk, in line with the bank's risk appetite, and analyses the impact of tolerance on ICT disruptions in operations,
   3) describes the reference ICT architecture and any changes that need to be implemented to achieve specific business objectives,
   4) describes the mechanisms in place to detect ICT incidents, prevent their impact and protect against such impacts,
   5) presents the current situation in terms of digital operational resilience based on the number of reported significant ICT incidents and the effectiveness of preventive measures,
   6) defines procedures for testing digital operational resilience,
   7) describes communication plans in the event of a significant ICT incident, and
   8) defines the strategy for the procurement of ICT from various ICT service providers.

Article 15

(1) Within the framework for the ICT risk management system, the bank shall be obliged to identify, classify and adequately document all business functions supported by ICT, roles and responsibilities, information assets and ICT assets supporting those functions, as well as their roles and dependencies in relation to ICT risk. The bank shall be obliged to review the adequacy of the classification and relevant documentation as necessary, and at least annually.

(2) When implementing the classification referred to in Paragraph 1, the bank shall be obliged to consider the requirements regarding confidentiality, integrity and availability.

(3) The bank shall identify all information assets and ICT assets, including those at remote locations, network resources and hardware equipment, and map critical and key information and ICT assets and clearly define responsibility for the assets. It is also necessary to map the configuration of information and ICT assets, as well as the connections and interdependencies between different information and ICT resources.

(4) Within the framework for the ICT risk management system, the bank shall be obliged to identify and document all processes that depend on ICT service providers, and determine the interconnection with ICT service providers that provide services that support critical functions or core business activities.

(5) The bank shall continuously identify all sources of ICT risk, in particular exposure to risks from and to other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT-supported business functions, information and ICT assets. The bank shall regularly, and at least once a year, review the risk scenarios affecting them.

(6) The bank shall be obliged to establish adequate records for the purposes of Paragraphs 1, 3 and 4, and to update them regularly, and necessarily after significant changes.

Article 16

(1) The bank shall conduct and document an ICT risk assessment at least annually or more frequently, and necessarily after any significant change in the ICT system, processes or procedures that affect its business functions supported by ICT, information assets or ICT assets.

(2) The bank shall conduct a separate ICT risk assessment for all outdated ICT systems at least once a year, and necessarily before and after the integration of technologies, applications or systems.

(3) Based on the ICT risk assessment referred to in Paragraph 1 of this Article, the bank shall determine what measures are necessary to reduce ICT risks to an acceptable level, and whether changes are necessary in the existing business processes, applied protection measures, ICT system and ICT services. In doing so, the bank shall be obliged to take into account the time required to implement these changes and the time required to take appropriate temporary measures to reduce ICT risks, so that the risks remain within acceptable limits in accordance with the bank's risk appetite.

(4) The bank shall be obliged to adopt a plan for the implementation of measures and continuously monitor the implementation of this plan. This plan shall at least include a review of all identified risks, a description of corrective measures, priorities and deadlines for implementation, and responsible persons. If the bank extends the deadline for unacceptable risks, it is obliged to promptly notify the Agency thereof.

Article 17

(1) In order to achieve and maintain an adequate level of ICT system security, the bank shall continuously monitor and control the functioning and security of ICT systems and tools, and minimize the impact of ICT risks to the minimum possible extent, so that the risks are in line with the bank's risk appetite.

(2) The bank shall define, develop and implement policies, procedures, protocols and tools for ICT security, in order to ensure the resilience, continuity and availability of ICT systems, especially those supporting critical functions and core business activities, and maintain high standards of availability, authenticity, integrity and confidentiality of data during storage, use and transmission.

(3) In order to achieve the objectives referred to in Paragraph 2, the bank shall be obliged to implement ICT solutions and processes in order to:

1) ensure the security of data transmission means,
2) minimize the risk of data corruption or loss, unauthorized access and technical deficiencies that may disrupt operations;
3) prevent reduced availability, violation of authenticity and integrity, breach of confidentiality and loss of data and
4) ensure data protection from risks arising from data management, including administrative failures, risks associated with data processing and human error.

(4) As part of the ICT risk management framework, the bank shall be obliged to:
1) adopt and implement an information security policy, which defines the rules for protecting the availability, authenticity, integrity and confidentiality of data, and information and ICT assets, in order to achieve the objectives in the field of information security,
2) establish a reliable structure for managing the ICT system, using an approach based on risk assessment, using appropriate techniques, methods and protocols, which may include automated mechanisms for isolating affected information and ICT assets in the event of a cyber attack (the possibility of immediate interruption or segmentation in order to minimize and prevent the transfer of risk);
3) implement policies that restrict physical or logical access to information and ICT assets on a least privilege basis, including remote access, and to that end, implement policies, procedures and controls that relate to access rights and ensure adequate management of access rights,
4) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, as well as measures to protect cryptographic keys used to encrypt data, based on the results of data classification and the ICT risk assessment process, and
5) establish procedures for managing ICT changes, in accordance with Article 31 of this Decision.

Article 18

(1) As part of the regular monitoring of ICT risk, the Bank shall establish mechanisms for continuous monitoring of ICT system and timely detection of unusual activities in accordance with Article 32 of this Decision, which includes problems with the performance of ICT system and ICT incidents, as well as the identification of potentially critical points of failure.

(2) The detection mechanisms referred to in Paragraph 1 should enable multiple layers of control, define alert thresholds and criteria for activating and initiating the ICT incident response process, including automatic mechanisms for informing relevant personnel responsible for responding to ICT incidents.

(3) The bank shall ensure adequate segregation of duties of employees in the monitoring process and the processes subject to monitoring.

(4) The bank shall regularly review the implemented protection and control measures for managing ICT risks, and assess their effectiveness and efficiency, including the framework for testing digital operational resilience defined in Articles 35 to 39.

(5) The bank shall continuously determine whether changes in the existing operational environment affect the implemented security measures or whether additional measures need to be implemented to adequately mitigate the associated risks. These changes should be an integral part of the formal change management process.

(6) The bank shall provide sufficient resources and capacity for:

1) monitoring user activities, detecting unusual occurrences in ICT systems and ICT incidents, in particular cyber attacks, and
2) collecting information on vulnerabilities and cyber threats, ICT incidents, in particular cyber attacks, and analyzing the impact they may have on the bank's digital operational resilience.

Article 19

(1) The bank shall adequately document the ICT risk management framework and review it at least annually or upon the occurrence of significant ICT changes, as well as in accordance with the findings of audit and supervisory reviews.

(2) The bank shall adequately and continuously incorporate into the ICT risk assessment process the lessons learned from digital operational resilience testing, as well as from actual ICT incidents, in particular cyber attacks, together with the challenges faced when activating ICT business continuity plans and ICT system response and recovery plans, as well as relevant information exchanged with financial entities and the findings of audit and supervisory reviews. Based on the above, the bank shall conduct appropriate reviews of the relevant components of the ICT risk management framework and their adequacy.

(3) The bank shall monitor the development of ICT risks over time, analyse the frequency, types, impact and development of ICT incidents, in particular cyber attacks and their patterns, with the aim of understanding the level of exposure to ICT risk, especially in relation to critical functions and core business activities, and improving the bank's cyber maturity and preparedness.

(4) The bank shall continuously monitor relevant technological developments, with the aim of understanding the possible impact of the application of new technologies on information security and digital operational resilience requirements. It shall also be up to date with the latest ICT risk management processes, in order to be able to respond effectively to current or new forms of cyber attacks.

Article 20

(1) As part of the ICT risk management framework, the bank shall be obliged to adopt crisis communication plans, which will define procedures for managing internal and external communication in the event of activation of the ICT business continuity plan or ICT system response and recovery plans, including significant ICT incidents.

(2) When defining the plans referred to in Paragraph 1 of this Article, the bank shall implement communication policies for employees and external participants. Communication policies for employees shall take into account the need to distinguish between employees involved in managing ICT risks, in particular employees responsible for response and recovery, and employees who need to be notified.

(3) The bank shall ensure responsible notification of clients and partners, at least about significant ICT incidents or vulnerabilities, as well as the public when relevant.

Article 21

(1) The bank shall include programmes for raising awareness on ICT system security and digital operational resilience training as mandatory modules within the employee training programme. The programmes and training shall be implemented for all employees, including senior management, and the level of complexity shall be commensurate with the scope of their duties and responsibilities. The bank may, where necessary, involve ICT service providers in these programmes and training in accordance with Article 27, Paragraph 3, Item 4.

(2) The bank shall ensure that the programmes and training are implemented regularly, and at least once a year, with particular attention to timely training in relation to identified ICT threats.

V MANAGING ICT RISKS RELATED TO THIRD PARTIES

Article 22

(1) Notwithstanding the provisions of the Decision on Outsourcing Management, the bank shall manage ICT risks related to third parties as an integral part of the ICT risk management framework referred to in Article 12 of this Decision.

(2) The bank shall establish managing ICT risks related to third parties in accordance with the following principles:

1) the bank that has concluded contracts for the use of ICT services for the purposes of its operations shall at all times bear full responsibility for compliance with and execution of all obligations under this Decision and the applicable legal framework,

2) the principle of proportionality and taking into account:

1. the nature, scope, complexity and importance of the dependence in the field of ICT and
2. the risks arising from contracts for the use of ICT services concluded with ICT service providers, taking into account the criticality or importance of the contracted service, process or function, and the possible impact on the continuity and availability of financial services and activities at the bank and group level.

(3) The bank shall include in its ICT risk management framework a policy on the use of ICT services, in particular ICT services supporting critical functions and core business activities, provided by third parties in the ICT sector, and shall apply it on an individual and, where necessary, consolidated basis.

(4) The bank shall timely notify the Agency of all planned contracts for the use of ICT services supporting critical functions and core business activities, as well as of the fact that a particular function or activity has become critical (core) in accordance with Articles 14, 15 and 16 of the Decision on Outsourcing Management.

Article 23

The bank shall be obliged to maintain and regularly update, both at the bank level and at the consolidated level, a register of information regarding all contracts for the use of ICT services provided by third parties.

Article 24

(1) Prior to concluding a contract for the use of ICT services, the bank shall be obliged to:

1) assess whether the contract includes the use of ICT services that support a critical function or core business activity,

2) assess whether regulatory requirements regarding contracting are met,

3) identify and assess all relevant risks related to the contract, in accordance with Article 8, Paragraph 1 of the Decision on Outsourcing Management, including the possibility that the contract may contribute to the strengthening of concentration risk, in accordance with Article 26 of this Decision,

4) conduct due diligence on potential ICT service providers and ensure the suitability of the ICT service provider throughout the entire selection and assessment process, and

5) identify and assess any conflicts of interest that the contract may give rise to.

(2) The bank shall enter into contracts exclusively with ICT service providers that apply appropriate ICT security standards. If the contract relates to services that support critical functions or core business activities, the bank shall, prior to entering into the contract, determine that the service provider applies relevant and recognized ICT security standards.

(3) The bank shall continuously monitor whether the ICT service provider complies with appropriate ICT security standards, which are in line with the bank's security objectives and measures, and request an independent assessment of compliance (e.g. relevant certificates, independent audit reports, etc.).

(4) The bank shall ensure and exercise the right of access to data and the right to audit the ICT service provider in accordance with Articles 12, 13 and 17 of the Decision on Outsourcing Management.

Article 25

(1) The bank shall ensure the possibility of terminating and/or cancelling the contract for the use of ICT services, in accordance with Article 9, Paragraph 7 of the Decision on Outsourcing Management, including the following situations:

1) monitoring of ICT risk related to third parties has identified circumstances that are considered to lead to changes in the performance of activities provided under the contract, including significant changes affecting the contract or the condition of the ICT service provider, and

2) weaknesses of the ICT service provider related to its management of ICT risks, and in particular in the manner in which it ensures the availability, authenticity, integrity and confidentiality of data, whether personal or other sensitive data or general data, have been documented.

(2) If the contract relates to activities that support critical functions or core business activities, the bank shall be obliged to adopt an exit strategy and procedures that are in line with the policy on the use of ICT services and the bank's business continuity plans, adhering to the provisions of Article 10 of the Decision on Outsourcing Management.

(3) The bank shall take into account in its exit strategies the risks that may arise at the level of ICT service providers, in particular the risk of termination of their services, deterioration in the quality of ICT services, disruption of business due to inappropriate or unsuccessful provision of ICT services or any other significant risk that could arise from inadequate and continuous provision of ICT services or termination/cancellation of contracts with ICT service providers.

(4) The bank shall ensure the possibility of termination and/or cancellation of contracts without interruption of its business activities, restrictions in achieving compliance with regulatory requirements and without negative consequences for the continuity and quality of services provided to clients.

Article 26

If the contract relates to activities that support critical functions or core business activities, the bank shall be obliged to, when determining and assessing the risks referred to in Article 24 of this Decision, consider the following:

1) the impact of concentration risk arising from a number of contracts concluded with the same ICT service provider or closely related ICT service providers,

2) the level of substitutability of the ICT service provider,

3) the benefits and costs of alternative solutions, such as the engagement of different ICT service providers, taking into account whether and how the envisaged solutions meet the business needs and objectives defined in the digital operational resilience strategy,

4) the potential benefits and risks of subcontracting, if the contract provides for the possibility that the ICT service provider may subcontract ICT services supporting critical functions or core business activities to another ICT service provider, in particular if the subcontractor is outside the territory of Bosnia and Herzegovina,

5) the legal provisions that would apply in the event of the bankruptcy of the ICT service provider, as well as any limitations that may arise during emergency recovery of bank data,

6) compliance with legal and regulatory requirements relating to data protection applicable to the bank, if the ICT service provider or the location for data storage and processing is located outside the territory of Bosnia and Herzegovina,

7) the impact of potentially long and complex subcontracting chains on the bank's ability to fully monitor contracted activities, as well as on the Agency's ability to effectively supervise the bank in such a case.

Article 27

(1) The bank shall enter into a written contract with the ICT service provider, which shall clearly define all relevant terms, conditions, rights, obligations and responsibilities of the contracting parties. The contract shall also include service level agreements and shall be available in physical or electronic form, in accordance with relevant and applicable regulations.

(2) The bank shall ensure compliance of the contracts referred to in Paragraph 1 of this Article with Article 9, Paragraph 3 of the Decision on Outsourcing Management.

(3) Contracts for the use of ICT services, in addition to the conditions referred to in Paragraph 2 of this Article, should also include the following:

1) the provisions on availability, authenticity, integrity and confidentiality in relation to data protection, including personal data,
2) the provisions on ensuring access to personal and other bank data, and on ensuring their recovery and return in an easily accessible format in the event of insolvency, resolution or termination of business activities of the ICT service provider or in the event of contract termination,
3) the obligation of the ICT service provider to provide assistance to the bank at no additional cost or at a pre-determined cost in the event of an ICT incident related to the ICT service it provides to the bank,
4) conditions for the participation of the ICT service provider in ICT security awareness programs and digital operational resilience training conducted by the bank, in accordance with Article 21 of this Decision,
5) specifications of the bank's data life cycle and
6) procedures for incident resolution, including escalation and reporting procedures.

(4) Contracts for the use of ICT services that support critical functions and core business activities should be in accordance with Article 9, Paragraph 4 of the Decision on Outsourcing Management and Paragraph 3 of this Article, and include the following:

1) deadlines for prior notices and reporting obligations of the ICT service provider to the bank, including notification on any change that could have a significant impact on the ICT service provider's ability to effectively provide ICT services that support critical functions or core business activities in accordance with the agreed service levels,
2) requirements that the ICT service provider establish measures, tools and policies for the security of ICT systems and that provide an adequate level of security for the provision of services to the bank in accordance with its regulatory framework, including requirements for data encryption, network security and security monitoring procedures,
3) the obligation of the ICT service provider to participate in the bank's TLPT, in accordance with Article 38 of this Decision, and its full cooperation,
4) the right to continuous monitoring of the work of the ICT service provider, which includes the following:
    1. the provisions defined in Article 9, Paragraph 4, Item 1) of the Decision on Outsourcing Management, including the right to take copies of relevant documentation on site if they are essential for the work of the ICT service provider, where the effective exercise of these rights may not be prevented or restricted by other contracts or policies,
    2. the right to contract alternative levels of insurance if the rights of other clients are included,
    3. the obligation of the ICT service provider to cooperate fully during on-site inspections and audits conducted by the Agency, the bank, including third parties appointed by them and
    4. the obligation to provide details of the scope, procedures to be followed and frequency of such inspections and audits,
5) exit strategies, in particular the definition of a mandatory transition period:
    1. during which the ICT service provider will continue to provide the subject activities or ICT services to the bank in order to reduce the risk of disruption to the bank's operations or to ensure its effective recovery and resolution and

2. in which the bank may choose another ICT service provider or return the relevant activity to the bank, in accordance with the complexity of the service that is the subject of the contract.

VI MANAGING ICT OPERATIONS

Article 28

(1) The bank shall manage its ICT operations based on documented, adopted and implemented processes and procedures. These documents shall define how the bank uses, monitors and controls its ICT systems and services.

(2) The bank shall ensure that the performance of ICT operations is in accordance with the requirements of the bank's business operations, including information security requirements.

(3) The bank shall maintain and improve the efficiency of its ICT operations, including, but not limited to, the need to consider ways to reduce potential errors arising during the performance of manual tasks.

(4) The bank shall record, monitor and keep records of critical ICT operations to enable the detection, analysis and correction of errors.

(5) The bank shall establish a process for managing ICT assets, at all stages of their life cycle – from acquisition or development to withdrawal from use, taking into account the risks, in particular those arising from the use of outdated or unsupported ICT assets and systems, including ICT assets of service providers.

(6) The bank shall conduct planning procedures and performance and capacity monitoring in order to timely prevent, detect and respond to significant problems in the operation of the ICT system and deficiencies in the capacity of the ICT system.

Article 29

(1) The bank shall be obliged to establish a project management process that defines the roles and responsibilities necessary for effective support for the implementation of the ICT system strategy.

(2) The bank shall appropriately monitor and mitigate risks arising from ICT projects, taking into account risks that may arise from the interdependence of different projects and the dependence of multiple projects on the same resources and/or expertise. The bank shall include project risk in the framework of ICT risk management.

(3) Through the project management methodology, the bank shall ensure that information security requirements are analyzed and approved by the information security management function.

(4) The bank shall ensure that project team members have the appropriate knowledge for the secure and successful implementation of the project in all areas affected by the ICT project.

(5) Depending on the importance and size of the ICT project, and the impact on critical functions and core business activities, the bank shall regularly, and additionally as necessary, report to the bank's management on the establishment and progress of the ICT project, and the associated risks.

Article 30

(1) The bank shall define and implement procedures that stipulate the manner of procurement, development and maintenance of ICT systems.

(2) The bank shall ensure that, prior to any procurement or development of ICT systems, functional and non-functional requirements, including requirements regarding information security, are clearly defined and approved at the appropriate management level.

(3) The bank shall ensure that measures are in place to reduce the risk of unintentional changes or intentional manipulation of ICT systems during development and introduction into the production environment.

(4) The bank shall establish procedures for testing and accepting ICT systems and services before their first use or significant change.

(5) The bank shall:

1) establish separate ICT environments to ensure adequate segregation of duties and mitigate the effect of uncontrolled changes in production environments,
2) separate production environments from development, test and other non-production environments,
3) protect the integrity and confidentiality of production data in non-production environments, and limit access to production data to authorized users, and
4) protect the integrity of the source code of internally developed ICT systems.

(6) The bank shall document in detail the development, implementation, functioning and configuration of the ICT system. The documentation shall contain at least user and technical documentation of the ICT system, as well as operational procedures.

(7) In accordance with the risk assessment, the bank shall apply the procedures for the procurement and development of ICT systems and to those ICT systems developed or managed by end users in business functions outside the ICT organization. The bank shall maintain a register of such systems that support critical business functions or processes.

Article 31

(1) The bank is obliged to establish a process for managing changes in the ICT system, in order to avoid them leading to unexpected and unwanted behavior of the ICT system, or violating its security or functionality.

(2) The bank should ensure that all changes referred to in Paragraph 1 of this Article are recorded, assessed, approved, implemented, tested and verified in a controlled manner. This includes at least:

1) initiation, analysis, risk assessment and approval of change requests, and the method of determining priorities and implementation,
2) testing, approval and documentation before implementing changes in production,
3) implementation plan, which includes a plan to return to the previous state,
4) separation of duties related to the development and implementation of changes and
5) informing users of the information system about the details of the changes made.

(3) The bank shall be obliged to establish procedures for managing so-called urgent changes (i.e. changes that must be implemented as soon as possible) which include procedures that ensure appropriate protection measures.

(4) The bank shall be obliged to establish the initial versions of the software components of the ICT system, and record and chronologically document all changes to these components and the database architecture.

(5) The bank shall be obliged to establish procedures for managing security and functional patches, which will define how information on security patches is monitored, the longest period in which these patches must be applied depending on the criticality and risk assessment for the bank, and the method of their application.

VII MANAGING ICT INCIDENTS

Article 32

(1) The bank shall be obliged to define, establish and implement an ICT incident management process for the purpose of timely detection, management and notification of ICT incidents.

(2) The bank shall be obliged to, within the framework of the ICT incident management process referred to in Paragraph 1 of this Article:

1) establish early warning indicators,
2) establish procedures for identifying, monitoring, recording, categorizing and classifying ICT incidents according to their priority and severity, as well as the criticality of the affected services, in accordance with the criteria set out in Article 33 of this Decision,
3) assign roles and responsibilities for managing different types of ICT incidents (e.g. errors, malfunctions, cyberattacks, etc.) and scenarios,
4) establish communication plans with employees, external stakeholders and the media in accordance with Article 20 of this Decision, as well as plans for informing clients, procedures related to internal escalation, which includes user complaints related to ICT and, where necessary, informing other financial sector entities,
5) ensure that at least significant ICT incidents are reported to relevant senior management, and inform the management bodies about these incidents, explaining their impact, the response to incident and additional controls that need to be implemented due to such incidents,
6) establish ICT incident response procedures to mitigate their impact and ensure that the bank's services become available and secure in a timely manner,
7) establish appropriate procedures and activities to ensure consistent and integrated monitoring of ICT incidents, and actions and follow-up measures to ensure that their root causes are identified and documented and that such incidents are prevented from recurring, and update ICT system security measures in accordance with the knowledge gained.

(3) establish appropriate procedures and activities to ensure consistency and the bank shall be obliged to record all ICT incidents and significant cyber threats.

(4) As part of the incident response procedure referred to in Paragraph 2, Item 7) of this Article, the bank shall be obliged to implement procedures for adequate evidence management, whenever possible, taking into account the following:
1) maintain a chain of custody,
2) consider possible legal consequences when initiating a digital forensic investigation,
3) ensure that critical aspects of evidence preservation are not overlooked, and
4) ensure that the collected evidence is admissible before the competent court.

Article 33

(1) The bank shall be obliged to classify ICT incidents and determine their impact based on the following criteria:
1) the number and/or relevance of the clients or third parties involved and, if applicable, the amount or number of transactions involved in the ICT incident, as well as the fact whether the ICT incident had an impact on the bank's reputation;
2) the duration of the ICT incident, including the time of service interruption,
3) the geographical spread in relation to the areas involved in the ICT incident;
4) the loss of data caused by the ICT incident, in relation to the availability, authenticity, integrity or confidentiality of the data;
5) the criticality of the services involved, including the bank's transactions and operations, and
6) the economic impact of the ICT incident, in particular direct and indirect costs and losses in absolute and relative terms.

(2) The bank shall be obliged to classify a cyber threat as significant based on the criticality of the service which is exposed to risk, including the bank's transactions and operations, the number and/or relevance of affected clients or third parties, as well as the geographical spread of the area which is exposed to risk.

Article 34

(1) The bank shall, upon becoming aware of a significant ICT incident, immediately notify the Agency in accordance with Paragraph 6 of this Article.

(2) For the purposes of Paragraph 1 of this Article, the bank shall, after collecting and analyzing all relevant information, prepare the initial notification and reports referred to in Paragraph 6 of this Article.

(3) The initial notification and reports referred to in Paragraph 6 of this Article shall contain all information necessary for the Agency to determine the severity of the significant ICT incident and its impact on the financial sector.

(4) The bank shall, upon becoming aware of a significant cyber threat, immediately notify the Agency if it considers that the threat is relevant to the financial sector, service users or clients.

(5) In the event of a significant ICT incident that has an impact on the financial interests of clients, the bank shall, without undue delay, as soon as it becomes aware of the incident, inform its clients of that significant ICT incident and of the measures undertaken to mitigate the negative consequences of such incident. In the case of a significant cyber threat, the bank shall, if applicable, inform its clients, who are potentially affected, in a timely manner of all appropriate protection measures that they may consider.

(6) The bank shall be obliged to submit the following to the Agency:

1) initial notification,

2) an interim report, following the initial notification referred to in Item 1) of this Paragraph, as soon as the status of the original incident changes significantly or the handling of the significant ICT incident changes based on new available information, and thereafter, as necessary, updated notifications whenever relevant status updates occur, as well as at the express request of the Agency, and

3) a final report, when the analysis of the root cause of the ICT incident is completed, regardless of whether mitigation measures have already been implemented and when the estimated impact values can be replaced by actual data on the impact of the ICT incident.

(7) After receiving the notification, the Agency shall, as necessary, undertake all necessary measures to protect the stability of the banking system.

VIII TESTING DIGITAL OPERATIONAL RESILIENCE

Article 35

(1) For the purpose of assessing readiness to deal with ICT incidents, identifying weaknesses, deficiencies and deviations in digital operational resilience, the bank shall be obliged to define, implement and regularly update a digital operational resilience testing program, as an integral part of the ICT risk management framework.

(2) The digital resilience testing program referred to in Paragraph 1 of this Article includes various assessments, tests, methodologies, procedures and tools that are applied in accordance with Articles 37 and 38 of this Decision.

(3) When implementing the digital resilience testing program referred to in Paragraph 1 of this Article, banks shall apply a risk-based approach, taking into account the development of ICT risks, the specific risks to which the bank is or could be exposed, the criticality of the information assets and services it provides, as well as all other factors that the bank considers relevant.

(4) The bank shall establish procedures for prioritizing, classifying and addressing all weaknesses and deficiencies identified by performing the tests referred to in Paragraph 2 of this Article, and shall establish internal verification methodologies to ensure that all identified weaknesses and deficiencies have been fully addressed.

(5) The bank shall ensure that appropriate tests are carried out regularly, performing the following:

1) at least once a year for all ICT systems and applications that support critical functions and core business activities,
2) for other ICT systems and applications, in accordance with the risk assessment, at least once every three years,
3) before any changes to existing or addition of new applications and infrastructure components of systems and ICT services, which support critical functions and core business activities, including applications accessible via internet.

Article 36

The digital resilience testing program referred to in Article 35 of this Decision should include the performance of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, deviation analyses, physical security checks, questionnaires and software solutions for scanning, source code reviews if applicable, scenario-based testing, compatibility testing, performance testing, end-to-end testing and penetration testing. Scenario-based testing should also include scenarios of relevant and known potential attacks, based on identified security threats.

Article 37

(1) Banks, which are determined in accordance with Article 38, Paragraph 2, are required to conduct advanced TLPT (threat-led penetration testing) at least once every 3 years. Taking into account the bank's risk profile and operational circumstances, the Agency may, when necessary, require the bank to reduce or increase this frequency.

(2) Each penetration test referred to in Paragraph 1 of this Article should cover several critical functions of the bank and core business activities or all such functions and activities and be conducted on production systems that support those functions and activities.

(3) The bank shall be required to identify all relevant ICT systems, processes and technologies that support critical functions and core business activities, as well as ICT services, including those that are outsourced or contracted with ICT service providers.

(4) The bank shall assess which critical functions and core business activities must be covered by the TLPT and submit the assessment results to the Agency.

(5) If ICT service providers are covered by the TLPT, the bank shall undertake the necessary measures to ensure the participation of these service providers in the TLPT, including safeguards. The bank shall remain fully responsible for compliance with the provisions of this Decision at all times.

(6) Without prejudice to Paragraphs 2 and 3 of this Article, if it can be reasonably expected that the participation of the ICT service provider referred to in Paragraph 5 of this Article will negatively affect the quality or security of the services provided by that ICT service provider to other users to which this Decision does not apply or the confidentiality of data related to such services, the bank and the ICT service provider may agree in writing that the ICT service provider directly engages a third party to conduct a joint TLPT involving several banks (joint testing), under the leadership of one specific bank, to which it provides ICT services, and in compliance with the provisions of this Decision.

(7) The joint testing referred to in Paragraph 6 of this Article shall cover the relevant scope of ICT services supporting critical functions and core business activities contracted by the banks with the ICT service provider. The number of banks participating in this testing should be proportionate to the complexity and type of services covered.

(8) The bank shall, in cooperation with ICT service providers and other involved parties, including third parties conducting the testing, but not the Agency, implement effective risk management controls to mitigate the risks of potential impact on data, damage to property and disruption of critical functions and core business activities, services or operations within the bank itself, its partners or the financial sector.

(9) At the end of the testing, after the reports and corrective action plans have been completed, the bank shall submit to the Agency a summary of relevant findings, corrective action plans and other documentation confirming that the TLPT was conducted in accordance with the provisions of this Decision.

(10) Competent authorities shall issue to banks a certificate that the test has been conducted in accordance with the requirements, as specified in the documentation, in order to enable the competent authorities to mutually recognize the TLPT. If a bank participates in a joint test led by a bank not supervised by the Agency, it shall provide the Agency with a certificate, a summary of the relevant findings and plans for corrective measures. Notwithstanding this certificate, the bank shall remain fully responsible for the impact and consequences that may arise during the testing.

Article 38

(1) The bank shall engage the testers for the implementation of the TLPT in accordance with Article 39 of this Decision. If the bank has engaged internal resources for the purposes of implementing the TLPT, it shall engage external testers for every third test.

(2) The Agency shall determine which banks are required to conduct TLPT, taking into account the principle of proportionality, and taking into account the following:
   1) factors affecting the financial sector, with particular reference to the extent to which the services and activities provided by the bank affect the financial sector as a whole,
   2) the potential impact on the stability of the financial sector, including the systemic importance of the bank,
   3) the specific ICT risk profile, the level of ICT maturity of the bank or the characteristics of the technologies used.

Article 39

(1) For the implementation of the TLPT, the bank shall be obliged to engage only testers which:
   1) are of high standing and reputation,
   2) possess technical and organizational capabilities, expertise in the field of collecting and analyzing cyber threats, conducting penetration testing and red team testing,
   3) possess internationally recognized certificates/accreditations for conducting penetration testing, and adhere to formal codes of conduct or ethical norms,
   4) provide independent assurance or an audit report regarding the quality of risk management associated with the implementation of the TLPT, including appropriate protection of the bank's confidential information and legal protection with regard to the risks to which the bank is exposed in its operations,
   5) are adequately and fully covered by relevant liability insurance, including risks of inappropriate and negligent conduct.

(2) If a bank conducts testing internally, it shall, in addition to the conditions referred to in Paragraph 1 of this Article, also meet the following conditions:
   1) the engagement of the persons conducting the testing has been approved by the Agency,
   2) the Agency has confirmed that the bank has adequate resources and that there is no conflict of interest in the planning and conduct of the testing, and
   3) the bank uses external sources of threat information.

(3) The bank shall ensure that the contract with the third party conducting the testing covers adequate management of the results of the TLPT, and that any data processing in connection therewith, including generation, storage, processing, reporting, transmission or destruction, does not create risks for the bank.

IX MANAGING BUSINESS CONTINUITY

Article 40

(1) The bank shall establish a business continuity management process in order to ensure, to the greatest extent possible, the continuous provision of services and limit losses in the event of serious disruptions to business operations. The provisions of the Decision on the management system in banks shall apply to the business continuity management process, unless otherwise stipulated by this Decision

(2) As part of the ICT risk management framework, the bank shall adopt a business continuity plan in the ICT area (hereinafter: ICT Continuity Plan), which may be adopted as a separate document and shall form an integral part of the bank's business continuity plan.

Article 41

(1) The bank shall regularly conduct a business impact analysis (BIA) in view of its exposure to more serious business disruptions and shall include an assessment of the potential impact of such disruptions on confidentiality, integrity and availability, using quantitative and qualitative criteria, using internal and/or external data, as well as scenario analysis.

(2) The business impact analysis should be conducted taking into account the criticality of the identified and mapped business functions, supporting processes, third-party dependencies and information assets, as well as their interdependencies, in accordance with Article 15 of this Decision.

(3) As part of the business impact analysis, it is necessary to at least:

1) list the critical functions and core business activities, as well as the processes that support them, in accordance with Article 15, Paragraph 1 of this Decision
2) list the ICT assets required for the performance of individual business processes, as well as their interdependencies and connections, in accordance with Article 15, Paragraph 3 of this Decision,
3) determine, as a minimum, the RTO, RPO and SDO for each individual business activity, taking into account outsourcing and third-party dependencies.

(4) The bank shall ensure that its ICT systems and ICT services are established and aligned with the business impact analysis, in particular with regard to the redundancy of critical and key ICT components in order to prevent disruptions caused by events affecting those components.

Article 42

(1) Based on the business impact analysis, the bank is required to adopt an ICT Continuity Plan in order to ensure the re-establishment of its critical functions and core business activities after the interruption within the required Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the event of a serious business interruption or emergency.

(2) The plan referred to in Paragraph 1 of this Article, as well as other dedicated plans, procedures and mechanisms relevant to the business continuity process, aim to:

1) ensure the continuity of critical functions and core business activities of the bank in accordance with the defined parameters for RTO and RPO,
2) respond promptly, adequately and effectively to all ICT incidents and their resolution, in a manner that limits damage and prioritizes business continuity and recovery measures,
3) activate, without delay, dedicated plans that enable measures, processes and technologies to contain the spread and that are adapted to each type of ICT incident and prevent further damage, as well as adapted response and recovery procedures defined in accordance with Article 43 of this Decision,
4) assess the preliminary impact, damage and losses,
5) determine communication measures, as well as measures for crisis management in order to ensure that all relevant parties (employees, management bodies, external stakeholders, service providers) are informed in a timely and adequate manner, and in accordance with Article 20 of this Decision, including reporting to the Agency in accordance with Article 43 of this Decision.

(3) The bank's ICT Continuity Plan shall support the objectives of protecting, and if necessary, restoring, the confidentiality, integrity and availability of business processes, supporting processes and information assets.

(4) Within the framework of the ICT Continuity Plan, the bank shall consider a number of different scenarios to which it could be exposed, including extreme but possible scenarios, and assess their potential impact. Based on these scenarios, the bank shall describe how it will ensure the continuity of ICT systems and services, as well as the information security of the bank.

(5) As part of the process of managing the business continuity plan in the ICT area, the bank shall be obliged to:

1) determine the methodology for assessing damage and define coefficients for the maximum allowed downtime of critical business processes, as well as to determine individual values for RPO, RTO and SDO,
2) determine the priorities for recovering business processes,
3) determine a backup location for recovering critical business processes where data will be protected, which should be at an appropriate geographical distance from the primary location, in order to reduce the risk of both locations being simultaneously exposed to the same risk,
4) identify alternative mechanisms for the continuity of business processes in the event of an interruption of the primary mechanisms,
5) identify the method of protection and recovery of data required for the continuation of the business process at the backup location,
6) take into account physical measures for the protection of critical bank's infrastructure at primary and backup locations and ensure appropriate conditions for their uninterrupted and secure functioning and
7) take into account the roles and responsibilities of persons responsible for ICT infrastructure in the context of using services from third parties, through appropriate plans and activities to ensure business continuity and digital resilience.

Article 43

(1) Based on the business impact analysis referred to in Article 41 of this Decision and the ICT Continuity Plan referred to in Article 42 of this Decision, the bank shall adopt ICT system response and recovery plans, which will enable the recovery and availability of ICT systems and services necessary for the operation of critical functions and core business activities within the required recovery time objective and recovery point objective.

(2) ICT system response and recovery plans shall define the conditions for activating the plans, as well as the measures that need to be undertaken to ensure the availability, continuity and recovery of at least critical and key ICT systems and services. These plans should be directed towards achieving the bank's business recovery objectives.

(3) The bank shall update the ICT Continuity Plan and the ICT system response and recovery plans at least once a year, based on the results of testing, knowledge of current threats, as well as experience gained from previous events, and the findings of audit and supervisory reviews, and necessarily when changing recovery objectives, business functions, supporting processes or information assets.

(4) In the event of activating the ICT Continuity Plan or the ICT system response and recovery plans, including significant ICT incidents, the bank shall keep records of activities before and after the disruption, which must be easily accessible. In doing so, it shall notify the Agency immediately upon learning of all relevant facts and circumstances relating to this.

Article 44

(1) As part of the ICT risk management framework, the bank shall:

1) regularly test the ICT Continuity Plan, and the ICT system response and recovery plans which support all functions, at least once a year, as well as in the event of significant changes in the ICT systems supporting critical functions and core business activities, and
2) test the crisis communication plans.

(2) As part of the response and recovery plans, the bank shall establish and implement measures to ensure the continuity of business of key ICT services contracted with ICT service providers.

(3) As part of the testing referred to in Paragraph 1, Item 1) of this Article, the bank shall obligatorily include scenarios of cyber-attacks and switching from the primary ICT infrastructure to redundant capacities, backup copies and the location of the backup computer center.

(4) The bank shall be obliged to:

1) document the results of the testing,
2) analyze and eliminate all identified deficiencies observed during the testing, and inform the bank's management bodies, and
3) regularly review the ICT Continuity Plan and the ICT system response and recovery plans, taking into account the results of the testing referred to in Paragraph 1, Item 1) of this Article, as well as the findings of audit and supervisory reviews.

Article 45

(1) The bank shall be obliged to establish a backup computer center that:
1) is at an appropriate geographical distance from the location of the primary data center, in order to ensure that the primary and backup data centers are not simultaneously exposed to the same risks,
2) ensures the continuity of critical functions or core business activities in the same way as the primary data center or provides the level of services required to ensure the continuity of critical functions and core business activities within the defined objective values (RTO, RPO and SDO) and
3) is accessible to bank employees in order to ensure the continuity of critical functions and core business activities in the event of unavailability of ICT resources at the primary location.

(2) The effective functionality of the backup computer center must be confirmed at least once a year, and necessarily after significant changes in the bank's ICT system. The bank shall be obliged to notify the Agency at least 30 days before testing the functionality of the backup computer center.

(3) The bank shall be obliged to document the results of the testing referred to in Paragraph 2 of this Article, and ensure that the report on the test results is adopted by the bank's management.

Article 46

(1) If a bank has outsourced ICT systems and services that support the performance of critical functions and core business activities outside the bank's headquarters, for these ICT systems and services it shall be obliged to:
1) determine appropriate RTO, RPO and SDO parameters in order to ensure an adequate level of services and compliance with legal regulations,
2) define an ICT Continuity Plan and response and recovery plans at the bank's headquarters,
3) provide in the local computer center at the bank's headquarters the ICT resources which are necessary for their required recovery time, taking into account the training of bank employees for the recovery of these systems, as well as the up-to-dateness of data in accordance with the defined RPO from Item 1) of this Paragraph, including systems for generating reports in accordance with this Paragraph.

(2) The bank shall be obliged to test the functionalities at the bank's headquarters in accordance with the provisions of Article 45.

Article 47

(1) The bank shall establish a backup management process to ensure the recovery of ICT systems and data within the required recovery time and the availability of data, which includes:
1) procedures and activities for creating data backup copies, which determine the volume of data for which they are created, and the minimum frequency of creation in accordance with the risk assessment, the results of the business impact analysis and the criticality of ICT systems and data, and
2) procedures and methods for restoring and recovering data.

(2) The bank shall implement data backup systems that can be activated in accordance with the procedures and activities for data backup, and the procedures and methods for data restoration and recovery. The activation of the data backup system shall not compromise the security of the ICT system, nor the availability, authenticity, integrity or confidentiality of data. The bank shall periodically test the backup procedures, as well as the procedures and methods for data restoration and recovery.

(3) ICT systems used for data restoration and recovery must be physically and logically separated from the original ICT systems and protected from unauthorized access or damage in the ICT system area.

(4) The bank shall be obliged to ensure that backup copies of data are stored in one or more secondary locations, at least one of which must be sufficiently distant from the primary location where the original data is located, so that they are not exposed to the same risks. Backup copies of data must be up-to-date and adequately protected from relevant risks (cyber attacks, risks during transmission, etc.).

Article 48

(1) The bank shall be obliged to provide protective (regulatory) copies of data:
   1) containing the minimum set of data necessary for the provision of critical functions and the performance of core business activities, as well as the implementation of the bank resolution procedure by the Agency,
   2) in an easily accessible format, which enables data portability, regardless of the source systems in which the data were created, using tools that are widely available on the market, with documentation specifying how the data can be accessed,
   3) up-to-date in accordance with the regulatory requirements of the Agency and
   4) available at the bank's headquarters.

X MANAGING RELATIONS WITH PAYMENT SERVICE USERS

Article 49

(1) The bank shall establish and implement processes to raise awareness of payment service users about security risks associated with payment services, which shall include the provision of assistance and guidance to payment service users.

(2) Assistance and guidance offered to payment service users shall be regularly updated in light of new threats and vulnerabilities, and payment service users shall be informed of these changes in a timely manner.

(3) The bank shall allow payment service users to disable certain payment functionalities related to the payment services provided by the bank to the payment service user, if such an option exists within the functionality of the product.

(4) If the bank agrees with the user regarding spending limits for payment transactions carried out through certain payment instruments, the bank shall provide the user with the option to adjust these limits up to the amount of the highest agreed limit.

(5) The bank shall enable payment service users to receive alerts about the initiation and/or failed attempts to initiate payment transactions, in order to be able to detect fraudulent or malicious use of their accounts in a timely manner.

(6) The bank shall inform payment service users about changes in security procedures that affect payment service users in relation to the provision of payment services.

(7) The bank shall communicate with its payment service users in such a way as to assure them of the authenticity of the messages received.

(8) The bank shall provide payment service users with assistance in relation to all questions, support requests and notifications of irregularities or problems with regard to security issues related to payment services. Payment service users should be adequately informed about how to obtain such assistance.

XI EXCHANGE OF INFORMATION

Article 50

(1) Banks shall exchange information and knowledge on cyber threats with the Agency, including indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. The Agency shall exchange information and knowledge with banks to the extent that such exchange of information and knowledge aims to: improve the digital operational resilience of banks, in particular by raising awareness of cyber threats, limiting or preventing the possibility of the spread of cyber threats, strengthening defensive capacities and threat detection techniques, mitigation or response and recovery strategies.

(2) For the purposes of Paragraph 1 of this Article, the Agency shall establish an information exchange protocol and provide a platform for information exchange.

(3) The protocol on the exchange of information referred to in Paragraph 1 shall define at least the following: participants and their roles, frequency and method of exchange, scope of information, measures for the protection of potentially sensitive information that fully respect professional secrets and the protection of personal data, conditions for the involvement of other stakeholders.

XII REPORTING AND NOTIFICATION TO THE AGENCY

Article 51

(1) The bank shall submit the following internal documents and reports to the Agency:
   1) ICT system strategy and operational plans defined in Article 5 of this Decision,
   2) information security policy,
   3) policies related to ICT risk management, defined in Article 14 of this Decision,
   4) policies related to ICT incident management, defined in Article 32 of this Decision,
   5) digital operational resilience testing program, defined in Article 35 of this Decision,
   6) policies related to the use of third-party ICT services, defined in Article 22 of this Decision,
   7) business impact analysis, ICT Continuity Plan and ICT system response and recovery plans, defined in Articles 41, 42 and 43 of this Decision,
   8) program on raising awareness about information security, defined in Article 21 of this Decision,
   9) information register defined in Article 23 of this Decision,
   10) report on the number of new contracts for the use of ICT services, categories of ICT service providers and type of contract,
   11) report on the results of the ICT risk assessment, defined in Article 16 of this Decision, including the corrective action plan,
   12) reports on the management of ICT risks and the implementation of corrective action, as well as a report on the level of digital operational resilience,
   13) reports on the implementation of the operational plan referred to in Item 1) of this Paragraph,
   14) reports on the conducted tests of digital operational resilience defined in Article 35 of this Decision,
   15) reports on the testing of plans defined in Articles 44-46 of this Decision.

(2) The bank shall submit the internal acts referred to in Paragraph 1, Items 1) – 8) annually, no later than 90 days after the end of the calendar year, and that were adopted or updated during the reporting period.

(3) The bank shall submit the reports referred to in Paragraph 1, items 9) – 15) 15 days after their adoption by the management body.

(4) The bank shall be obliged to notify the Agency in a timely manner of any significant and complex change that may have an impact on the bank's ICT system and to submit appropriate documentation (detailed description of the change, activity plan, project teams, planned budget, results of the ICT risk

assessment, etc.), including changes in key personnel (head of the organizational unit for ICT management, person responsible for information security, chief administrators, etc.).

(5) A bank that plans to migrate data to a new bank's core business application system or to another computer center, or that changes the location of the computer center, and has previously notified the Agency in accordance with Paragraph 4, shall notify the Agency thereof no later than 30 days before the start of the planned testing.

The notification referred to in this Paragraph shall contain at least:

1) detailed descriptions of the systems between which data is transferred;
2) a plan, dynamics and description of activities related to data migration, including the testing methodology;
3) the results of the risk assessment and a description of the controls that will be applied during data migration with the aim of preserving the confidentiality, integrity and availability of data;
4) a plan for restoring the state before the data migration, which includes the dynamics of such restoration and a description of activities, as well as the criteria for making a decision to apply this plan.

XIII DISCLOSURE OF INFORMATION SIGNIFICANT TO THE PUBLIC

Article 52

The Agency may publish information, including measures, that it deems to be of public importance, relating to the management of ICT systems, the security of ICT systems, cyber risks, as well as other specific areas related to the use of ICT.

XIV TRANSITIONAL AND FINAL PROVISIONS

Additional instructions on the implementation of the Decision

Article 53

The Agency shall stipulate in more detail the requirements for the purpose of implementing the provisions of this Decision through special instructions.

Transitional and final provisions

Article 54

(1) This Decision shall enter into force on the eighth day from the date of its publication in the "Official Gazette of Republika Srpska", and shall be applied from April 1, 2026.

(2) On the date of the commencement of the application of this Decision, the Decision on the management of information systems in banks ("Official Gazette of Republika Srpska", No. 116/17) shall cease to be valid.

(3) The bank shall be obliged to bring the contracts on the use of ICT services concluded with ICT service providers before the entry into force of this Decision into line with the provisions of this Decision, no later than 3 months from the date of application of this Decision.

Number: UO-159/25

Date: May 13, 2025

PRESIDENT OF THE
MANAGEMENT BOARD

Dejan Kusturić