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 114 of the Banking Law of Republika Srpska ("Official Gazette of Republika Srpska", No. 4/17, 19/18 and 54/19), Article 6, Paragraph 1, Item b and Article 19, 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 27th session, held on 29 October, 2020 adopted the

DECISION
ON OUTSOURCING MANAGEMENT

Subject
Article 1

(1) This Decision stipulates the minimum standards that a bank is obliged to provide in the process of conducting outsourcing, managing outsourcing, and outsourcing risk.

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

(3) The bank is obliged to apply the provisions of this Decision on individual and consolidated basis.

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

Definitions
Article 2

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

1) **Outsourcing** is the contractual entrustment of the bank's activities to service providers, that would otherwise be undertaken by the bank itself.
2) In the context of this Decision, outsourcing shall not mean:
    1. activities which, under the law, are performed by a service provider (e.g. external audit),
    2. services of interbank communication services (SWIFT) in case the key resources of the information system are located within the bank,
    3. interbank communication and trading services (Reuters, Bloomberg, etc.),
    4. use of market information services by ECAI (Moody's, Standard & Poor's, Fitch, etc.),
    5. global network infrastructure services (Visa, MasterCard, etc.),

6. correspondent banking services,
7. settlement systems and clearing services,
8. rent, lease and goods procurement (e.g. plastic cards, card readers, office supplies, computers, furniture, etc.), and
9. other activities that the bank does not otherwise perform itself (e.g. architectural services, cleaning services, facility maintenance services, service maintenance of official cars, catering services, utilities, travel services, postal services, providing legal opinions and representation in court and before the administration authorities, medical services, etc.).

3) **Activities that the bank would otherwise perform itself** are activities that enable the bank to perform the activities of providing banking and / or financial services, including activities that support the performance of those activities.
4) **Outsourcing risk** is a common name for all risks that arise when the bank contractually entrusts service providers to perform activities that it would otherwise perform itself.
5) **Critical functions** - in accordance with Article 2, Paragraph 1, Item 34 of the Banking Law of Republika Srpska (hereinafter: the Banking Law), are activities, services or operations whose interruption would likely jeopardize the stability of the financial sector or disturbances in the provision of necessary services to the real sector due to the size and market share of the entity performing them and its connections with other participants in the financial sector, and especially taking into account the possibility for someone else to take over performing these activities, services or operations without hindrance.
6) **Key functions in the bank** - in accordance with Article 76 of the Banking Law, are control functions and other functions in the bank that have a significant impact on the management and operations of the bank.
7) **Control functions** - in accordance with Article 92 of the Banking Law, are: risk management function, compliance monitoring function and internal audit function.
8) **Core business lines** - in accordance with Article 2, Paragraph 1, Item 35 of the Banking Law, are business activities and services related to these activities whose performance generates a significant part of income or profit for the bank or the banking group to which the bank belongs.
9) **Service provider** is a third party that performs a certain outsources activity in part or in full, based on a contract concluded with the bank.
   The service provider may be:
   1. a banking group member,
   2. a legal entity which, according to the regulations of the country in which it was established, or in which it is headquartered, is authorized to perform the activity subject of outsourcing, or
   3. a private individual who, according to the regulations of the country in which he/she resides, is authorized to perform the activity subject of outsourcing.
10) **Subcontractor** is a legal entity to which the service provider has entrusted the performance of part of the contract, i.e. specific tasks, which the service provider has contracted with the bank.

11) **Cloud** services are services provided using a cloud infrastructure, i.e. a model that provides ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, data storage, applications and services) that can be rapidly provisioned and released to customers with minimal management effort or interaction with service provider. We distinguish three types of services (infrastructure as a service - IaaS, platform as a service - PaaS, software as a service - SaaS) and four models of use (public, private, community and hybrid).
12) **Public cloud** means cloud infrastructure available for open use by the general public.
13) **Private cloud** means cloud infrastructure available for the exclusive use by a single entity.
14) **Community cloud** means cloud infrastructure available for the exclusive use by a specific number of entities.
15) **Hybrid cloud** means cloud infrastructure that is composed of two or more distinct cloud infrastructures (e.g. public and private).

(2) Definitions that are not defined by this Article, and are used in this Decision, have meaning in accordance with legal regulations and other bylaws.

Conditions for outsourcing
Article 3

(1) The bank may outsource activities that enable it to perform the activities of providing banking or financial services, including activities that support the performance of those activities, if the outsourcing does not violate:

1) performance of regular bank operations,
2) efficient management of bank risks,
3) bank internal control system and
4) the possibility of the Agency's supervision over outsourced materially significant activities.

(2) The bank may not outsource the activity of providing banking or financial services for which it has obtained a license and authorization from the Agency, in accordance with the applicable regulations.

(3) By means of agreements on outsourcing, the bank may not delegate or transfer the rights and obligations of the management body, which, among other things, relate to the establishment of risk management strategy, policy and procedures.

(4) The bank may not outsource key functions in the bank, including control functions.

(5) Notwithstanding Paragraph 4 of this Article, the bank may outsource internal audit activities related to certain specific segments of operations that require special expert knowledge (e.g. internal audit of information systems) with the following conditions:

1) that the bank entrusts the internal audit activity to a company authorized to perform internal audit or to a member of the same banking group,

2) when conducting internal audit, the provisions of the Banking Law and by-laws of the Agency regulating the area of internal audit in Republika Srpska shall be complied with,

3) that the persons performing internal audit possess professional knowledge and skills in the field that is the subject of internal audit (e.g. internationally recognized certificates for information system audit),

4) that the bank, if entrusting the internal audit of a certain segment of operations to an audit company, ensures that the same company cannot perform an external audit of that segment of operations of the bank in that year.

Materially significant activities

Article 4

(1) Materially significant activities are:

1) activities of such importance that any weakness or error in the provision of these activities may have a significant impact on the bank's ability to meet legal and regulatory requirements and / or continue its operations, i.e. the provision of banking services and activities,

2) activities that may have a significant impact on risk management and the financial result of the bank,

3) activities that enable the bank to perform core business lines and critical functions and

4) all activities related to the performance of the internal audit function, which may be outsourced in accordance with Article 3, Paragraph 5.

(2) When assessing whether the activity being outsourced is a materially significant bank, the following shall be taken into account:

1) Is the outsourcing agreement directly related to the provision of banking services and the performance of activities for which the bank has received an operating license;

2) Possible impact of any interruption of the outsourced activity or inability of the service provider to continuously and adequately perform the outsourced activities on:

1. short-term and long-term operations of the bank, including, if applicable, the impact on the financial result, capital and liquidity,

2. continuity of the bank's operations,

3. operational risk, including execution risk, information and communication technology risk (hereinafter: ICT) and legal risk,

4. reputational risk,

5. recovery and resolution plan, the possibility of resolution and the continuity of the bank's operations in the situation of early intervention, recovery or resolution;

3) Possible impact of the outsourcing agreement on the bank's ability to:

1. identify and monitor risks and manages them,

2. meet all legal and regulatory requirements,

3. conduct an audit of outsourced activities in accordance with Article 17 of this Decision;

4) Possible impact on the services provided by the bank to its clients;

5) All outsourcing agreements, the bank's total exposure to the same service provider and the possible cumulative effect of outsourcing agreements relating to the same segment of operations;

6) The size and complexity of the business area covered by outsourcing;

7) Possibility to adjust the proposed outsourcing agreement without replacing or revising the basic agreement;

8) The possibility of transferring, contractually and in practice, outsourcing agreements to other service providers if necessary, including assessed risks, barriers to business continuity, costs and timeframe within which to do so ("substitutability");

9) Circumstances that may lead to the activity that was not initially assessed as materially significant subsequently becoming materially significant;

10) Possibility to return the outsourced activity within the bank, if necessary;

11) Data protection and the possible impact of a breach of confidentiality or failure to ensure the availability and integrity of data on the bank and its clients.

(3) The bank may outsource materially significant activities to the following service providers:

1) members of a banking group or

2) any legal entity which, according to the regulations of the country in which it was established, or in which it is headquartered, is authorized to perform activities that are the subject of outsourcing.

Responsibilities of the supervisory board and the bank management

Article 5

(1) The supervisory board is obliged, as a minimum, to:

1) establish an adequate system for managing outsourcing and outsourcing risk, and all other risks related to outsourcing,

2) adopt adequate strategies, i.e. policies for outsourcing risk management, provide conditions for their implementation and supervise their implementation, taking into account the bank's business model and risk appetite,

3) ensure the bank's compliance with the law, this Decision and other regulations, strategy, i.e. policies,

4) identify potential conflicts of interest, assesses and manages it,

5) stipulate the content and periodicity of reporting to the supervisory board and other relevant committees, bodies or persons in connection with outsourced activities, at least once a year,

6) make a decision on materially significant outsourcing and

7) establish an effective system of internal control and ensure that the bank's control functions continuously monitor and verify whether the bank outsources activities in accordance with the law, this Decision, other regulations, strategy, policies, procedures and other internal acts of the bank.

(2) The bank management is obliged, as a minimum, to:

1) prepare and propose to the supervisory board strategies, i.e. policy for outsourcing risk management, and adopt other internal acts related to outsourcing,

2) at least once a year, analyze strategies and policies for outsourcing risk management, adapt them to changes in economic and market conditions and propose their adoption to the supervisory board,

3) establish and ensure the application of procedures for identification, measurement, i.e. assessment, monitoring, analysis and control of outsourcing risks and all other risks related to outsourcing,

4) provide monitoring of economic and market conditions in order to envisage possible changes, including the financial condition of the service provider,

5) ensure the implementation of an efficient system of internal control and the conditions for the bank's control functions to continuously monitor and evaluate policies, procedures and other internal acts and their implementation,

6) ensure confidentiality in terms of data protection and other information through contracts,

7) provide an uninterrupted flow of relevant information with the service provider,

8) timely ensure unhindered implementation of outsourced activities that are materially significant (e.g. when that activity is transferred to another service provider, when the bank takes over the said activity from the service provider, etc.) and

9) establish and implement an appropriate system of reporting to the bank management and the supervisory board on outsourced activities.

(3) The bank's management bodies retain full responsibility for the effective implementation of this Decision and the harmonization of the relevant outsourcing with all regulatory requirements and in the event of outsourcing of activities within the same banking group.

Standards for outsourcing risk management
Article 6

(1) The bank shall establish an effective system for managing outsourcing and outsourcing risk, proportionate to the type, scope and complexity of the bank's operations and the complexity of outsourced activities.

(2) The bank shall ensure that the members of the bank's management body have the skills and abilities that ensure adequate management of outsourced activities and supervision over them, and that outsourced activities are adequately covered by the bank's internal control system.

(3) The bank shall adopt and implement appropriate internal acts stipulating procedures related to outsourcing, which shall include, as a minimum, the following:

1) Clearly defined competencies and responsibilities in terms of making decisions on outsourcing and their changes, management of outsourcing and risk of outsourcing within the bank;

2) Procedures and activities carried out before concluding a contract with a service provider, including:

1. defining business requirements regarding outsourcing agreements,

2. criteria and procedures for determining materially significant activities,

3. the method of determining, assessing and mitigating the risks arising from outsourcing,

4. method of conducting in-depth analysis of potential service providers depending on the results of risk assessment,

5. procedures for identifying and assessing potential conflicts of interest, managing those conflicts and their reduction,

6. method of business continuity planning,

7. defining criteria for selection of service providers and

8. the procedure for approving new outsourcing agreements;

3) Method of implementation, monitoring and management of outsourcing agreements, including:

1. continuous assessment of the operations of service providers,

2. procedures for notifying the changes and actions of the bank in case of changes in the outsourcing agreements or circumstances related to the service provider (e.g. financial condition, organizational or ownership structure, relations with subcontractors, etc.),

3. independent verification of compliance with legal and regulatory requirements and internal acts of the bank by the function of compliance monitoring of operations and

4. agreement renewal procedures;

4) Method of documenting and keeping a register of outsourced activities;

5) Method of defining exit strategies and procedures for cancelation or termination of the contract;

6) Method of performing supervision over the activities that are the subject of the contract, i.e. obligations and responsibilities of the competent organizational unit, providing an adequate level of knowledge and experience of employees who perform supervision over outsourcing and its management, and

7) Method of reporting to the supervisory board and the bank management on outsourcing activities and risks.

(4) The bank should distinguish in its internal acts between:

1) outsourcing of materially significant activities and other outsourcing,

2) outsourcing within the group and outsourcing outside the group and

3) outsourcing to service providers in Bosnia and Herzegovina and outsourcing to service providers in other countries.

Register of outsourced activities

Article 7

(1) The bank is obliged to keep a detailed register of outsourced activities, which as a minimum should contain the following information:

1) number, name and date of signing the contract,

2) duration of the contract as well as the agreed notice period,

3) subject of outsourcing, description of outsourced activities, data to be outsourced and information on whether personal data is transferred,

4) assessment of outsourcing costs on an annual basis,

5) name of the service provider,

6) assessment of outsourcing costs on an annual basis,

7) name of the subcontractor in case of engagement,

8) a designation of material significance and a brief description of the reasons why the activity is considered materially significant,

9) name of the person, i.e. name of the organizational part of the bank responsible for outsourcing,

10) the country or countries where the service will be performed, the location of data storage and processing,

11) in the case of providing a cloud service, type of service, model of use, type of data and location of their storage,

12) date of the last assessment of the material significance of the activity.

(2) In the case of outsourcing materially significant activities, the register of outsourced activities, in addition to the specified in Paragraph 1 of this Article, should also contain:

1) a list of all banks or companies within the same group that use these outsourced services, if applicable,

2) information on whether the service provider or subcontractor is part of the group or is owned by one of the group members,

3) applicable law,

4) date of the last risk assessment related to the given outsourcing and review of the main conclusions,

5) date of the last and next planned audit, if applicable,

6) names of all subcontractors to whom the performance of parts of materially significant activities have been outsourced,

7) the result of the assessment of the substitutability of the service provider (easy, difficult, impossible), and the possibility for the bank to continue performing the outsourced materially significant activity or the impact of the interruption in the performance of the materially significant activity,

8) identification of alternative service providers in accordance with Item 7 of this Paragraph,

9) information on whether the outsourced materially significant activity supports business activities that are time-critical.

Analysis prior to outsourcing
Article 8

(1) Prior to making any decision on outsourcing, the bank shall:

1) Determine whether the planned business relation, i.e. the planned contract with the service provider corresponds to the definition of outsourcing. As part of this assessment, the bank should consider whether the service provider (or any part of it) the activity which is being outsourced to it performs regularly or continuously and whether that activity (or any part of it) is an activity that the bank would otherwise perform itself;

2) Assess whether the conditions for outsourcing referred to in Article 3 of this Decision are met;

3) Assess the complexity of outsourced services and their material significance in accordance with Article 4 of this Decision;

4) Identify and assess all risks arising from outsourcing, at least:

1. Identify and classify relevant activities and related data and systems with respect to their sensitivity and necessary protection measures;

2. Conduct a detailed analysis of activities and related data and systems covered by outsourcing, and consider possible risks, primarily operational, including legal, reputational, ICT risk and compliance risk. This assessment should include, as appropriate, scenarios of possible risk-related events, including high loss events. As part of the scenario analysis, the bank should assess the possible impact of interruptions in the provision of services or their inadequate provision, including risks arising from failed or inadequate processes, systems, staff failures or external events;

3. Consider the impact of concentration risks arising from outsourcing to a significant non-replaceable service provider and the number of outsourcing agreements entered into with the same service provider or related service providers, and the overall risks arising from the bank's outsourced activities;

4. Identify the risk that may arise from the need to provide financial support to a service provider facing difficulties or due to the need to take over its business activities;

5. Consider the impact of the location of the service provider (in BiH or outside BiH), possible restrictions on supervision related to the countries where outsourced services will be provided and data stored and processed, and consider the political stability and security situation of the countries concerned, as well as relevant regulatory framework;

6. Define and make a decision on the adequate level of data confidentiality protection, business continuity of service providers, and data and system integrity in the context of planned outsourcing. The bank should also consider specific measures related to the storage, use and transmission of data, including the possibility of using encryption technologies;

5) Conduct an appropriate analysis of potential service providers;

6) If the agreement on outsourcing materially significant activity involves the possibility for the service provider to hire a subcontractor, the bank should consider all associated risks, including additional risks that may arise if the subcontractor's location is in a country other than that of the service provider and

7) Identify and assess conflicts of interest that could arise from outsourcing and take appropriate measures to manage those conflicts of interest.

(2) In terms of materially significant activities, the bank should conduct an in-depth analysis of service providers, i.e. it should ensure that the service provider has a business reputation, appropriate skills, expertise, capacity, resources (e.g. human, ICT, financial), organizational structure, and is registered to perform materially significant activities. This also includes:

1) analysis of the business model, nature, size, complexity, financial condition and ownership structure of the service provider,

2) analysis of long-term relations with service providers that have already been assessed and provide services to the bank.

(3) If outsourcing involves the processing of personal or confidential data, the bank shall satisfy itself that the service provider implements the appropriate technical and organizational measures necessary for data protection.

(4) The bank should take appropriate steps to ensure that service providers comply with its values and code of conduct. In particular, when it comes to service providers in other countries and, if applicable, their subcontractors, the bank needs to make sure that the service provider operates in an ethically and socially responsible manner.

(5) The decision on outsourcing should be harmonized with the business strategy and objectives of the bank and should contain an explanation that includes a detailed description of the activities intended to be outsourced and the reasons for making the decision on outsourcing.

Contractual relation between the bank and the service provider

Article 9

(1) When concluding a contract with a service provider, the bank is obliged to take care that the contractual provisions are appropriate in terms of their scope and content, i.e. proportionate to the risks of outsourcing and the scope and complexity of outsourced activities.

(2) The bank is obliged to conclude a written contract with the service provider, which will clearly define all relevant terms, conditions, rights, obligations and responsibilities of the contracting parties.

(3) The outsourcing agreement shall contain as a minimum the following:

1) a detailed description of the activities that are the subject of the contract,

2) place, time and manner of fulfilling contractual obligations,

3) duration of the contract, i.e. date of beginning and end of the contract,

4) the method of supervision over the performance of activities that are the subject of the contract by the bank on a continuous basis, and the obligation to report to the bank by the service provider,

5) description of the expected quality and level of services,

6) financial obligations of the contracting parties,

7) the location where the activity will be performed, including possible data storage and conditions that must be met, and the requirement to notify the bank if the service provider decides to change the location of the activity,

8) the possibility of hiring subcontractors, stating the necessary conditions,

9) the obligation of the service provider to fully act in accordance with the existing regulations of Republika Srpska and Bosnia and Herzegovina when providing services,

10) the obligation to keep business secrets, and the obligation of keeping and the manner of protection of confidential data, requirements for the availability and integrity of relevant data,

11) the obligation of the service provider to timely inform the bank of all facts and changes in circumstances that significantly affect, or could significantly affect, the fulfillment of contractual obligations,

12) a detailed description of the conditions for cancel and / or termination of the contract, including the right of the bank to terminate or cancel the contract with the service provider (at the request of the bank or by order of the Agency),

13) provisions regarding the timely elimination of security risks and other deficiencies identified in the provision of services (at the request of the bank or by order of the Agency),

14) the right to access data by the bank in case of bankruptcy, resolution or interruption of business activities of the service provider,

15) the obligation of the service provider to cooperate with the Agency, including other persons appointed by it,

16) choice of applicable law and

17) manner of resolving disputes.

(4) In the case of outsourcing materially significant activities, the contract, in addition to the provisions referred to in Paragraph 3 of this Article, must also contain the following:

1) the obligation of the service provider to enable the Agency to perform on-site supervision over the part of the operations of the service provider that has links or may be related to outsourcing, as well as on-site supervision over the activities that are the subject of the contract, and to provide timely, unrestricted and unimpeded access to documentation, premises, responsible persons and data related to outsourcing, and owned by the service provider,

2) the obligation of the service provider not to disclose or announce the visit by the Agency to third parties,

3) requirement that the service provider has a contract on professional liability insurance,

4) a detailed description of the rights and obligations of the contracting parties in the event of initiating the bank resolution procedure, especially taking into account the powers of the Agency referred to in Articles 235–238 of the Banking Law,

5) a detailed description of the rights and obligations of the contracting parties in the event of early termination of the contract in order to ensure the continuity of service provision,

6) requirements for the application and testing of business continuity plans.

(5) The service provider is obliged to, before concluding the contract with the subcontractor, ensure that the contract of the service provider with the subcontractor is harmonized with the items of the contract between the bank and the service provider, and that the subcontractor meets all requirements defined by the contract, this Decision and other laws and bylaws. as well as to provide the same access and supervision rights to the bank and the Agency as provided by the service provider.

(6) In case of outsourcing a part of materially significant activity to a subcontractor, it is necessary for the bank to contractually require from the service provider the following:

1) Detailed description of the activities to be outsourced to the subcontractor;

2) Indication of certain conditions that must be met in that case;

3) Obligation of the service provider to notify the bank in writing and in accordance with the agreed deadlines of any planned subcontracting or significant changes, especially if they may affect the ability of the service provider to fulfill its obligations under the outsourcing contract. The agreed deadlines for notifying the bank should at least allow the bank to conduct a risk assessment before subcontracting or significant changes;

4) Obligation of the service provider to exercise control over the transferred activities;

5) To ensure that the bank has the right to object to the planned subcontracting or significant change or to require the explicit approval of the bank for the planned subcontracting or significant change, and

6) The possibility for the bank to terminate the contract in the event that the transfer of services to a subcontractor increases the risks to which the bank is exposed by the outsourcing itself.

(7) The outsourcing agreement should explicitly allow the bank to terminate the agreement, in accordance with applicable law, in the following situations:

1) if the service provider violates the applicable law, regulations or contractual provisions,

2) if obstacles are identified that could change the method of performing the outsourced activity,

3) if there are material changes that affect the outsourcing or the service provider (e.g. subcontracting or changing subcontractors),

4) if there are weaknesses in terms of the management of confidential, personal or otherwise sensitive data or information or in terms of their security, and

5) if the Agency issues such an order (for example, if the Agency is no longer able to effectively supervise the bank due to outsourcing).

(8) The contract on outsourcing should define the possibility of transferring outsourcing to another service provider or returning activities within the bank. For this reason, a written contract on outsourcing should:

1) clearly define the obligations of the existing service provider in case of transfer of outsourced activity to another service provider or return of activities within the bank, including obligations regarding data handling,

2) determine an appropriate notice period in order to reduce the risk of interruption of outsourced activity and

3) determine the obligation of the service provider to provide support to the bank during the transfer of activities in case of cancelation and / or termination of the outsourcing contract.

Exit strategy

Article 10

(1) The bank is obliged, in accordance with Article 6, Paragraph 3, Item 5 of this Decision, to adopt an exit strategy and procedures for cases when the contract on outsourcing, bankruptcy or liquidation of service providers is terminated, the deterioration of quality of outsourced activities and potential business disturbances caused by inappropriate or unsuccessful performance of outsourced activity. The exit strategy includes:

1) objectives,

2) impact analysis in terms of identifying the necessary financial and human resources in order to implement the strategy and the time required for its implementation,

3) distribution of responsibilities and competencies for managing the exit strategy and transfer of activities,

4) criteria according to which it is assessed whether the transfer of activities and data has been performed in an adequate manner,

5) indicators that should point out to the activation of the exit strategy,

6) the strategy of continuing to perform outsourced activities by another service provider or returning the same activities within the bank, and providing conditions for its implementation.

(2) As part of its regular business continuity testing, the bank shall also include a scenario related to the inability of the service provider to adequately perform outsourced materially significant activities. This scenario should also include the possibility of bankruptcy or liquidation of the service provider or the impact of relevant risks on the service provider's business (e.g. political risks in the service provider's country).

Data security

Article 11

(1) The bank should ensure that service providers, where relevant, comply with appropriate ICT security standards.

(2) Where appropriate (e.g. when outsourcing cloud services or other outsourcing in the field of ICT), the bank should define data and system security requirements in the outsourcing agreement and continuously monitor compliance with these requirements.

(3) In the case of outsourcing of cloud services and other outsourcing agreements, which include the handling and transfer of personal or confidential data, the bank should apply a risk-based approach based on the location or locations (i.e. country or region) for storage. and data processing, and information security issues.

(4) If the location for data storage and processing is located outside the territory of Bosnia and Herzegovina, it is necessary to take into account the differences between national regulations on data protection. The bank should ensure that the outsourcing agreement includes the obligation of the service provider to keep confidential, personal or otherwise sensitive information, and to comply with all legal and regulatory requirements relating to data protection applicable to the bank (e.g. personal data protection and compliance with banking secrecy or similar legal and regulatory obligations regarding confidentiality relating to client information, if applicable).

Right of access to data and right to audit
Article 12

(1) The bank shall ensure that the service provider provides the bank itself, the bank's certified auditor, the Agency and third parties appointed by the Agency with timely, unrestricted and unhindered access to documentation, relevant business premises (headquarters, computer center, etc.), including access to all relevant devices, systems, networks, information and data used to provide the outsourced activity, which are in the possession of the service provider or subcontractor, as well as all related financial information and responsible persons.

(2) If it is an outsourcing of activities that are not material, the bank is obliged to provide the right of access and the right to audit referred to in Paragraph 1 of this Article based on risk assessment, having in mind the nature of outsourced activity, and related operational and reputational risk, impact on the continuous performance of activities and the agreed period.

(3) The bank shall ensure that the outsourcing agreement or some other agreement does not prevent or jeopardize its successful exercise of the right of access and the right to audit the bank, as well as the right of access and the right to audit by the Agency or third parties appointed by the Agency.

(4) Contracts and findings, as well as reports of internal and external auditors relating to outsourced activities, should be available in one of the official languages of Republika Srpska.

(5) The bank should exercise its access rights and audit rights, determine the frequency of audits and the areas in which audits should be conducted based on a risk-based approach, and comply with relevant national and international auditing standards.

(6) In exercising its right of access and right to audit, the bank may apply:

1) group audits, organized together with other clients of the same service provider, conducted by themselves and those clients or a third party appointed by them in order to make more rational use of audit resources and to reduce the organizational burden on clients and service providers, and

2) third-party certificates and third-party audit reports or internal audit reports made available by the service provider.

(7) In the case of materially significant activities, the bank should assess whether the certificates and reports of third parties referred to in Paragraph 6, Item 2 of this Article are sufficient to meet regulatory requirements, and should not rely solely on these reports in the long run.

(8) The bank should use the method referred to in Paragraph 6, Item 2 of this Article only in the following cases:

1) if it is satisfied with the audit plan for the outsourced activity,

2) if it ensures that the scope of the certification or audit report includes systems (i.e. procedures, applications, infrastructure, computer centers, etc.) and controls identified by the bank as key, as well as compliance with relevant regulatory requirements,

3) if it examines in detail and continuously the content of audit reports and the scope of certification, and checks that the above are not obsolete, i.e. that they are still relevant,

4) if it is satisfied with the qualification of the auditing company conducting the audit and the legal entity conducting the certification (e.g. regarding the change of the auditing company conducting the audit and the legal entity for certification, qualification, expertise, etc.),

5) if it is satisfied that the certificates are issued and audited in accordance with the relevant professional standards, and include testing the operational efficiency of existing key controls,

6) if it has the contractual right to request the extension of the scope of certification or audit reports to other relevant systems and controls, where the number and frequency of such requests should be reasonable and justified from the point of view of risk management, and

7) if it retains the contractual right to perform, according to its own decision, individual audits of materially significant outsourced activities.

(9) The bank is obliged to ensure the implementation of penetration testing in order to verify the effectiveness of implemented protection measures, controls and procedures in the field of ICT, in cases where the data (key ICT systems) are with the service provider.

(10) The bank, the Agency or third parties appointed by the Agency or the bank should promptly notify the service provider of the audit at the service provider's location, except in cases where this would lead to a situation where the audit would no longer be effective.

(11) When conducting audits in multi-client environments, measures should be taken to avoid or mitigate risks to another client's environment (e.g. impact on service quality, data availability, confidentiality, etc.).

(12) If outsourcing involves a high level of technical complexity, for example in the case of outsourcing of cloud services, the bank should verify that the auditor, whether its internal auditors, group of auditors or external auditors, has appropriate and relevant skills and knowledge for the effective conduct of audits and / or assessments. The same applies to persons in the bank who review audit reports and third-party certificates.

Supervision of outsourced activities
Article 13

(1) The bank shall take appropriate measures to ensure that the outsourced activities meet the quality standards that would be applied in the case of performing the same activities within the bank. In doing so, the bank is fully responsible for meeting all regulatory requirements regarding outsourced activities.

(2) The bank shall continuously monitor the operations of service providers in all outsourcing contracts, based on risk assessment, and obligatorily in the case of outsourcing of materially significant activities, including the availability, integrity and confidentiality of data and information. In doing so, it is obliged to:

1) ensure that service providers submit appropriate reports to it,

2) evaluates the operations of service providers on the basis of key performance indicators, service delivery reports, relevant certificates and independent verification reports, and

3) monitor and analyze all other relevant information received from the service provider, including business continuity plans and reports on their testing.

(3) Banks are obliged to regularly update their risk assessments, as well as the material significance of the outsourced service, in accordance with Articles 4 and 8 of this Decision, at least once a year, and obligatorily during a significant change in the provision of outsourced service. As part of these risk assessments, banks are required to also monitor and manage concentration risks caused by outsourcing.

(4) The bank should take appropriate measures if it identifies deficiencies in the provision of outsourced activities. In particular, the bank should respond to all indications that service providers may not perform materially significant activity efficiently or in accordance with applicable laws and regulatory requirements. If deficiencies are identified, the bank should take appropriate corrective measures. Where appropriate, these measures may include termination of the outsourcing contract.

Notifying the Agency

Article 14

(1) If the bank intends to outsource materially significant activities, it shall notify the Agency thereof in advance and submit the complete stipulated documentation.

(2) The Agency, within 90 days from the day of receipt of the notification, i.e. complete stipulated documentation, shall determine whether the conditions for outsourcing are met in accordance with laws and bylaws and shall inform the bank about the results of the assessment.

(3) The bank, after receiving the notification that the conditions for outsourcing referred to in Paragraph 2 of this Article have been met, may enter into an agreement on materially significant outsourcing.

(4) The bank shall promptly notify the Agency of any significant change (including the hiring or replacement of hired subcontractors) and / or serious events that could materially jeopardize the outsourcing agreement and have consequences for the bank's business activities, profitability or reputation. In addition to the said notification, a reassessment of the risk must be submitted, taking into account the said change.

(5) In the event of termination of the contract, the bank shall, no later than 30 days before the termination of the contract, notify the Agency and submit a report on the manner of performing activities, i.e. future plans for continued outsourced activities.

(6) The bank shall promptly notify the Agency in the event of a change in the material significance of the previously outsourced activity, and submit an assessment of the material significance.

Request for documentation in the case
outsourcing materially significant activities
Article 15

The bank is obliged to enclose the following documents with the draft decision of the bank supervisory board on outsourcing, which relates to materially significant activities:

1) an excerpt from the court or other appropriate register, from which the ownership structure of the service provider can be determined, in the original or a certified copy, not older than six months from the day of delivery of the decision,

2) a list of persons in a special relation with the bank, which/who are also related to the service provider, and a description of the manner in which they are related,

3) audit reports of service providers for the previous calendar year,

4) proof of previous experience of service providers in activities that are the subject of outsourcing,

5) audit reports of the service provider for the previous calendar year (financial and, if applicable, reports of the IT system auditor). If the service provider is not subject to the obligation to audit the financial statements, the bank is obliged to submit copies of the balance sheet and income statement of the service provider for the previous two calendar years,

6) proof that the bankruptcy procedure, i.e. the liquidation procedure of the service provider has not been opened,

7) the draft contract, which contains the elements defined by this Decision, and the bank intends to conclude it with the service provider in connection with the outsourcing of materially significant activities,

8) results of risk assessment related to outsourcing,

9) results of in-depth analysis of service providers,

10) the results of the outsourcing impact assessment referred to in Article 4, Paragraph 2 of this Decision,

11) a description of the obligations and responsibilities of the department or employees which/who will be in charge of supervising the contractual relation with the service provider and managing that relation,

12) exit strategy of the bank,

13) internal acts related to outsourcing referred to in Article 6, Paragraph 3 of this Decision,

14) a detailed description of technical and organizational solutions that enable safe and quality performance of activities that are intended to be outsourced, including a description of how to protect the confidentiality, availability and integrity of data,

15) a statement by the bank that the members of the management body are not in a direct or indirect interest with the service provider, and that there is no other type of conflict of interest, and

16) other acts that the bank considers important.

Additional requirements
Article 16

(1) The Agency reserves the right to impose specific conditions, i.e. prohibition of outsourcing, if it assesses that the bank in the intended and / or existing outsourcing cannot adequately manage the risks associated with outsourcing or if it assesses that outsourcing would lead to the risk of excessive bank exposure towards the same service provider or the risk of exposure of several banks to the same service provider, which may have a potential impact on the bank or the banking system as a whole.

(2) In addition to the documents referred to in Articles 14 and 15 of this Decision, the Agency may request other documentation, which it deems necessary to assess the fulfillment of the conditions for outsourcing.

Audit of outsourced activities
Article 17

(1) The bank's internal audit function shall regularly audit outsourced activities and report thereon to the audit committee and the supervisory board. The plan and work program of internal audit in this segment should be determined in such a manner that the frequency of audits and areas in which audits are to be conducted are defined on the basis of an approach based on the assessment of risks arising from outsourcing. Regardless of the outcome of the risk assessment, any materially significant outsourced activity should be fully audited over a period of three years.

(2) The audit referred to in Paragraph 1 of this Article should at least include the following:

1) assessment of the correct and efficient application of internal acts related to outsourcing,

2) adequacy, quality and efficiency of assessment of materially significant activities,

3) adequacy, quality and efficiency of outsourcing risk assessment and that it is in line with the risk appetite strategy,

4) adequacy of the involvement of management bodies in the process of outsourcing,

5) adequacy of monitoring and management of outsourced activities,

6) control environment at service providers and / or subcontractors through direct verification, where applicable, taking into account the provisions of Article 12 of this Decision.

(3) The external audit of the bank shall take into account outsourced activities and their significance and impact on the bank's operations, and accordingly draft an audit plan and a more efficient approach to the audit.

Coming into force
Article 18

(1) This Decision shall come into force on the eighth day from the day of its publication in the "Official Gazette of Republika Srpska".

(2) Banks are obliged to harmonize their operations with the provisions of this Decision no later than 31 March, 2021.

(3) Banks are obliged to harmonize the existing outsourcing agreements with the provisions of this Decision by 31 December, 2021.

(4) With the entry into force of this Decision, the Decision on Outsourcing Management shall cease to be valid ("Official Gazette of Republika Srpska", No. 75/17).

Number: UO-188/20

Date: 29 October, 2020

PRESIDENT OF THE
MANAGEMENT BOARD
Bratoljub Radulović