Pursuant to Article 35, paragraph 1 subparagraph 1.1 and Article 65 of the Law No. 03/L–209 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010), amended and supplemented by Law No. 05/L–150 (Official Gazette of the Republic of Kosovo / No. 10/03 April 2017), pursuant to Article 21 and 135 of the Law No. 08/L-328 on Payment Services, and Article 58 of the Law No. 08/L-304 on Banks the Board of the Central Bank of the Republic of Kosovo, at its meeting held on December 17, 2024, approved the following:

REGULATION ON OUTSOURSING

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose and scope

1. This Regulation specify the internal governance arrangements, including sound risk management, regarding outsource functions, in particular to the outsourcing of critical or important functions.
2. This Regulation shall apply to banks, electronic money institutions, payment institutions, microfinance institutions and non-bank financial institutions ("institutions").

Article 2
Definitions

1. The terms and definitions used in this Regulation shall have the same meaning as in Law on Payment Services, the Law on Banks and the Law on Microfinance Institutions and Non-Bank Financial Institutions.
2. In addition to paragraph 1 of this Article, for the purpose of implementing this Regulation, the following terms and abbreviations shall have the following meanings:
   - 2.1. **"Outsourcing"** means an arrangement of any form between a bank, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the bank, the payment institution or the electronic money institution itself;
   - 2.2. **"Function"** means any processes, services or activities;
   - 2.3. **"Critical or important function"** means any function that is considered critical or important as set out in this Regulation;
   - 2.4. **"Sub-outsourcing"** means a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider;

2.5. **"Service provider"** means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement;

2.6. **"Cloud services"** means services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction;

2.7. **"Public cloud**" means cloud infrastructure available for open use by the general public.

2.8. **"Private cloud"** means cloud infrastructure available for the exclusive use by a single institution or payment institution.

2.9. **"Community cloud"** means cloud infrastructure available for the exclusive use by a specific community of institutions or payment institutions, including several institutions of a single group.

2.10. **"Hybrid cloud"** means cloud infrastructure that is composed of two or more distinct cloud infrastructures.

2.11. **"ICT"** means information and communication technologies.

2.12. **"Institutional protection scheme"** means a contractual or statutory liability arrangement which protects those institutions that are a member of the scheme and in particular ensures their liquidity and solvency to avoid bankruptcy where necessary.

2.13. **"Management body" means:**

2.13.1. for banks, microfinance institutions and non-bank financial institutions, this terms as the same meaning as in Article 36, of the Law No. 08/L-304 on Banks;

2.13.2. for payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the payment institutions and electronic money institutions and, where relevant, persons responsible for the management of the payment services activities of the payment institutions and electronic money institutions;

2.13.3. for PSPs referred to in subparagraphs 1.4, 1.5 and 1.6 of Article 1 of the Law on Payment Services, this term has the meaning conferred to it by the applicable Law;

2.14. **"Institutions"** means banks, electronic money institutions, payment institutions, microfinance institutions and non-bank financial institutions;

2.15. **"Law on protection of personal data"** means Law No. 06/L –082 on Protection of Personal Data and/or the Law in force for Protection of Personal Data;

2.16. "**Law on Banks"** means Law No. 08/L-304 on Banks and/or the applicable Law on Banks;

2.17. "**Law on Microfinance Institutions and Non-Bank Financial Institutions**" means Law no. 04/L-093 for Banks, Microfinance Institutions and Non-Banking Financial Institutions and/or the Law in force for MFI and NBFI;

2.18. "**Law on Payment Services"** means Law No. 08/L-328 on Payment Services.

CHAPTER II

PROPORTIONALITY: GROUP APPLICATION AND INSTITUTIONAL PROTECTION SCHEMES

Article 3
Proportionality

1. Institutions and CBK should have regard to the principle of proportionality to ensure that governance arrangements, including those related to outsourcing, are consistent with the individual risk profile, the nature and business model of the institution and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved.
2. When applying the requirements set out in this regulation, institutions should take into account the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities.

Article 4
Outsourcing by groups and institutions that are members of an institutional protection scheme

1. This regulation should also apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation. For this purpose, the parent undertakings should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries, including payment institutions, are consistent, well integrated and adequate for the effective application of this regulation at all relevant levels.
2. Institutions in accordance with paragraph 1 of this Article, and institutions that, as members of an institutional protection scheme, use centrally provided governance arrangements should comply with the following where those institutions:
    2.1. have outsourcing arrangements with service providers within the group or the institutional protection scheme, the management body of those institutions retains, also for these outsourcing arrangements, full responsibility for compliance with all regulatory requirements and the effective application;
    2.2. outsource the operational tasks of internal control functions to a service provider within the group or the institutional protection scheme, for the monitoring and auditing of outsourcing arrangements, institutions should ensure that, also for these outsourcing arrangements, those operational tasks are effectively performed, including through the receiving of appropriate reports.
3. In addition to paragraph 2 of this Article, institutions within a group for which no waivers have been granted, institutions that are a central body or that are permanently affiliated to a central body for which no waivers have been granted, or institutions that are members of an institutional protection scheme should take into account the following:
    3.1. where the operational monitoring of outsourcing is centralized (e.g., as part of a master agreement for the monitoring of outsourcing arrangements), institutions should ensure that, at least for outsourced critical or important functions, both independent monitoring of the

service provider and appropriate oversight by each institution is possible, including by receiving, at least annually and upon request from the centralized monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring. In addition, institutions should receive from the centralized monitoring function a summary of the relevant audit reports for critical or important outsourcing and, upon request, the full audit report;

3.2. institutions should ensure that their management body will be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

3.3. where those institutions within the group, institutions affiliated to a central body or institutions that are part of an institutional protection scheme rely on a central pre-outsourcing assessment of outsourcing arrangements, as referred to in Articles 14 to 16 of this regulation, each institution should receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process;

3.4. where the register of all existing outsourcing arrangements, as referred to in Article 15 of this regulation, is established and maintained centrally within a group or institutional protection scheme, all institutions should be able to obtain their individual register without undue delay. This register should include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group or institutional protection scheme;

3.5. where those institutions rely on an exit plan for a critical or important function that has been established at group level, within the institutional protection scheme or by the central body, all institutions should receive a summary of the plan and be satisfied that the plan can be effectively executed.

CHAPTER III

OUTSOURCING MANAGEMENT

Article 5
Assessment of outsourcing arrangements

1. Institutions shall establish whether the entrusting by an institution of the performance of processes, services or activities to a service provider falls under the definition of outsourcing.

2. For the purposes of this Regulation, the following shall not be considered as outsourcing:

   2.1. services of global financial communication services (e.g., SWIFT) if key information system resources needed for the provision of such service are within the institution;

   2.2. function that is legally required to be performed by a service provider, (e.g., statutory audit);

2.3. market information services (e.g., provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);

2.4. global network infrastructures (e.g., Visa, MasterCard) and telecommunication services;

2.5. clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;

2.6. global financial messaging infrastructures that are subject to oversight by relevant authorities;

2.7. correspondent banking services;

2.8. the acquisition of services that would otherwise not be undertaken by the institution (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line);

2.9. software which, being off-the-shelf, is commercially available in the market and does not require substantial customization; and

2.10. other services similar to those under subparagraphs 2.1 to 2.9 of this paragraph subject to the CBK's prior opinion stating that the provisions of this Regulation shall not apply to the use of those services.

3. Institutions shall not transfer authorizations and competences of its management and supervisory bodies to the service provider.

4. Each service provider involved in the outsourcing must have a separate legal identity distinct from the institution outsourcing the services.

5. Institutions shall, proportionally to the nature, scale and complexity of its activities and the risks inherent in its business model, manage risks to which it is or might be exposed, which result from the entrusting of the performance of processes, services or activities to the service provider, regardless of whether that entrusting falls under the definition of outsourcing.

6. The prior opinion of the CBK referred to in paragraph 2.10 of paragraph 2 of this article, if it relates to an application or request by an institution, a service provider or a prospective institution or service provider, shall be issued within a maximum of two months from the submission of the application or request.

Article 6
Assessment of criticality or importance of function/service to be outsourced

1. Institutions should always consider a function as critical or important in the following situations:

1.1. where a defect or failure in its performance would significantly impair, financial performance and continuity of institution's activity.

1.2. when operational tasks of internal control functions are outsourced, an assessment must be conducted to determine whether a failure to provide the outsourced function or

inappropriate provision thereof would adversely impact the effectiveness of the internal control function.

2. It is necessary to determine the criticality or importance, of the function that shall be outsource in order to manage outsourcing risk.
3. Institutions must establish criteria and define methodology in order to assess the criticality or importance of a function, including its impact on regulatory compliance and licensing, influence on financial performance, contribution to operational resilience and continuity of services, importance in maintaining customer trust and service quality, potential impact on the institution's reputation or market standing, and degree of dependency on core business operations.
4. The assessment of criticality or importance is an ongoing process that should be conducted at regular intervals. Regularly review the assessment of criticality or importance to ensure it stays relevant as business conditions, regulations, and operations change over time.
5. The assessment of critical or important functions involves a structured approach to determine the significance of each function to the institution's operations and regulatory obligations. This assessment is essential for making informed decisions about outsourcing and ensuring that outsourced arrangements do not compromise operational resilience or regulatory compliance.

Article 7
Organizational structure

1. Institutions shall ensure:
   1.1. a clear, transparent and documented decision-making process on outsourcing;
   1.2. a clear allocation of powers and responsibilities of organizational units or employees responsible for documenting, managing and overseeing the process of entering into and implementing any outsourcing arrangements; and
   1.3. adequate resources to ensure compliance with the provisions of regulations and good practices governing outsourcing.
2. Institutions shall establish an outsourcing function or designate a senior staff member (e.g., a person responsible for the work of a control function) responsible for overseeing the risks of outsourcing arrangements and overseeing the documentation of outsourcing arrangements.
3. By way of derogation from paragraph 2 of this Article, Institutions may assign the outsourcing function to a member of the management board.
4. When outsourcing, institutions shall at least ensure the following:
   4.1. the adoption and implementation of decisions related to its business activities and critical or important functions;
   4.2. the maintenance of the orderly conduct of its business and the provision of financial services;
   4.3. adequate identification, assessment, management and mitigation of risks arising from outsourcing;
   4.4. where applicable, appropriate confidentiality arrangements regarding data and other information;

4.5. the maintenance of an appropriate flow of relevant information with service providers;

4.6. with regard to the outsourcing of critical or important functions, the undertaking of at least one of the following actions, within an appropriate time frame:

4.6.1.1. transfer of the function to alternative service providers;

4.6.1.2. reintegration of the function into institution; or

4.6.1.3. discontinuation of the business activities that are depending on the function; and

4.7. where personal data are processed by service providers located in the third countries, data are processed in accordance with Law on Protection of Personal Data.

5. Institutions shall ensure that outsourcing does not result in the transfer of responsibilities from the responsible persons of the institution to the service provider.

Article 8
Outsourcing by a group of institutions

1. Where institutions outsource functions to service providers within the group of institutions to which it belongs, the management and the supervisory board of the institution that outsourced the activity or service in question shall, in line with their competence, be responsible also for those outsourced services and activities and shall retain full responsibility for compliance with all regulatory requirements and the effective implementation of this Regulation.
2. Where institutions entrusts the performance of some control function tasks to a service provider within the group of institutions to which it belongs, for the monitoring and auditing of outsourcing arrangements, it shall ensure that those operational tasks are effectively performed, including through the receiving of appropriate reports.
3. Where the operational monitoring of a particular outsourcing arrangement is centralized within the group of institutions to which an institution belongs (e.g., as part of a master agreement for the monitoring of outsourcing arrangements), the institution shall ensure that, at least for outsourced critical or important functions:

3.1. both independent monitoring of the service provider and appropriate oversight is possible, including by receiving, at least annually and upon request from the centralized monitoring function of the group of institutions, reports that include, at least, a summary of the risk assessment and performance monitoring; and

3.2. it is possible to receive from the centralized monitoring function of the group of institutions a summary of the relevant audit reports for critical or important outsourcing arrangements and, upon request, the full audit report.

4. Institutions shall ensure that its management body will be duly notified of relevant planned changes regarding service providers that are monitored centrally within the group of institutions to which the institution belongs and of the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels.
5. Where institutions relies on an assessment of outsourcing arrangements, as referred to in Article 14 of this Regulation, which is carried out centrally within the group of institutions to which the

institution belongs, before entering into an arrangement with a service provider, it shall ensure that it receives a summary of the assessment and ensure that its specific structure and risks are taken into consideration within the decision-making process.

6. Where the register of all existing outsourcing arrangements is maintained centrally within the group of institutions to which an institution belongs, the institution shall ensure that it is able to obtain without delay its individual register, which contains all outsourcing arrangements with service providers, including outsourcing arrangements with service providers inside that group of institutions, at least to the extent laid down in Article 13 of this Regulation.
7. Where institutions relies on an exit plan for a critical or important function that has been established for the group of institutions to which the institution belongs, it shall ensure that it receives a summary of the plan and be satisfied that the plan can be effectively executed.

Article 9
Outsourcing policy

1. In its policies, institutions shall lay down the principles, responsibilities and procedures in relation to outsourcing.
2. Institutions' management board shall approve and regularly review the policies referred to in paragraph 1 of this Article.
3. The policies referred to in paragraph 1 of this Article shall contain at least the criteria and procedures related to:
   3.1. the process of adopting decisions on outsourcing;
   3.2. the planning of outsourcing arrangements;
      3.2.1.1. the definition of business requirements regarding outsourcing;
      3.2.1.2. the definition of critical or important functions;
      3.2.1.3. the definition, assessment and management of risks arising from outsourcing;
      3.2.1.4. due diligence checks on prospective service providers;
      3.2.1.5. the identification, assessment, management, mitigation or prevention of actual or potential conflicts of interest;
      3.2.1.6. business continuity planning; and
      3.2.1.7. the approval of new outsourcing arrangements;
   3.3. the implementation, monitoring and management of outsourcing arrangements, including:
      3.3.1.1. the ongoing assessment of the service provider's performance;
      3.3.1.2. the procedures for being notified and responding to changes to an outsourcing arrangement or service provider;
      3.3.1.3. the independent review and audit of compliance with legal and regulatory requirements and policies; and
      3.3.1.4. the renewal processes;
   3.4. the documentation and register maintenance; and

3.5. the exit strategies and termination or cancellation processes, including a requirement for a documented exit plan for each critical or important function to be outsourced, where such an exit is considered possible taking into account possible service interruptions or the unexpected cancellation or termination of an outsourcing agreement with the service provider.

Article 10
Conflicts of interests

1. Institutions, in line with Article 11 of Regulation on corporate governance of banks, electronic money institutions, payment institutions, microfinance institution and non-banks financial institutions should identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.
2. Where outsourcing creates material conflicts of interest, including between entities within the same group or institutional protection scheme, institutions and payment institutions need to take appropriate measures to manage those conflicts of interest.
3. When functions are provided by a service provider that is part of a group or a member of an institutional protection scheme or that is owned by the institution, payment institution, group or institutions that are members of an institutional protection scheme, the conditions, including financial conditions, for the outsourced service should be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several institutions within a group or an institutional protection scheme may be factored in, as long as the service provider remains viable on a stand-alone basis; within a group this should be irrespective of the failure of any other group entity.

Article 11
Business continuity plans

1. Institutions, in line with the requirements under Article 17 of Regulations on information technology for banks, electronic money institution and payment institutions should have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions. Institutions and payment institutions within a group or institutional protection scheme may rely on centrally established business continuity plans regarding their outsourced functions.
2. Business continuity plans should take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans should also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.

Article 12
Internal audit function

1. The internal audit function's activities should cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and program should include, in particular, the outsourcing arrangements of critical or important functions.
2. With regard to the outsourcing process, the internal audit function should at least ascertain:
   2.1. that the institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable Laws and regulation, the risk strategy and the decisions of the management body;
   2.2. the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;
   2.3. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the institution's risk strategy;
   2.4. the appropriate involvement of governance bodies; and
   2.5. the appropriate monitoring and management of outsourcing arrangements.

Article 13
Records of outsourced activities

1. Institutions shall keep up-to-date records of outsourced information system-related activities, containing:
   1.1. the number of outsourcing contracts;
   1.2. dates of conclusion, possible changes and termination of validity of the contract;
   1.3. data about the service provider – business name, headquarters, registration number and other relevant data;
   1.4. information on whether the service provider is connected to the institution by ownership and/or management relations;
   1.5. the classification of the outsourced activity that should facilitate its identification (e.g. maintenance of hardware equipment, implementation of software components, penetration testing, maintenance of the core business application, etc.);
   1.6. a brief description of the outsourced activity;
   1.7. description of the data that the service provider has access to or are in its possession, and/or the information on whether the data were transferred to another service provider;
   1.8. information on whether the outsourced activity is critical/key or affects critical/key business processes;
   1.9. the name of the country or countries in which the outsourced activity is carried out and the country or countries in which the data are located;
   1.10. information about the model and type of cloud service;
   1.11. the date of the last assessment of the level of the service provided and the risk assessment of the information system in connection with outsourced activities;

1.12. information about sub-outsourced services (short description of the service, basic data about the subservice provider, etc.).

2. Institutions shall, when requested or in the periodicity determined by the CBK, submit to the CBK an excerpt from the records containing an overview of all outsourced activities of the institution's activities to a third party.

CHAPTER IV
OUTSOURCING PROCESS

Article 14
Pre-outsourcing analysis

1. Before adopting a decision on any outsourcing arrangement, institutions shall:

1.1. assess if the outsourcing arrangement concerns a critical or important function, as set out in Article 6 of this Regulation;

1.2. assess if the supervisory conditions for outsourcing set out in Article 15 of this Regulation are met;

1.3. identify and assess all of the relevant risks arising from the outsourcing arrangement in accordance with Article 16 of this Regulation;

1.4. undertake appropriate due diligence on the prospective service provider in accordance with Article 17 of this Regulation; and

1.5. identify and assess conflicts of interest that the outsourcing may cause in line with corresponding regulation on corporate governance.

Article 15
Supervisory conditions for outsourcing

1. Where an institution outsources a function directly connected to the provision of core financial services to a service provider located in the Republic of Kosovo, one of the following conditions must be met:

1.1. the service provider is authorized by a competent authority or entered in an appropriate register with a competent authority to perform that function; or

1.2. the service provider is authorized to perform that function if such specific authorization for the performance of that function is required under the relevant legislation in force.

2. Where an institution outsources a function directly connected to the provision of core financial services to a service provider located in a third country, the following conditions must be met:

2.1. the service provider is authorized or entered in an appropriate register with a competent authority to perform that function in the third country and is supervised by a relevant competent authority; and

2.2. there is an appropriate cooperation agreement between the CBK and the supervisory authority responsible for the supervision of the third-country service provider.

3. Regardless of outsourced functions, an institution shall maintain at all times sufficient substance and shall ensure that:

   3.1. it meets all the conditions of its authorization at all times;

   3.2. its management and supervisory boards effectively carry out their responsibilities;

   3.3. it retains a clear and transparent organizational framework and structure that enables it to ensure compliance with prescribed requirements;

   3.4. where operational tasks of control functions are outsourced, it monitors and manages the risks arising from the outsourcing of critical or important functions; and

   3.5. it has sufficient resources to ensure compliance with subparagraphs 3.1. to 3.4. of this paragraph.

Article 16
Assessment and management of risks arising from outsourcing

1. Before entering into an arrangement with a service provider and during ongoing monitoring of the service provider's performance, institutions shall assess risks and establish an appropriate system for managing operational and concentration risks and other risks arising from outsourcing.
2. Where the arrangement with a service provider includes the possibility that the service provider sub-outsources critical or important functions to other service providers, institutions shall when carrying out the risk assessment take into account at least the following:

   2.1. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider; and

   2.2. the risk that long and complex chains of sub-outsourcing reduce the ability of the institution to oversee the outsourced critical or important function and the ability of the CBK to effectively supervise them.
3. Before entering into outsourcing arrangements, institutions shall assess the potential impact of outsourcing arrangements on its operational risk and take into account the assessment results when deciding if the function should be outsourced to a service provider.
4. Institutions shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.
5. Institutions rules for the establishment and implementation of a risk management system according to relevant legal acts and regulations adopted under those laws shall apply *mutatis mutandis* to the management of risks arising from outsourcing.
6. Outsourced functions must be adequately covered by institutions' internal control system. Institutions rules for the establishment and implementation of the internal control system and control functions according to relevant laws and regulations adopted under those laws shall apply *mutatis mutandis* to outsourced functions.

Article 17

Due diligence

1. Before entering into outsourcing arrangements and taking into account the assessment of operational risks related to the function to be outsourced, institutions shall ensure in its selection and assessment process that the service provider is suitable.
2. When assessing the suitability of an outsourcing service provider of a critical or important function, institutions shall assess whether the service provider:
   2.1. is of good repute;
   2.2. has appropriate abilities, the expertise, the resources (e.g., human, ICT, financial), the organizational structure; and
   2.3. if applicable, has the authorization to perform that function or is entered in an appropriate register with a competent authority.
3. When conducting due diligence on a prospective outsourcing service provider of a critical or important function, institutions shall also consider the following:
   3.1. the business model of the service provider, its nature, scale, complexity, financial situation, ownership structure and, where the service provider is a member of a group, the structure of the group to which it belongs;
   3.2. the long-term relationships with service providers that have already been assessed and perform services for the institution;
   3.3. whether the service provider is a parent undertaking or subsidiary of the institution and whether it is part of the accounting scope of consolidation; and
   3.4. whether or not the service provider is supervised by the competent supervisory authority.
4. Where outsourcing involves the processing of personal or confidential data, institutions shall verify that the service provider implements appropriate technical and organizational measures to protect the data.

Article 18
Contractual relationship between institutions and a service provider

1. When entering into an arrangement with a service provider, institutions shall ensure that the scope and content of the contractual provisions are adequate to the risks associated with outsourcing and to the scope and complexity of outsourced functions.
2. Institutions shall enter into a written agreement with a service provider which shall contain at least the following:
   2.1. a detailed description of the outsourced function which is the subject of the agreement;
   2.2. the start date and end date of meeting the contractual obligations;
   2.3. the parties' financial obligations;
   2.4. the provisions governing the manner in which an institution continuously monitors the performance of the function, which is the subject of the agreement, including the types of reports to be received by the institution from the service provider and the frequency of their delivery;

2.5. the obligation of the service provider to notify the institution in a timely manner of all facts and changes in the circumstances that have, or might have, a significant influence on meeting the contractual obligations;

2.6. the agreed service level and quality of the performed functions, including the qualitative and, where applicable, quantitative performance targets for the outsourced function that allow for timely corrective action by the institution;

2.7. where appropriate, the obligation of business secrecy and the obligation and manner of protecting confidential and personal data, including provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;

2.8. where relevant, the location(s) where the outsourced function will be provided and where relevant data will be kept, processed and stored, including a requirement to notify the institution if the service provider proposes to change the location(s);

2.9. provisions on whether the sub-outsourcing of the function is permitted;

2.10. the obligation of the service provider to provide the services in such a way that it fully complies with the existing applicable legislation in force of the Republic of Kosovo;

2.11. the obligation of the service provider to ensure access and onsite inspection rights to the CBK in the manner laid down in Article 22, paragraph 1. of this Regulation;

2.12. provisions that ensure that the data that are owned by the institution can be accessed in the case of dissolution or discontinuation of business operations of the service provider (e.g. bankruptcy, resolution, winding up or similar proceedings);

2.13. provisions on whether the service provider should take a professional indemnity insurance policy and, if applicable, the level of insurance cover requested;

2.14. the obligation of the service provider to cooperate with the CBK as competent authorities and resolution authorities of the institution;

2.15. the duration of the contractual relationship or an indication that the agreement is of indefinite duration;

2.16. a description of the conditions for the termination and/or cancellation of the agreement with defined notice periods for the institution and for the service provider;

2.17. the rights of the institution to terminate or cancel an agreement with the service provider, if so, ordered by the CBK;

2.18. the selection of the applicable Law; and

2.19. the method of dispute settlement.

3. Where institutions and the service provider enter into an outsourcing agreement for critical or important functions, the agreement must, in addition to the content specified in paragraph 2, contain the following:

3.1. the obligation of the service provider to ensure access and audit rights to the institution in the manner laid down in Article 22, paragraph 2 of this Regulation;

3.2. provisions on the implementation and testing of business contingency plans;

3.3. the obligations of the service provider in the case of a transfer of the outsourced function to another service provider or back to the institution, including the obligations regarding the treatment of data;

3.4. setting of an appropriate transition period, during which the service provider, after the termination or cancellation of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and

3.5. the obligation of the service provider to support the institution in the orderly transfer or reintegration of the function in the event of the cancellation or termination of the outsourcing agreement.

4. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.

5. If sub-outsourcing of critical or important functions is permitted, institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e., a material part of the critical or important function) and, if so, record it in the register.

6. Where an outsourcing agreement for critical or important functions includes the possibility of sub-outsourcing, in addition to the content specified in paragraphs 2. and 3. of this Article, that agreement must contain at least the following:

6.1. the obligation of the service provider to notify the institution of any planned sub-outsourcing, or material changes thereof, within the period that would allow the institution to carry out a risk assessment of the proposed changes and, where necessary, to object in a timely manner to planned sub-outsourcing, or material changes thereof;

6.2. the right to cancel/terminate the agreement where the sub-outsourcing increases the risks for the institution or where the service provider sub-outsources without notifying the institution and in other justified cases;

6.3. where the sub-outsourcing involves the processing of personal data, the obligation of the service provider to obtain written authorization of the institution;

6.4. the obligation of the service provider to oversee those services that it has sub-contracted;

6.5. the conditions to be complied with in the case of sub-outsourcing;

6.6. the types of functions that may not be sub-outsourced;

6.7. the obligation of the service provider to request written approval of the institution for any planned sub-outsourcing, or material changes thereof or the right to object to planned outsourcing; and

6.8. the obligation of the service provider to negotiate with the sub-contractor on access and audit or on-site inspection rights in the manner laid down in Article 22, paragraph 1 of this Regulation.

7. Institutions may permit sub-outsourcing only where the sub-contractor undertakes to act in compliance with applicable Law and regulatory requirements, comply with relevant contractual obligations and ensure to the institution and the CBK the same access and audit or onsite inspection rights as those granted by the service provider in accordance with Article 22 of this Regulation.

8. Institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 7 of this Article would not be met, the institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

Article 19
Security of data and systems

1. Institutions shall ensure that service providers, where relevant, comply with appropriate ICT security standards.
2. In the case of outsourcing to cloud service providers or other ICT outsourcing, institutions shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.
3. Before entering into an arrangement with cloud service providers or other arrangements that involve the handling or transfer of personal or confidential data, institutions shall assess the risks associated with data storage and data processing location(s) (i.e., country or region) and ensure that those risks are within acceptable limits.
4. When outsourcing, in particular to third countries, institutions shall take into account differences in national provisions regarding the protection of data.

Article 20
Cloud outsourcing

1. Cloud outsourcing shall be carried out in accordance with the provisions of this Regulation.
2. In the event of outsourcing referred to in paragraph 1 of this Article, the institution shall additionally determine:
   2.1. clear roles and responsibility for information security of the cloud service provider towards the institution;
   2.2. responsibilities for maintaining hardware and software components according to the manufacturer’s requirements, testing and applying security patches;
   2.3. the method of managing incidents so that the procedures and roles for solving incidents are determined, as well as the method of reporting on the incident and its consequences for the institution;
   2.4. secure authentication mechanism, and/or control of access to data and services using multi-factor authentication;
   2.5. procedures that ensure adequate encryption of data during data transmission, storage and backup.
3. The institution intending to perform cloud outsourcing shall additionally take into account the following when assessing the risk of such outsourcing:

3.1. cloud service implementation model (public, private, shared, hybrid, etc.);

3.2. type of cloud services (infrastructure as a service – IaaS, platform as a service – PaaS and software as a service – SaaS, etc.);

3.3. the impact of data migration and resource implementation in the chosen type of cloud services;

3.4. network capacities for simple and secure data transfer (data portability);

3.5. data protection during cloud migration and storage.

4. When cloud outsourcing, the institution shall develop an adequate exit strategy in the event of termination of the provision of these services, which additionally includes procedures governing the termination and re-establishment of cloud services or their transfer to another service provider or that institution, as well as detailed plans for the migration of data and/or resources of information systems depending on the type of cloud services.

5. The institution shall ensure that any contract on cloud outsourcing shall also contain provisions governing the ownership of data, the method of accessing data and services, as well as the download of the institution's data in a readable format after the termination of the provision of that service and their adequate deletion by the service provider.

Article 21
Sensitive Data Risk Management

1. For the purpose of ensuring data protection and effectively managing risks related to potential loss, alteration, destruction, or unauthorized disclosure of sensitive data, the CBK expects institutions to regulate:

1.1. identify and classify all relevant functions and associated confidential data and systems, as well as measures prescribed to protect those data;

1.2. implement appropriate measures to secure and protect their data and to set out these measures in the outsourcing policy and the contracts agreements governing outsourcing arrangements particularly for critical and important services;

1.3. have a documented data management strategy that addresses the range of risks, which can arise in the context of outsourcing and take into account potential risks, in particular operational risk, including legal risk, ICT related risk, compliance and reputational risks, and potential control limits for performing outsourced activities.

1.4. when conducting risk assessments, to the data characteristics of confidentiality, integrity, availability and authentication of data and information required to deliver outsourced business or service functions.

2. Institutions under this Regulation, must ensure that any transmission of personal data, should be carried out in accordance with applicable Law on the protection of personal data.

Article 22
Access and audit or on-site inspection rights

1. Institutions shall ensure within the outsourcing agreement with the service provider that the service provider ensures the following to the CBK or any persons appointed by the CBK for that purpose:

   1.1. timely and full access to business premises, including devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors; and

   1.2. the carrying out of on-site inspections of a part of the service provider's operation that relates or can be related to outsourcing, as well as on-site inspections of the performance of the functions which are the subject of the agreement with the service provider, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

2. With regard to the outsourcing of critical or important functions, institutions shall ensure within the outsourcing agreement with the service provider that the service provider ensures the following to the institution, its external auditors and other persons it appoints for that purpose and CBK as resolution authorities designated under the relevant provisions of the legislation in force on official administration and liquidation governing the resolution of institutions:

   2.1. timely and full access to business premises, including devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors; and

   2.2. the carrying out of audits or reviews of a part of the service provider's operation that relates or can be related to outsourcing, as well as reviews of the performance of the outsourced functions which are the subject of the agreement with the service provider, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

3. Institutions shall ensure within the outsourcing agreement with the service provider that its internal audit function is able to review the outsourced function using a risk-based approach.

4. Institutions shall exercise its access and audit rights referred to in this Article and determine the audit frequency and areas to be audited on a risk-based approach.

5. For the purpose of carrying out audits and reviews referred to in paragraph 2, subparagraph 2.2 of this Article, an institution may use:

   5.1. pooled audits organized jointly with other clients of the same service provider, and carried out by the institution and these clients or by a third party appointed by them; and

   5.2. third-party certifications and third-party or internal audit reports, made available by the service provider.

6. For the outsourcing of critical or important functions, an institution shall assess whether third-party certifications and reports as referred to in paragraph 5, subparagraph 5.2 of this Article are adequate and sufficient for the carrying out of appropriate audits and reviews of outsourcing arrangements and shall not rely solely on these reports over time.

7. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, an institution shall verify:

7.1. whether the persons referred to in paragraph 5 of this Article who carry out the audit and/or assessment have appropriate and relevant skills and knowledge to carry out relevant audits and/or assessments effectively; and

7.2. whether the staff of the institution reviewing certifications and/or reports by the persons referred to in paragraph 5 of this Article have appropriate and relevant skills and knowledge to carry out relevant audits and/or reviews effectively.

Article 23
Termination rights

1. The outsourcing arrangement should expressly allow the possibility for the institution to terminate the arrangement, in accordance with the Law on Payment Services and the Law on Banks, including in the following situations:

   1.1. where the provider of the outsourced functions is in a breach of the Law on Payment Services and the Law on Banks, regulations or contractual provisions;

   1.2. where impediments capable of altering the performance of the outsourced function are identified;

   1.3. where there are material changes affecting the outsourcing arrangement or the service provider (e.g., sub-outsourcing or changes of sub-contractors);

   1.4. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and

   1.5. where instructions are given by CBK, e.g., in the case that the CBK is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution.

2. The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution. To this end, the written outsourcing arrangement should:

   2.1. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution, including the treatment of data;

   2.2. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and

   2.3. include an obligation of the service provider to support the institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.

Article 24
Oversight of outsourced functions

1. Institutions should monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured. Where the risk, nature or scale of an outsourced

function has materially changed, institutions should reassess the criticality or importance of that function in line with Article 6 of this Regulation.

2. Institutions should apply due skill, care and diligence when monitoring and managing outsourcing arrangements.

3. Institutions should regularly update their risk assessment in accordance with Article 16 of this Regulation and should periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.

4. Institutions should monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account Article 16 of this Regulation.

5. Institutions should ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by:

   5.1. ensuring that they receive appropriate reports from service providers;

   5.2. evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and

   5.3. reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.

6. Institutions should take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, institutions should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, institutions and payment institutions should take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.

Article 25
Exit strategies

1. For the purpose of ensuring a continuous performance of the functions which are subject to outsourcing, without adverse impact on the compliance with regulatory requirements and on the quality of provision of services to clients, institutions shall establish for all outsourced critical and important functions an exit strategy at least in the case of:

   1.1. the cancellation or the termination of outsourcing arrangements;

   1.2. the failure of the service provider;

   1.3. the deterioration of the quality of the outsourced function and actual or potential business disruptions caused by the inappropriate or failed provision of services associated with the outsourced function;

   1.4. material risks arising for the appropriate and continuous application of the outsourced function.

2. Institutions shall ensure that it is able to cancel or terminate outsourcing arrangements with service providers without undue disruption to its business activities, without limiting its compliance with

regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients.

3. To achieve the conditions referred to in paragraph 2 of this Article, institutions shall:

   3.1. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g., by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and

   3.2. identify alternative solutions and develop transition plans to enable the institution to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the institution or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.

4. When developing exit strategies, institutions shall:

   4.1. define the objectives of the exit strategy;

   4.2. perform a business impact analysis that is commensurate with the risk of the outsourced functions, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;

   4.3. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;

   4.4. where applicable, define success criteria for the transition of outsourced functions and data; and

   4.5. define the indicators to be used for the monitoring of the outsourcing arrangement with the service provider, including indicators based on unacceptable service levels that should trigger the exit.

CHAPTER V

OBLIGATION FOR PRIOR APPROVALS

Article 26
Prior approvals of the outsourcing of a critical or important function

1. Institutions which intends to outsource a critical or important function as set out in Article 6 of this Regulation shall, within a reasonable time frame, but no later than 30 days before entering into an arrangement with a service provider, notify the CBK thereof and request prior approvals.

2. The request referred to in paragraph 1 of this Article must contain an explanation comprising a description of critical or important functions to be outsourced and the reasons for adopting a decision on outsourcing.

3. The request referred to in paragraph 1 of this Article shall be accompanied by the information referred to in Article 13, paragraphs 3 and 4 of this Regulation that shall be contained in the register after entering into an outsourcing arrangement.
4. Where a service provider has its head office and/or operates in third countries, institutions shall submit evidence that the regulations of a country or countries in which the service provider operates enable the CBK:
   4.1. in order to reach the objectives of supervision, to carry out an on-site inspection of a part of the service provider's operation that relates or can be related to outsourcing, as well as an on-site inspection of the functions which are the subject of the agreement; and
   4.2. to have timely and full access to the documentation and data related to outsourcing which are in the possession of the service provider.
5. In addition to the information referred to in paragraphs 3 and 4 of this Article, the CBK may request any additional information that it deems necessary for the assessment whether the conditions for outsourcing laid down in the Law on Banks, the Law on Payment Services and this Regulation have been met.
6. The CBK's prior approval under this Article shall be granted or denied within a maximum of two months from the date of submission of the relevant information, including the relevant information referred to in the previous paragraph.

CHAPTER VI

FINAL PROVISIONS

Article 27
Transitional period

1. Institutions subject to this Regulation shall fully adapt their activities and operations, including existing contractual arrangements for outsourcing, to the provisions of this Regulation within 24 months of the date of entry into force referred to in Article 30 of this regulation.
2. All outsourcing arrangements entered into after the date specified in Article 30 shall be subject to the provisions of this Regulation.

Article 28
Enforcement, Improvement Measures and Penalties

Any violation of the provisions of this Regulation shall be subject to corrective measures civil and administrative and civil penalties, as defined in Article 67 of the Law 03/L-209 on the Central Bank of the Republic of Kosovo as amended and supplemented by the Law No. 05/L –150 and the Law on Payment Services, Article 124, subparagraphs 2.8 and 2.9.

Article 29
Repeal

Upon entry into force of this Regulation, the regulation on agents and subcontracting of activities of the payment service providers chapter V adopted by the Board of the Central Bank of the Republic of Kosovo on 29 November 2019, shall be repealed.

Article 30
Entry into force

This Regulation shall enter into force 10 (ten) days after the entry into force of Law No. 08/L-328 on Payment Services, with the exception of the provisions applicable to banks determined under the Law on Banks which shall enter into force 10 (ten) days after the entry into force of the Law on Banks.

Dr.sc. Bashkim Nurboja
Chairperson of the Board of the Central Bank of the Republic of Kosovo