

Rwanda

Regulation on Outsourcing

Regulation 49 of 2022

Legislation as at 17 June 2022

FRBR URI: /akn/rw/act/reg/2022/49/eng@2022-06-17

There may have been updates since this file was created.

PDF created on 21 February 2024 at 16:47.

[Check for updates](#)



About this collection

The legislation in this collection has been reproduced as it was originally printed in the Government Gazette, with improved formatting and with minor typographical errors corrected. All amendments have been applied directly to the text and annotated. A scan of the original gazette of each piece of legislation (including amendments) is available for reference.

This is a free download from the Laws.Africa Legislation Commons, a collection of African legislation that is digitised by Laws.Africa and made available for free.

www.laws.africa
info@laws.africa

There is no copyright on the legislative content of this document.
This PDF copy is licensed under a Creative Commons Attribution 4.0 License (CC BY 4.0). Share widely and freely.

Regulation on Outsourcing

Contents

| | |
|--|----|
| Chapter One – General provisions | 1 |
| Article One – Purpose | 1 |
| Article 2 – Definition of terms | 1 |
| Article 3 – Functions or activities that cannot be outsourced | 2 |
| Chapter II – Regulatory requirements | 2 |
| Article 4 – Pre-outsourcing conditions | 2 |
| Article 5 – Responsibility of the Board and Senior Management | 3 |
| Article 6 – Outsourcing of material activities | 4 |
| Article 7 – Outsourcing risk management | 4 |
| Article 8 – Due diligence and assessment of service providers | 5 |
| Article 9 – Outsourcing agreement | 6 |
| Article 10 – Service Level Agreements and performance metrics | 7 |
| Article 11 – Conflict of interest | 8 |
| Article 12 – Exit strategy | 8 |
| Article 13 – Control environment offered by the service provider | 8 |
| Article 14 – Confidentiality and security of non-public data | 9 |
| Article 15 – Business Continuity Management | 9 |
| Article 16 – Monitoring and control of outsourcing arrangements | 10 |
| Article 17 – Audit and inspection | 11 |
| Article 18 – Outsourcing outside Rwanda | 12 |
| Article 19 – Outsourcing within a group | 13 |
| Article 20 – Cloud Computing | 13 |
| Chapter III – Requirements for outsourcing material activities | 14 |
| Article 21 – Application to outsource material activities | 14 |
| Article 22 – Approval for outsourcing of material activities | 14 |
| Article 23 – Supervisory Authority's decision | 15 |
| Chapter IV – Miscellaneous and final provisions | 15 |
| Article 24 – Involvement of Supervisory Authority in outsourcing arrangement | 15 |
| Article 25 – Examples of outsourcing arrangements | 16 |
| Article 26 – Compliance landscape | 16 |
| Article 27 – Application of other laws | 16 |
| Article 28 – Penalties and administrative sanctions | 16 |
| Article 29 – Transitional provisions | 16 |
| Article 30 – Repealing provisions | 16 |

| | |
|--|----|
| Article 31 – Drafting, consideration and approval of this regulation | 16 |
| Article 32 – Commencement | 17 |
| Appendix I | 17 |
| Appendix II | 18 |

Rwanda

Regulation on Outsourcing

Regulation 49 of 2022

Published in Official Gazette special on 17 June 2022

Assented to on 2 June 2022

Commenced on 17 June 2022

[This is the version of this document from 17 June 2022.]

Pursuant to Law N° 48/2017 of 23/09/2017 governing the National Bank of Rwanda as amended to date, especially in its articles 6, 8, 9, 10 and 15;

Pursuant to Law N° 47/2017 of 23/09/2017 governing the organization of banking, especially in its Articles 37 and 117;

Pursuant to Law N° 030/2021 of 30/06/2021 governing the organisation of insurance business, especially in its article 82;

Pursuant to Law N° 072/2021 of 05/11/2021 governing deposit-taking microfinance institutions, especially in its articles 23, 24 and 102;

Pursuant to Law N° 061/2021 of 14/10/2021 governing the payment system, especially in its article 30;

Pursuant to Law N° 73/2018 of 31/08/2018 governing credit reporting system, especially in its articles 9, 13 and 23;

Pursuant to Law N° 05/2015 of 30/03/2015 governing the Organization of Pension Schemes, especially in its article 3;

Having reviewed Regulation N° 03/2018 of 24/01/2018 on outsourcing;

The National Bank of Rwanda hereinafter referred to as « Supervisory Authority Supervisory Authority » issues the following regulation:

Chapter One

General provisions

Article One – Purpose

This regulation aims at establishing minimum prudent standards for regulated institutions that outsource their material activities to an external service provider.

Article 2 – Definition of terms

In this regulation, the following terms mean:

- 1° **regulated institution:** any institution regulated and supervised by the Supervisory authority;
- 2° **outsourcing:** the engagement of a service provider from outside the regulated institution to carry out activities or processes related to the execution of financial services or other typical services that would otherwise be performed by the regulated institution itself;

- 3° **material activities:** those activities or functions which:
 - a. if disturbed, may significantly affect the capital, liquidity, business operations, reputation or profitability of the regulated institution;
 - b. involves non-public data and, in the event of any unauthorized access or disclosure, loss or theft, may have a material impact on customers of a regulated institution;
- 4° **material outsourcing:** an outsourcing arrangement of a material activity;
- 5° **service provider:** a person that is undertaking the outsourced activity on behalf of the regulated institution and includes a member of the group to which the regulated institution belongs, related company whether located in Rwanda or outside;
- 6° **sub-outsourcing:** a situation where a service provider under an outsourcing arrangement further transfers an outsourced function to another service provider;
- 7° **cloud services:** services provided using cloud computing, that is, a model for enabling universal, 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;
- 8° **non-public data:** all data that are not publicly available that are:
 - a. related to product and services of a regulated institution or related statistics;
 - b. personal data as defined by specific laws.

Article 3 – Functions or activities that cannot be outsourced

A regulated institution shall not outsource the activities of providing financial services for which it obtained the license from the Supervisory authority.

Outsourcing must not lead to the delegation of responsibility of the board of directors and senior management.

A regulated institution shall not outsource core management functions including:

- 1° corporate planning;
- 2° organization;
- 3° management and
- 4° decision making functions like determination of compliance with applicable laws.

Chapter II Regulatory requirements

Article 4 – Pre-outsourcing conditions

A regulated institution shall ensure that outsourcing does not jeopardize the:

- 1° regular operations, i.e. providing services to customers and beneficiaries in accordance with the existing laws, regulations, and best practice;
- 2° capability to manage and control operations and activities;
- 3° regulated institution's risk management;
- 4° regulated institution's internal control system;
- 5° Supervisory authority's ability to perform supervision.

Regulated institution shall only appoint a service provider providing sufficient guarantees to implement appropriate security, technical and organizational measures in such a manner that processing of person data will meet the requirements of the Law.

The regulated institution shall demonstrate to the Supervisory Authority that, under the outsourcing arrangement, regulations from the Supervisory Authority and laws from the Republic of Rwanda will continue to be met.

Article 5 – Responsibility of the Board and Senior Management

The Board and senior management are ultimately responsible for outsourcing arrangements and for managing risks inherent in such outsourcing relationships.

The board, or a committee delegated by it, is responsible for:

- 1° approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the policies that apply to such arrangements;
- 2° setting a suitable risk appetite to define the nature and extent of risks that the regulated institution is willing and able to assume from its outsourcing arrangements;
- 3° laying down appropriate approval authorities for outsourcing arrangements consistent with its established strategy and risk appetite;
- 4° assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements;
- 5° ensuring that senior management establishes appropriate governance structures and processes for sound and prudent risk management, such as a management body that reviews controls for consistency and alignment with a comprehensive institution-wide view of risk; and
- 6° undertaking regular reviews of these outsourcing strategies and arrangements.

Senior management is responsible for:

- 1° evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework approved by the board;
- 2° developing sound and prudent outsourcing policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements as well as ensuring that such policies and procedures are implemented effectively by line managers;
- 3° regularly reviewing the effectiveness of, and appropriately adjusting, policies and procedures to reflect changes in the regulated institution's overall risk profile and risk environment;
- 4° monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an undertaking regular reviews of these outsourcing strategies and arrangements -wide basis;
- 5° ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and regularly tested;
- 6° ensuring that there is independent review and audit for compliance with outsourcing policies and procedures;
- 7° ensuring that appropriate and timely remedial actions are taken to address audit findings;
- 8° communicating information pertaining to risks arising from its material outsourcing arrangements to the board in a timely manner.

Article 6 – Outsourcing of material activities

Regulated institution shall define the material activities to be outsourced.

In order to assess whether the activity is material, the regulated institution shall consider factors, such as:

- 1° importance of the business activity to be outsourced (e.g., in terms of contribution to income and profit of a regulated institution);
- 2° potential impact of the outsourcing on earnings, solvency, liquidity, funding and capital, and risk profile;
- 3° impact on the regulated institution's reputation and brand value, and ability to achieve its business objectives, strategy and plans, should the service provider fail to perform the service or encounter a breach of confidentiality or security (e.g., compromise of non-public data);
- 4° impact on the institution's customers, should the service provider fail to perform the service or encounter a breach of confidentiality or security;
- 5° impact on the institution's counterparties and the Rwandan financial system, should the service provider fail to perform the service;
- 6° cost of the outsourcing as a proportion of total operating costs of the institution;
- 7° cost of outsourcing failure;
- 8° aggregate risk exposure to a particular service provider in cases where the regulated institution outsources various functions to the same service provider;
- 9° ability to maintain appropriate internal controls and meet regulatory requirements if the service provider faces operational problems.

A regulated institution shall undertake a periodic review of its outsourced processes to identify new outsourcing risks as they arise for example, when the service provider has further sub-outsourced work to other service providers or has undergone a significant change in processes, infrastructure, or management.

Materiality shall be considered both at a regulated institution level and on a consolidated basis i.e. together with the institution's branches and corporations/entities under its control.

Article 7 – Outsourcing risk management

The board and senior management shall be aware of and understand the risks arising from outsourcing. The regulated institution shall establish a framework for risk evaluation which shall include the following activities

- 1° identifying the role of outsourcing in the overall business strategy and objectives of the regulated institution;
- 2° performing comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement to identify and mitigate key risks;
- 3° assessing the service provider's ability to employ a high standard of care in performing the outsourced service and meet regulatory standards as expected of the regulated institution, as if the outsourcing arrangement is performed by the regulated institution itself;
- 4° analysing the impact of the outsourcing arrangement on the overall risk profile of the regulated institution, and whether there are adequate internal expertise and resources to mitigate the risks identified;
- 5° analysing the concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or important functions to a limited number of service providers.
- 6° analysing the benefits of outsourcing against the risks that may arise;

7° establish a threshold (a limit) that a service provider must not exceed while sub outsourcing.

The risk evaluations shall be performed when the regulated institution is planning to enter into an outsourcing arrangement with an existing or a new service provider, and also re-performed periodically on existing outsourcing arrangements, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the regulated institution.

Article 8 – Due diligence and assessment of service providers

In considering, renegotiating, or renewing an outsourcing arrangement, the regulated institution shall subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.

The regulated institution shall assess all relevant aspects of the service provider, including:

- 1° its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the regulated institution itself to meet its obligations as a regulated institution;
- 2° the physical and IT security controls the service provider has in place as well as capability of the technology service provider to comply with obligations in the outsourcing agreement;
- 3° the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement.

The due diligence shall involve an evaluation of all relevant information about the service provider including:

- 1° experience and capability to implement and support the outsourcing arrangement over the contracted period;
- 2° financial soundness and ability to service commitments even under adverse conditions;
- 3° corporate governance, business reputation and culture, compliance, and pending or potential litigation;
- 4° security and internal controls, audit coverage, reporting and monitoring environment;
- 5° risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement;
- 6° disaster recovery arrangements and disaster recovery track record;
- 7° secure infrastructure facilities;
- 8° reliance on and success in dealing with sub-contractors;
- 9° insurance coverage;
- 10° external environment (such as the political, economic, social, technological and legal environment of the jurisdiction in which the service provider operates);
- 11° ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.

The regulated institution must ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the regulated institution's hiring policies for the role they are performing, consistent with the criteria applicable to its own employees including:

- 1° whether they have been the subject of any proceedings of a disciplinary or criminal nature;
- 2° whether they have been convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty);
- 3° whether they have accepted civil liability for fraud or misrepresentation;

4° whether they are financially sound.

Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, shall also be obtained to supplement the regulated institution's assessment. Onsite visits shall be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.

Any adverse findings from this assessment shall be considered in light of their relevance and impact to the outsourcing arrangement.

The due diligence undertaken during the assessment process shall be documented and re-performed at least annually as part of the monitoring and control processes of outsourcing arrangements. The regulated institution must ensure that the information used for due diligence evaluation is sufficiently current. The regulated institution shall also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.

Article 9 – Outsourcing agreement

Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement shall be carefully and properly defined in written agreements.

Outsourcing agreement shall clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses.

The regulated institution shall ensure that every outsourcing agreement addresses the risks identified at the risk evaluation and due diligence stages.

Each outsourcing agreement shall allow for timely renegotiation and renewal to enable the regulated institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations.

The outsourcing agreement shall at least, have provisions to address the following aspects of outsourcing:

- 1° specification of the scope of the outsourcing arrangement, the services to be supplied, the nature of the relationship between the regulated institution and the service provider, confidentiality and security terms, and procedures governing the sub outsourcing of services;
- 2° performance, operational, internal control and risk management standards;
- 3° confidentiality and security requirements as provided in this regulation;
- 4° business continuity management requirement as provided in this regulation;
- 5° a process of monitoring and oversight of the outsourced activities as provided this regulation;
- 6° audit and inspection as provided in this regulation;
- 7° specification that the regulated institution and the Supervisory Authority shall have access to data from the service provider;
- 8° notification of adverse developments: The regulated institution shall specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the regulated institution in order for the regulated institution to take prompt risk mitigation measures and notify Supervisory Authority of such developments;
- 9° dispute resolution: The regulated institution shall specify in its outsourcing agreement the dispute resolution process, events of default, and the indemnities, remedies and recourse of the respective parties in the agreement. The regulated institution shall ensure that its contractual rights can be exercised in the event of a breach of the outsourcing agreement by the service provider;

- 10° default termination and early exit: a regulated institution shall have the right to terminate the outsourcing agreement in the event of default, or under circumstances where:
- a) the service provider undergoes a change in ownership;
 - b) the service provider becomes insolvent or goes into liquidation;
 - c) the service provider goes into receivership or judicial management whether in Rwanda or elsewhere;
 - d) there has been a breach of security or confidentiality;
 - e) there is a demonstrable deterioration in the ability of the service provider to perform the contracted service;
- 11° business continuity: The contract shall contain clauses for contingency plans and testing thereof to maintain business continuity.
- 12° sub-outsourcing: The regulated institution shall retain the ability to monitor and control its outsourcing arrangements when a service provider uses a sub-outsourcing. An outsourcing agreement shall contain clauses setting out the rules and limitations on sub-outsourcing. A regulated institution shall include clauses making the service provider contractually liable for the performance and risk management practices of its sub-outsourcing arrangements and for the sub-outsourcing's compliance with the provisions in its agreement with the service provider, including the prudent practices set out in this regulation. The regulated institution must ensure that the sub-outsourcing of any part of material outsourcing arrangements is subject to the institution's prior approval;
- 13° applicable laws: Agreements shall include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;
- 14° data ownership: The agreement shall clearly state that the regulated institution retains the ownership of data. The data shall be retained to satisfy the purpose for which it is processed except where the law provides otherwise. The regulated institution and the service provider shall understand how data ownership rights are affected by different laws of countries, which will host the data;
- 15° confidentiality: the agreement shall include confidentiality provisions.

The regulated institution shall tailor each agreement to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Rwanda.

Article 10 – Service Level Agreements and performance metrics

The regulated institution shall include Service Level Agreements (SLAs) in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels.

The regulated institution shall develop the following towards establishing an effective oversight program:

- 1° formal policy that defines the SLA program;
- 2° SLA monitoring process;
- 3° recourse in case of non-performance;
- 4° escalation process;
- 5° dispute resolution process;
- 6° conditions in which the contract may be terminated by either party
- 7° Disaster Recovery (DR) and Business Continuity;

- 8° data management;
- 9° service availability commitment;
- 10° penalties and credit outage calculation;
- 11° indemnity.

For outsourced technology operations, specific metrics may be defined around the service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization.

The regulated institution shall define performance expectations, under both normal and contingency circumstances. The regulated institution shall put in place provisions for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

Article 11 – Conflict of interest

A regulated institution shall identify, assess and manage conflicts of interests with regard to the outsourcing arrangements.

Where outsourcing creates material conflicts of interests, the regulated institution needs to take appropriate measures to manage those conflicts of interest.

Article 12 – Exit strategy

Regulated institutions shall have a documented exit strategy in the material outsourcing arrangements that is in line with their outsourcing policy and business continuity plans, taking into account at least the possibility of:

- 1° the termination of outsourcing arrangements;
- 2° the failure of the service provider;
- 3° the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;
- 4° material risks arising for the appropriate and continuous application of the function;
- 5° regulated institution shall ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, the regulated institution shall:
 - a. test their exit plans (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);
 - b. identify alternative solutions and develop transition plans to enable the regulated institution to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the regulated institution;
 - c. 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.

Article 13 – Control environment offered by the service provider

The regulated institution shall evaluate the adequacy of internal controls environment offered by the service provider. Due consideration shall be given to the implementation of following by the service provider:

- 1° information security policies and employee awareness;

- 2° controls for logical access to non-public financial data by service provider staff, so that information may be accessed on a need-to-know basis only;
- 3° environmental security controls;
- 4° network security controls;
- 5° formal process for tracking and monitoring program changes;
- 6° process for incident reporting and problem management;
- 7° special control considerations for service providers using cloud computing as part of service;
- 8° control considerations for handling of financial data;
- 9° data classification and controls for handling data.

Article 14 – Confidentiality and security of non-public data

The regulated institution shall satisfy itself that the service provider's security policies, procedures and controls will enable the regulated institution to protect the confidentiality and security of non-public data.

The regulated institution must be proactive in identifying and specifying requirements for confidentiality, integrity and availability in the outsourcing arrangement. The regulated institution must take the following steps to protect the confidentiality and security of non-public data:

- 1° State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which each party has the right to change security requirements. The outsourcing agreement shall also address:
 - a. the issue of the party liable for losses in the event of a breach of confidentiality, security of personal data and the service provider's obligation to inform the institution;
 - b. the issue of access to and disclosure of information by the service provider. Non-public data shall be used by the service provider and its staff strictly for the purpose of the contracted service;
- 2° disclose non-public data to the service provider only on a need-to-know basis;
- 3° ensure the service provider is able to protect the confidentiality of non-public data, documents, records, and assets, particularly where multi-tenancy arrangements are present at the service provider;
- 4° review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, adequacy of security of non-public data, compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the institution breaches of confidentiality in relation to non-public information.

Contracting parties shall sign a non-disclosure agreement.

Article 15 – Business Continuity Management

A regulated institution shall ensure that its business continuity is not compromised by outsourcing arrangements. The institution shall adopt the sound practices and standards contained in the Business Continuity Management (BCM) regulation issued by Supervisory Authority, in evaluating the impact of outsourcing on its risk profile and for effective BCM.

In line with the BCM regulation, the institution shall take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that the institution remains able to conduct its business with integrity and competence in the event of a service

disruption or failure, unexpected termination of the outsourcing arrangement or liquidation of the service provider. These shall include taking the following steps:

- 1° Determine that the service provider has in place satisfactory business continuity plans (BCP) that are commensurate with the nature, scope and complexity of the outsourcing arrangement. Outsourcing agreements shall contain BCP requirements on the service provider, in particular, recovery time objectives (RTO), recovery point objectives (RPO), and resumption operating capacities;
- 2° Proactively seek assurance on the state of BCP preparedness of the service provider, or participate in joint testing, where possible. The institution shall ensure the service provider regularly tests its BCP plans and that the tests validate the feasibility of the RTO, RPO and resumption operating capacities. Such tests would serve to familiarize the institution and the service provider with the recovery processes as well as improve the coordination between the parties involved. The regulated institution shall require the service provider to notify it of any test finding that may affect the service provider's performance. The institution shall also require the service provider to notify it of any substantial changes in the service provider's BCP plans and of any adverse development that could substantially impact the service provided to the institution;
- 3° Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the institution will be able to continue business operations and that all documents, records of transactions and information previously given to the service provider should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.

For assurance on the functionality and effectiveness of its BCP plan, a regulated institution shall design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement. For tests to be complete and meaningful, the institution must involve the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff. Similarly, the regulated institution shall take part in its service providers' BCP and disaster recovery exercises.

The regulated institution shall consider worstcase scenarios in its business continuity plans. Some examples of these scenarios are unavailability of service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions that result in collateral impact on both the institution and the service provider. Where the interdependency on an institution in the financial system is high, the institution should maintain a higher state of business continuity preparedness. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate interdependency risk.

Article 16 – Monitoring and control of outsourcing arrangements

The regulated institution shall establish a structure for the management and control of its outsourcing arrangements. Such a structure will vary depending on the nature and extent of risks in the outsourcing arrangements. As relationships and interdependencies in respect of outsourcing arrangements increase in materiality and complexity, a more rigorous risk management approach shall be adopted. The institution must be more proactive in its relationship with the service provider (e.g., having frequent meetings) to ensure that performance, operational, internal control and risk management standards are upheld.

The regulated institution shall put in place all the following measures for effective monitoring and control of any material outsourcing arrangement:

- 1° Maintain a register of all material outsourcing arrangements and ensure that the register is readily accessible for review by the board and senior management of the institution. The register shall be updated promptly and form part of the oversight and governance reviews undertaken by the board and senior management of the institution;
- 2° Establish multi-disciplinary outsourcing management groups with members from different risk and internal control functions including legal, compliance and finance, to ensure that all relevant technical issues and legal and regulatory requirements are met. The institution shall allocate sufficient resources, in terms of both time and skilled manpower, to the management groups to enable its staff to adequately plan and oversee the entire outsourcing lifecycle;

- 3° Establish outsourcing management control groups to monitor and control the outsourced service on an ongoing basis. There must be policies and procedures to monitor service delivery and the confidentiality and security of non-public data, For the purpose of gauging ongoing compliance with agreed service levels and the viability of the institution's operations. Such monitoring shall be regular and validated through the review of reports by auditors of the service provider or audits commissioned by the institution;
- 4° Periodic reviews, at least on an annual basis, on all material outsourcing arrangements. This is to ensure that the institution's outsourcing risk management policies and procedures, and this regulation, are effectively implemented. Such reviews shall ascertain the adequacy of internal risk management and management information systems established by the institution (e.g., assessing the effectiveness of processes and metrics used to evaluate the performance and security of the service provider) and highlight any deficiency in the regulated institution's systems of control;
- 5° Reporting: Reports on the monitoring and control activities of the institution shall be reviewed by its senior management and provided to the board for information. The regulated institution must ensure that monitoring metrics and performance data are not aggregated with those belonging to other customers of the service provider. The regulated institution shall also ensure that any adverse development arising in any outsourcing arrangement is brought to the attention of the senior management of the institution and service provider, or to the institution's board, where warranted, on a timely basis. When adverse development occurs, prompt actions must be taken by the institution to review the outsourcing relationship for modification or termination of the agreement;
- 6° Perform comprehensive pre and post-implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements. If an outsourcing arrangement is materially amended, a comprehensive due diligence of the outsourcing arrangement must also be conducted.

Article 17 – Audit and inspection

The regulated institution's outsourcing arrangements must not interfere with the ability of the institution to effectively manage its business activities or impede Supervisory authority in carrying out its supervisory functions and objectives.

The regulated institution shall include, in all its outsourcing agreements for material outsourcing arrangements, clauses that:

- 1° allow the regulated institution to conduct audits on the service provider and its sub-outsourcing whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its sub-outsourcing, whether produced by the service provider's or its sub-outsourcing internal or external auditors, or by agents appointed by the service provider in relation to the outsourcing arrangement;
- 2° allow Supervisory Authority, or any agent appointed by Supervisory Authority, where necessary or expedient, to exercise the contractual rights of the institution to:
 - a. access and inspect the service provider and its sub-outsourcing, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-outsourcing;
 - b. access any report and finding made on the service provider and its sub-outsourcing, whether produced by the service provider's and its sub-outsourcing' internal or external auditors, or by agents appointed by the service provider and its sub-outsourcing, in relation to the outsourcing arrangement.

Outsourcing agreements for material outsourcing arrangements shall also include clauses that require the service provider to comply, as soon as possible, with any request from Supervisory authority to the service provider or its sub-outsourcing, to submit any reports on the security and control environment of the service provider and its sub-outsourcing to Supervisory Authority, in relation to the outsourcing arrangement.

The regulated institution shall ensure that these expectations are met in its outsourcing arrangements with the service provider as well as any sub-outsourcing that the service provider may engage in the outsourcing

arrangement, including any disaster recovery and backup service providers. The Supervisory Authority will provide the institution reasonable notice of its intent to exercise its inspection rights and share its findings with the institution where appropriate.

The regulated institution shall ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the institution shall consider the nature and extent of risk and impact to the institution from the outsourcing arrangements. The scope of the audits and expert assessments shall include an assessment of the service providers' and its sub-outsourcing' security and control environment, incident management process (for material breaches, service disruptions or other material issues) and the institution's observance of this regulation in relation to the outsourcing arrangement.

The independent audit and/or expert assessment on the service provider and its sub-outsourcing may be performed by the institution's qualified internal or external auditors, the service provider's external auditors or by agents appointed by the institution. The appointed persons must possess the requisite knowledge and skills to perform the engagement, and be independent of the unit or function performing the outsourcing arrangement. Senior management shall ensure that appropriate and timely remedial actions are taken to address the audit findings. The regulated institution and the service providers shall have adequate processes in place to ensure that remedial actions are satisfactorily completed. Actions taken by the service provider to address the audit findings shall be appropriately validated by the regulated institution before closure. Where necessary, the relevant persons who possess the requisite knowledge and skills shall be involved to validate the effectiveness of the security and control measures taken.

Significant issues and concerns must be brought to the attention of the senior management of the institution and service provider, or to the institution's board, where warranted, on a timely basis. Actions shall be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the institution's risk tolerance.

Copies of audit reports shall be submitted by the institution to Supervisory Authority on quarterly basis. The regulated institution shall also, upon request, provide Supervisory Authority with other reports or information on the institution and service provider that is related to the outsourcing arrangement.

Article 18 – Outsourcing outside Rwanda

The engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in a foreign country, may expose an institution to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the regulated institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, the institution shall take into account, as part of its due diligence, and on a continuous basis:

- 1° government policies;
- 2° political, social, economic conditions;
- 3° legal and regulatory developments in the foreign country;
- 4° the institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.

The regulated institution must also be aware of the disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. As information and data could be moved to primary or backup sites located in foreign countries, the risks associated with the medium of transport, be it physical or electronic, shall be considered.

Material outsourcing arrangements with service providers located outside Rwanda must be conducted in a manner so as not to hinder Supervisory Authority's efforts to supervise the Rwanda business activities of the institution (i.e., from its books, accounts and documents) in a timely manner, in particular:

- 1° The institution shall, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements;

- 2° A regulated institution shall not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by Supervisory Authority or agents appointed by Supervisory Authority to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions. A regulated institution must at least commit to retrieve information readily from the service provider should Supervisory Authority request for such information;
- 3° The regulated institution shall ensure that all licenses of any system or application are maintained and are in the names of the regulated institution;
- 4° The regulated institution shall demonstrate that any information or systems can be easily transferred or separated from a centralized system even in case where outsourced services are performed by a group;
- 5° a regulated institution shall also demonstrate that outsourcing outside Rwanda guarantee the continuation of service provision in case a regulated institution is put into resolution or under liquidation;

The regulated institution shall notify Supervisory Authority if any overseas authority seeks access to its non-public data or if a situation were to arise where the rights of access of the institution and Supervisory Authority have been restricted or denied.

Article 19 – Outsourcing within a group

This Regulation is applicable to outsourcing arrangements with parties within the group. The expectations may be addressed within group-wide risk management policies and procedures. A regulated institution is expected to provide, when requested, information demonstrating the structure and processes by which its board and senior management discharge their role in the oversight and management of outsourcing risks on a group-wide basis.

Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects of the service provider's ability to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, audit and inspection, including confirmation on the right of access to be provided to Supervisory authority, to retain effective supervision over the institution, and compliance with local regulatory standards. The respective roles and responsibilities of each office in the outsourcing arrangement shall be documented in writing in a service level agreement or an equivalent document.

Outsourcing within the group outside Rwanda shall follow the requirements of outsourcing outside Rwanda as provided for by this Regulation

The Supervisory Authority may issue a directive governing the shared services arrangements.

Article 20 – Cloud Computing

The Supervisory Authority considers cloud services operated by service providers as a form of outsourcing and recognizes that regulated institutions may leverage on such a service to enhance their operations and service efficiency while reaping the benefits of Cloud services' scalable, standardized and secured infrastructure. In this regard, Cloud services providers selected by a regulated institution must have implemented strong authentication, access controls, and tokenization techniques and data encryption security to meet institution's requirements. The encryption key should be retained by the regulated institution;

The regulated institution shall perform the necessary due diligence and apply sound governance and risk management practices articulated in this regulation when subscribing to Cloud services.

The regulated institution shall be aware of cloud services' typical characteristics such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, regulated institution must take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, the institution shall ensure that the service provider possesses the ability to clearly identify and segregate non public data using strong physical or logical controls.

The service provider shall have in place robust access controls to protect non public data and such access controls should survive the tenure of the contract of the cloud services.

The regulated institution shall be ultimately responsible and accountable for maintaining oversight of Cloud services and managing the attendant risks of adopting Cloud services, as in any other form of outsourcing arrangements. A risk-based approach shall be taken by regulated institution to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the Cloud services.

The Supervisory Authority may issue specific requirement for cloud computing services.

Chapter III

Requirements for outsourcing material activities

Article 21 – Application to outsource material activities

A regulated institution that intends to outsource material activities shall obtain approval from the Supervisory authority. A prior approval of the Supervisory Authority is necessary to contract, modify or extend a material outsourcing arrangement.

The regulated institution shall submit a duly filled application form to outsource a material activity.

The application shall include documents and information specified hereafter:

- 1° outsourcing contract draft, containing the elements defined in this regulation, which the regulated institution intends to conclude with the service provider;
- 2° a statement certifying that the outsourcing arrangement has been approved in accordance with the regulated institution's outsourcing policies;
- 3° details of the activities to be outsourced as well as the rationale for the outsourcing;
- 4° list of persons related to the institution, who are at the same time related to the service provider, and a description of the manner in which they are related;
- 5° service provider's audited reports for the previous calendar year;
- 6° proof of the service provider's former experience related to the activities subject of outsourcing;
- 7° proof of the financial soundness of the service provider;
- 8° description of the obligations and responsibilities of the departments or employees in charge of the supervision and managing the contractual relationship with the service provider;
- 9° an analysis of the key risks involved in the outsourcing arrangement and the risk mitigation strategies to address these risks;
- 10° the institution exit strategy;
- 11° detailed description of technical and organizational solutions enabling safe and good quality performance of the activities planned to be outsourced, including a description of the manner of protection of confidentiality, availability and integrity of data;
- 12° the institution statement that the management do not have direct or indirect interest with the service provider, except in the case of parent related service provider is it a parent company;
- 13° Any information deemed necessary for the Supervisory Authority to assess the application.

Article 22 – Approval for outsourcing of material activities

Upon receipt of an application to outsource material activities and supporting documents, the Supervisory authority shall, within (10) ten working days, send the applicant a letter of acknowledgment or a letter of deficiency as the case may be.

A letter of acknowledgement shall constitute official notice that the documents submitted were deemed complete and that no further information is required for processing the analysis of the application.

A letter of deficiency shall outline deficiencies in the application and shall provide a deadline for rectification of the deficiencies and for providing additional information that may be deemed necessary by the Supervisory authority.

No further action shall be taken by the Supervisory authority unless the deficiencies are rectified within the period prescribed, and the Supervisory authority is satisfied about the information received.

Article 23 – Supervisory Authority’s decision

The Supervisory Authority shall, within (1) one month after signing the letter of acknowledgement that confirms that the information is complete, prepare a report in respect of each application.

The report shall indicate the decision of the Supervisory Authority to:

- 1° approve the outsourcing of the material activities, if it is satisfied that the application satisfies the requirements in this regulation;
- 2° rejection of outsourcing of the material activities in a given application, stating the grounds upon which it is based.

The Supervisory Authority shall inform the applicant, in writing, of its decision to approve or not the outsourcing of the material activities that the institution applied for.

Chapter IV Miscellaneous and final provisions

Article 24 – Involvement of Supervisory Authority in outsourcing arrangement

The regulated institution shall be ready to demonstrate to the Supervisory Authority its observance of this regulation by submission of its outsourcing register at least annually or upon request. The annual register shall be submitted as per the appendix 2 of this regulation within (15) fifteen days after the end of the year.

Where the Supervisory Authority is not satisfied with the regulated institution’s observance of this regulation, the Supervisory Authority may require the institution to take additional measures to address the deficiencies noted.

The Supervisory Authority may also take such non-compliance into account in its assessment of the regulated institution, depending on the potential impact of the outsourcing on the regulated institution and the financial system, severity of the deficiencies noted, the regulated institution’s track record in internal controls and risk management, and also on the circumstances of the case.

The Supervisory Authority may directly communicate with the home or host regulators of the regulated institution and the regulated institution’s service provider, on their ability and willingness to cooperate with Supervisory Authority in supervising the outsourcing risks to the institution.

The Supervisory Authority reserve rights to require the regulated institution to modify, make alternative arrangements or re-integrate an outsourced service into the institution where one of the following circumstances arises:

- 1° the regulated institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the outsourcing arrangement;
- 2° the regulated institution fails or is unable to implement adequate measures to address the risks arising from its outsourcing arrangements in a satisfactory and timely manner;
- 3° adverse developments arise from the outsourcing arrangement that could impact the institution;

- 4° The supervisory authority powers over the institution and ability to carry out its supervisory functions in respect of the institution's services are hindered;
- 5° The security and confidentiality of the institution's data is lowered due to changes in the control environment of the service provider.

The regulated institution shall notify Supervisory Authority as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the regulated institution. Such adverse developments include any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the nonpublic data. The regulated institution shall also notify Supervisory Authority of such adverse development encountered within the regulated institution's group. This shall be done as soon as possible but not in a period of later than (24) twenty-four hours from the time the institution is aware of these adverse developments.

Article 25 – Examples of outsourcing arrangements

Annex 1 provides some examples of outsourcing arrangements to which this regulation applies and arrangements to which it does not.

It should not be misconstrued that arrangements not defined as outsourcing need not be subject to adequate risk management and sound internal controls by the regulated institution.

Article 26 – Compliance landscape

A regulated institution shall consider all their specific regulators when considering outsourcing arrangements in order to ensure compliance.

A regulated institution shall be aware that, apart from local legislative requirements, regulators in other jurisdictions may impose additional requirements on the regulated institution

Article 27 – Application of other laws

In addition to the provisions of this regulation, a regulated institution shall abide with other legal and regulatory requirements notably those applicable to cybersecurity and data protection and privacy.

Article 28 – Penalties and administrative sanctions

Where a regulated institution fails to satisfy any of the requirements of this Regulation the Supervisory Authority may apply any sanctions available under relevant provisions of the Law /or provisions of a relevant regulation.

Article 29 – Transitional provisions

The regulated institution shall assess the materiality of all outsourced agreements prior to the time of the publication of this regulation, and shall seek approval of the Supervisory Authority to continue outsourcing these activities within 6 months after this regulation comes into force.

Article 30 – Repealing provisions

Regulation N° 03/2018 of 24/01/2018 on outsourcing and all previous provisions contrary to this Regulation are hereby repealed.

Article 31 – Drafting, consideration and approval of this regulation

This Regulation was drafted, considered and approved in English.

Article 32 – Commencement

This regulation shall come into force on the date of its publication in the Official *Gazette* of the Republic of Rwanda.

Appendix I

Examples of outsourcing arrangements

1. The following are examples of some services that, when performed by a third party, would be regarded as outsourcing arrangements for the purposes of this regulation although they are not exhaustive:
 - a. application processing (e.g., loan origination, credit cards);
 - b. cash processing and transportation;
 - c. business continuity and disaster recovery functions and activities;
 - d. claims administration (e.g., loan negotiations, loan processing, collateral management, collection of bad loans);
 - e. document processing (e.g., cheques, credit card and bill payments, bank statements, other corporate payments, customer statement printing);
 - f. information systems hosting (e.g., software-as-a-service, platform-as-a-service, infrastructure-as-a-service);
 - g. information systems management and maintenance (e.g., data entry and processing, data centres, data centre facilities management, end-user support, local area networks management, help desks, information technology security operations);
 - h. manpower management(e.g., benefits and compensation administration, staff appointment, training, and development);
 - i. management of policy issuance and claims operations;
 - j. professional services related to the business activities of the institution (e.g., accounting, internal audit, actuarial, compliance);
 - k. marketing and research (e.g., product development, data warehousing and mining, media relations, call centres, telemarketing);
 - l. support services related to archival, storage and destruction of data and records.
2. The following arrangements would generally not be considered outsourcing arrangements:
 - a. Arrangements in which certain industry characteristics require the use of third-party providers
 - b. telecommunication services and public utilities (e.g., electricity, SMS gateway services);
 - c. postal services;
 - d. common network infrastructure (e.g., Visa, MasterCard, etc);
 - e. clearing and settlement arrangements between clearing houses and settlement institutions and their members, and similar arrangements between members and non-members;
 - f. global financial messaging infrastructure which are subject to oversight by relevant regulators (e.g., SWIFT); and
 - g. correspondent banking services.

- h. Introducer arrangements and arrangements that pertain to principal-agent relationships:
 - i. sale of insurance policies by agents, and ancillary services relating to those sales;
 - ii. acceptance of business by underwriting agents; and
 - iii. introducer arrangements (where the institution does not have any contractual relationship with customers).
- i. Arrangements that the regulated institution is not legally or administratively able to provide
- j. statutory audit and independent audit or assessments;
- k. discreet advisory services(e.g., legal opinions, independent appraisals, trustees in bankruptcy, loss adjuster);
- l. independent consulting(e.g., consultancy services for areas which the institution does not have the internal expertise to conduct)

Appendix II

Register of the outsourced activities/services

| Name of the service provider | Outsourced service | Indicate whether material to the institution | Short description of the arrangement | Country from which service is provided | Commencement date of the arrangement and expiry date | The total value of the arrangement (FRW/USD) | Estimated spending amount per month (in FRW/USD) | Estimated spending amount per year (in FRW/USD) |
|------------------------------|--------------------|--|--------------------------------------|--|--|--|--|---|
| | | | | | | | | |
| | | | | | | | | |