National Bank of Rwanda
Banki Nkuru y'u Rwanda

KN 6 Av.4/P.O. Box 531 Kigali-Rwanda
Tel: (+250) 788199000 /
Website: www.bnr.rw /
E-mail: info@bnr.rw /
Swiftcode: BNRWRWRW /
Twitter: @CentralBankRw

The Governor

DIRECTIVE Nº 4230/2024-00038 [613] OF 17th/01/2024 ON CHANGE MANAGEMENT OF SYSTEMS IN REGULATED INSTITUTIONS

The National Bank of Rwanda;

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

Pursuant to Law nº 072/2021 of 05/11/2021 governing deposit-taking microfinance institutions, especially in Articles 23 and 24;

Pursuant to Law nº 47/2017 of 23/09/2017 governing the organization of banking, especially in Articles 37 and 117;

Pursuant to Law n° 061/2021 of 14/10/2021 governing payment system, especially in Article 6;;

Pursuant to Law n° 030/2021 of 30/06/2021 governing the organization of insurance business, especially in Articles 56, 58, 60 and 82;

Pursuant to Law N° 05/2015 of 30/03/2015 governing the organization of pension schemes especially in Article 3;

Pursuant to the Law nº 73/2018 of 31/08/2018 governing credit reporting system, especially in Articles 11,12,18 and 23;

Reference to Regulation no 43/2022 of 02/06/2022 governing business continuity management and operational resilience for regulated institutions, especially articles 33,34 and 40;

Following the increased dependence on technology, coupled with an accelerated pace of change that has led to a rise in operational incidents across Regulated Institutions;

Considering a need for assessing any change to an existing system, new systems, and applications before their acquisition or implementation to ensure adequate security measures and integrity of these systems or products;

Having realized that the financial system needs an approach to operational risk and resilience that includes preventative measures and capabilities in terms of people, processes, technology, and organizational culture to recover and adapt when disruptions occur;

ISSUES THE FOLLOWING DIRECTIVE:

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Directive

(1) This directive provides guidance to regulated institutions on the changes to information processing facilities and to controlled systems to ensure that the business objectives continue to be met following the change.
(2) It also sets modalities enabling the regulated institution to minimize business impact, losses, and incidents that are a result of implementing changes.

Article 2: Interpretation

In this Directive:

(a) "Central Bank" means the National Bank of Rwanda;

(b) "Regulated Institution (RI)" means the institution regulated and supervised by the Central Bank, namely banks, insurers, deposit-taking microfinance institutions, payment system operators, payment service providers, credit reporting operators, and other institutions that the Central Bank may subject to this Directive;

(c) "Change Advisory Board (CAB)" means a committee established at the management level to oversee and manage the change management process.

Article 3: Scope of application

This directive applies to Regulated Institutions as defined in this Directive. It covers changes to ICT systems and applications that are essential for everyday operations, which could cause a disruption leading to failure of product or service delivery to customers or cause financial and/or reputational damage.

CHAPTER II: CHANGE MANAGEMENT GOVERNANCE

Article 4: Required policies and procedures for managing changes

(1) A RI must have formal policies and procedures for managing changes to its systems and applications that support delivering financial services or products.

(2) The policies and procedures must define the change management process, including categorization of changes as minor, major, and critical; assessment of changes and criteria for categorizing changes; to ensure consistent evaluation and appropriate prioritization.

Article 5: Categories of changes

The categories of changes in the management of a RI are the following:

(a) minor changes;
(b) major changes;
(c) critical changes; and
(d) emergency changes.

Article 6: Criteria for categorizing the changes

(1) The corresponding criteria for each category of changes referred to in Article 5 of this directive are the following:

(a) Minor changes: for this directive, they are changes that typically have a low impact on the RI's operations, systems, and services. They may include –

(i) software patches or updates that address minor bugs or security vulnerabilities;

(ii) configuration changes to individual user accounts or preferences; and

(iii) routine maintenance activities that have minimal impact on service availability.

(b) Major changes: these have a moderate level of impact on the RI and require careful planning and evaluation at the senior management level. They may include but are not limited to:

(i) implementation of new operations software or systems;

(ii) infrastructure upgrades or migrations on none core business operations system;

(iii) modifications to existing systems or applications that may cause a system downtime; and

(iv) implementation of security measures to address emerging threats or vulnerabilities.

(c) critical changes: These are changes that have a high potential for significant impact on the RI's operations, security, or regulatory compliance. They often require extensive testing, approval, and risk mitigation measures. They include –

(i) System upgrades or replacements that may involve downtime of critical business operations or affect multiple departments;

(ii) changes to core systems or critical financial applications; and

(iii) changes that may cause noncompliance with regulatory procedures or reporting requirements.

(d) emergency changes: These are typically those that need to be implemented urgently to address critical issues or to prevent severe disruptions to the system or service. These changes are typically unplanned and are initiated to resolve emergencies that pose immediate risks to the business or its operations. Proper change management processes for emergency changes shall be in place to be followed, to ensure documentation, testing, and communication take place to minimize risks and prevent potential adverse impacts.

(2) A RI must adapt the criteria referred to in Paragraph (1) of this Article to their specific needs and risk profiles by clearly defining and providing specific examples for each category.

(3) A RI can accurately assess the impact and prioritize change requests, to ensure effective change management practices.

Article 7: Change Advisory Board (CAB) and its role

(1) A RI establishes a CAB to oversee and manage the change management process. The CAB is composed of a senior management team from various business functions, including business lines, IT, operations, risk management, compliance, and legal.

(2) The CAB reviews, evaluates and asses the risk, impact and approves or rejects a proposed change.

(3) The CAB can make special invitations internally or externally for subject matter experts if needed while reviewing the change.

Article 8: Change approval

(1) The minor changes can be approved as per the institutional policies and procedures however; they shall not violate any regulatory compliance requirements.

(2) The major changes undergo the internal change management policy and procedure and gain CAB approval. The RI shall notify the Central Bank within 10 working days before the change implementation with the template attached in the annex.

(3) The critical changes must seek approval from the CAB, and board of directors, and be notified to the Central Bank before implementation.

(4) For major Emergency changes, the RI shall notify the Central Bank with the change description and the justification of urgency.

(5) For the changes that require notification to the Central Bank, the RI must include in the request document the following–

(a) a change notification file including the change approvals by the RI

(b) the change description including the design and documentation;

(c) change assessment including impact, risk and mitigations, implementation plan; and

(d) a rollback plan including the maximum tolerable downtime that, once reached, the rollback plan is triggered.

(6) The Central Bank reserves the right to request further documentation or presentation that may be found necessary.

(7) Conversely, for changes requiring notification to the Central Bank, the latter will only respond if the proposed change poses operational, financial, legal, or reputational risks.

Article 9: Planning and execution of changes

A RI develops a detailed plan for implementing changes, including a timeline, resource requirements, and contingency plans. All changes are executed in a controlled manner and thoroughly tested before implementation.

Article 10: Risk assessment and mitigation

(1) A RI conducts a risk assessment for all change requests to systems and applications. Before implementing any changes, an impact assessment is conducted to identify potential risks, dependencies, and required resources. This includes assessing the impact on systems, data, processes, personnel, and assessment of returns on investment.

(2) The risk assessment considers factors such as the nature and complexity of the change, the criticality of the systems, the potential for system downtime where applicable, and the likelihood of security breaches, fraud, and data or financial losses.

(3) RI implements appropriate risk mitigation measures to minimize the impact of potential risks associated with the change.

Article 11: Steps of conducting a risk assessment

(1) The following are the guiding principles for conducting a detailed risk assessment:

(a) identification of potential risks;

(b) evaluation of the impact;

(c) assessment of the likelihood or probability of risk occurrence;

(d) risk mitigation strategies; and

(e) monitoring and review of the risk landscape.

(2) The management of an RI is accountable for the risk management It may accept the risk assessment performed or may reject it and ask for re-assessment.

Article 12: Identification of potential risks

(1) A RI considers both internal and external risks, including operational, financial, legal, and reputational risks.

(2) A RI identifies the potential risks associated with the specific change, such as system failures, data breaches, service disruptions, financial and data losses or non-compliance with regulatory requirements.

(3) A RI pays particular attention to third-party dependencies, as changes in their systems or services can have a direct impact on the institution.

(4) A RI ensures that all critical dependencies are known, and Service Level Agreement(SLA)'s defined in the contract.

(5) The change management process on the dependencies, the third-party/vendor shall inform the RI of the change, and the RI shall ensure SLAs are not breached in the change process.

Article 13: Evaluation of the impact

(1) A RI determines the potential impact of each identified risk on the institution's operations, customers, financial stability, and reputation and provides a business impact analysis report.

(2) A RI considers the potential cascading effects of changes, such as how a change in one system or process may affect other interconnected systems or departments.

Article 14: Assessments of likelihood and probability of risk occurrence

(1) A RI assesses the likelihood or probability of each risk occurring, considering historical data, industry trends, and expert opinions.

(2) A RI considers the potential frequency and persistence of risks associated with the change.

Article 15: Risk mitigation strategies

(1) A RI develops a comprehensive plan to mitigate identified risks. This may include preventive measures, such as implementing security controls or redundancy systems, as well as contingency plans to minimize the impact of risks if they occur.

(2) A RI considers the involvement of relevant stakeholders, including third-party sellers or service providers, in the risk mitigation process.

(3) A RI considers walk-around plans that can keep service delivery at acceptable levels in case of automated process failure.

Article 16: Monitoring and review of the risk landscape

(1) A RI establishes mechanisms to monitor the effectiveness of risk mitigation measures and to detect any emerging risks or changes in the risk landscape.

(2) A RI regularly reviews and updates risk assessments as new information becomes available or as changes in the institution's environment occur.

(3) A RI conducts more comprehensive risk assessments that consider third-party dependencies and potential cascading effects. This enables the RI to proactively identify and mitigate risks associated with changes, ensuring the smooth implementation of changes while safeguarding the institution and its stakeholders.

Article 17: Testing and deployment of changes

(1) A RI conducts rigorous testing of all changes before deploying them to the production environment. Testing includes functional testing and non-functional testing, performance testing, security testing, System Integration Testing (SITs), and User Acceptance Testing (UATs).

(2) Once the changes are deployed, it is essential to monitor the system closely to ensure that it is functioning as expected and that there are no new issues or disruptions. To ensure the successful and reliable deployment of changes, it is essential to have a test environment that closely resembles the production environment. This helps minimize discrepancies and potential issues.

Article 18: Considerations in case of deployment of changes

The following are the key considerations to ensure reliable deployment of changes:

(a) test environment;

(b) test scenarios;
(c) regression testing;
(d) load and performance testing;
(e) User Acceptance Testing (UAT);
(f) deployment.

Article 19: Test environment of change

(1) A RI establishes a dedicated test environment that mirrors the production environment as closely as possible in terms of hardware, software configurations, network setup, and data.

(2) A RI ensures that the test environment accurately represents the various components and dependencies of the production environment to identify any compatibility or integration issues.

(3) The test environment must have similar infrastructure, operating systems, databases, and security measures to ensure comprehensive testing.

(4) The approach of a test environment enhances the reliability and effectiveness of testing, increasing the likelihood of successful change implementation while reducing the risk of unexpected complications or disruptions.

(5) The test environment shall be segregated from the production environment, only accessible by authorized personnel, and data privacy measures should be in place in case of true/unmasked or unencrypted institution data is being used.

Article 20: Test scenarios of change

(1) A RI develops test scenarios that cover a wide range of potential use cases and scenarios.

(2) A RI tests the changes in various conditions and configurations to validate their functionality, performance, and interoperability with existing systems.

(3) A RI includes both positive and negative test cases to ensure the changes can handle expected inputs and identify potential vulnerabilities or weaknesses.

(4) A RI ensures that system integration testing is carried out with end-to-end case tests to ensure that systems are well integrated and tested with all third parties where applicable.

Article 21: Regression testing of change

A RI conducts regression testing to verify that the changes do not adversely impact existing functionalities and systems.

Article 22: Load and performance testing

(1) A RI performs load and performance testing to assess how the changes perform under anticipated workload and stress conditions where applicable.

(2) A RI identifies any bottlenecks, scalability issues, or performance degradation that may arise from the changes.

Article 23: User Acceptance Testing of Change

(1) A RI involves end-users or representatives from different departments in the User Acceptance Testing (UAT) process to validate the changes from their perspective.

(2) The RI gathers feedback and addresses any issues or concerns raised during the UAT phase.

Article 24: Deployment of the change

(1) A RI prioritizes a well-defined deployment plan that outlines the steps, dependencies, and rollback procedures if needed.
(2) A RI schedules deployment during low-impact periods to minimize disruption to regular operations.

(3) A RI implements proper change control and version management procedures to ensure the correct deployment of changes.

(4) Where the change is to be applied on a critical system and data migration or data integrity shall be affected, an RI shall involve external auditors in data validation and approval both before and after migration.

Article 25: Rollback plan

(1) The rollback plan clearly defines the criteria or triggers that would necessitate the implementation of the rollback plan, such as critical system failures, data corruption, or severe disruptions to operations.

(2) A RI ensures that the rollback plan includes specific instructions for each component or system affected by the changes, detailing the necessary actions to bring them back to the pre-change state with technical or procedural aspects.

(3) The Plan indicates the personnel with the authority to initiate a rollback.

(4) The plan also highlights the communication strategies for notifying stakeholders about the rollback.

(5) The RI ensures that there are testing procedures to ensure the system returns to its previous state properly and Verification steps to confirm that the rollback was successful.

(6) A RI ensures that there is a rollback procedure in place to guide the rollback implementation.

Article 26: Rollback procedure

(1) A RI establishes a detailed rollback procedure in case of any unexpected issues that arise during or after deployment.

(2) A RI establishes emergency and contingency procedures to address unexpected events that may arise during or after the change implementation process as part of the procedure.

(3) A RI also establishes clear fallback procedures to revert to the previous system state in case of any issues or incidents and these include;

(a) Exact commands or actions to be taken to uninstall updates, configurations, or changes.

(b) Specific files or settings that need to be restored.
(c) Order of operations to ensure dependencies are managed correctly.
(d) Checkpoints or validation points to ensure the rollback progresses smoothly.
(e) Potential troubleshooting steps if any issues arise during the rollback

Article 27: Considerations for a rollback plan

For the effectiveness of testing and validation of the rollback plan, the following are the key points to consider:

(a) test and validate the rollback plan;
(b) resources and responsibilities;
(c) communication and documentation;
(d) post-rollback validation.

Article 28: Test and validate the rollback plan

The steps for testing and validating the rollback plan are the following:

(a) it is crucial to test and validate the rollback plan before actual implementation.

(b) set up a dedicated test environment to simulate the production environment and perform test rollbacks.

(c) execute the rollback plan in the test environment to verify its effectiveness and identify any potential issues or gaps.

(d) incorporate lessons learned from the testing phase to refine and enhance the rollback plan as needed.

Article 29: Resources and Responsibilities

(1) A RI clearly defines the roles and responsibilities of individuals or teams involved in executing the rollback plan.

(2) A RI ensures that the necessary resources, including personnel, tools, and documentation, are readily available to facilitate a smooth and efficient rollback process.

Article 30: Communication and documentation

(1) A RI establishes a clear communication plan to notify relevant stakeholders, including IT staff, management, and end-users, about the potential rollback and its impact.

(2) A RI documents all steps, actions, and decisions taken during the rollback process to facilitate post-implementation analysis and future reference.

(3) A RI notifies the Central Bank of the rollback plan to be activated for critical and major changes as in this directive.

Article 31: Post-rollback validation

(1) After the rollback is complete, an RI conducts full validation to ensure that all systems, processes, and data have been successfully restored to their pre-change state.

(2) A RI performs testing and monitoring to verify that the rollback has resolved the issues or complications encountered during the initial change implementation.

(3) A RI can enhance its preparedness and confidence in handling unexpected issues to ensure that the rollback plan is well-tested, effective, and can be executed smoothly when required, minimizing the impact of adverse events and facilitating a swift recovery to normal operations.

CHAPTER III: ENGAGEMENT OF USERS

Article 32: Awareness and training on the change management

A RI ensures user engagement and awareness are critical components of effective change management processes. This is done by ensuring the following:

(a) user acceptance;
(b) user feedback;
(c) training and support;
(d) communication;
(e) resistance to change; and
(f) specific considerations for alternate delivery channels.

Article 33: User acceptance

The end-users are the ones who will ultimately use the systems or processes impacted by the change. Engaging them in the change management process helps to increase their acceptance and buy-in of the changes being made.

Article 34: User feedback

The end-users can provide valuable feedback during the change management process. They can help identify potential issues with the changes being made, suggest improvements, and refine the change management process.

Article 35: Training and support

The act of engaging end-users in the change management process ensures that they are properly trained and supported during the transition. This helps to minimize disruptions and errors during the change implementation.

Article 36: Communication with internal stakeholders

A RI shall engage internal stakeholders in the change management process to ensure that they are properly informed about the changes being made, the reasons behind the changes, and how they are impacted. This helps to reduce confusion and increase transparency.

Article 37: Specific considerations for alternate delivery channels and digital services

A RI considers the unique characteristics and risks associated with alternate delivery channels, such as digital services, when implementing change management practices. The changes to channels may require additional security measures to prevent fraud, while changes to mobile banking may require additional testing to ensure compatibility with various mobile devices and operating systems.

CHAPTER IV: IMPLEMENTATION OF CHANGE MANAGEMENT

Article 38: Change management and documentation tool

(1) A RI implements a change management and documentation tool. This tool provides automation features such as workflows, notifications, and approvals, which can help to streamline the change process and reduce manual intervention.

(2) Automation helps to reduce the time and effort required to manage changes, which can lead to increased productivity and reduced costs. This is crucial for institutions that want to manage all changes to systems and applications in a structured, systematic, and controlled manner and helps to improve collaboration, communication, accountability, transparency, efficiency, and effectiveness, which can lead to better outcomes and reduced risks.

Article 39: Additional requirements

All changes to business applications implemented in the production environment are governed by a formal documented process that includes necessary change details. The process defines the roles and responsibilities of stakeholders involved in the change management process, such as developers, testers, business analysts, and operations personnel.

Article 40: Change management framework

The changes follow a formal change management framework chosen by the institution, but at a minimum, it must possess the following components:

(a) authorization of changes;
(b) communication of changes;
(c) testing and acceptance of tests for changes;
(d) changes, including deployment plans;
(e) maintaining records of changes;
(f) operating documentation and user procedures;
(g) business continuity plans and response and recovery procedures;
(h) audit trails for its business applications.

Article 41: Authorization of changes

The changes are authorized by designated personnel, and approval is obtained before making any changes to the production environment.

Article 42: Communication of changes

The changes are communicated to all relevant interested parties, such as business users, customers, internal, and external stakeholders, in a timely and effective manner.

Article 43: Implementation of changes and deployment plans

The changes are implemented by a defined deployment plan that includes a schedule, resources, and contingency plans.

Article 44: Maintaining records of changes

A RI maintains a record of all changes made including the change details, approval, risk assessment, testing, implementation, and post-implementation review in line with the Institution's policies and procedures and applicable regulatory requirements.

However, documentation on critical changes shall minimally be kept for (5) five years.

A RI maintains audit trails for systems data and system configurations in the process of implementation of changes.

Article 45: Ensuring operating documentation and user procedures

A RI ensures that operating documentation and user procedures are updated immediately after a change occurs or as necessary to remain appropriate to reflect changes in the systems and applications.

Article 46: Ensuring business continuity plans, response, and recovery procedures

The RI ensures that business continuity plans, response, and recovery procedures are updated immediately after a change occurs on systems and applications to reflect on improvements or lessons learned from any incidents during the change implementation.

Article 47: Post-implementation review

(1) A RI institution conducts a post-implementation review of all changes to assess the effectiveness of the change management process and identify any areas for improvement.

(2) The review includes an analysis of the change's impact, any issues or incidents that occurred during or after deployment, and feedback from stakeholders.

(3) A RI carries out a continuous improvement plan to address any issues that arise post-implementation. This ensures that the system remains up-to-date and effective and that it continues to meet the evolving needs of the organization.

CHAPTER V: CONTROL OVER THE CHANGE MANAGEMENT AND ITS EVALUATION

Article 48: Control over the change management

(1) A RI is required to regularly evaluate the effectiveness of their change management controls and procedures. This assessment includes conducting user surveys at least once a year to gather feedback on the change management process.

(2) The results of the evaluation and user survey are documented in a report that summarizes any identified deficiencies and outlines a remediation plan.

(3) A RI, by regularly assessing its change management controls, can proactively identify areas for improvement and enhance its overall operational resilience.

Article 49: Metrics to be used when evaluating the control over the change management

(1) A RI shall put in place controls over the change management that is evaluated using the following metrics and the level of risk appetite and tolerance:

(a) change success rate metric; measures the percentage of changes that are implemented successfully without causing any adverse effects to the system or business processes

(b) change cycle time metric: measures the time it takes to complete a change from the initial request to the final implementation. A shorter cycle time may indicate more efficient and effective change management controls.

(c) change backlog: measures the number of pending changes that have not yet been implemented. A large backlog may indicate an ineffective change management process.

(d) change failure rate: measure the percentage of changes that fail to meet the expected outcomes or cause issues in the system or business processes. In addition, the number of disruptions and data errors caused by inaccurate change management process must be measured;

(e) user satisfaction measures the level of user satisfaction with the change management process, as reported through user surveys or feedback mechanisms.

(f) compliance rate metric: that measures the degree to which the change management controls and procedures comply with relevant laws, regulations, and industry standards

(g) percent of changes that follow formal change control processes: measures the percentage of changes that follow a formal change control process, as opposed to being implemented informally or without proper documentation

(h) applications, processes, or infrastructure rework caused by inadequate change management process: measures the number of reworks or modifications required due to inadequate change management process

(i) Service Level Agreements (SLAs): The RI tracks the SLA compliance and violations to determine the performance of change

(2) By tracking the metrics referred to in Paragraph (1) of this Article over time, a RI can gain insights into the strengths and weaknesses of their change management controls and procedures and make necessary improvements to enhance their overall effectiveness.

CHAPTER VI: MISCELLANEOUS AND FINAL PROVISION

Article 50: Service Level Agreements

The control over change management is crucial for RI to maintain stability, minimize disruptions, and effectively manage resources. Including specific provisions in Service Level Agreements (SLAs) for applications and systems like downtimes allowed or authorizations for the change can help to establish clear guidelines and expectations regarding the number of non-incident-related changes permitted for specific periods.

Therefore, the RI shall ensure that SLAs for all critical systems are defined and captured in contracts where systems depend on third-party service providers.

Article 51: Provisions to be included in SLA

The specific provisions to be included in SLAs tackle the following:

(a) maximum number of changes;
(b) change prioritization and approval process;
(c) review and adjustments;
(d) monitoring and reporting.

Article 52: Maximum number of changes

(1) The SLA defines the maximum number of non-incident-related changes allowed per year for each application or system covered by the SLA.
(2) A RI considers the capacity and resources of both the internal IT team and any involved third-party vendors or service providers when determining this limit. It takes into account the institution's risk appetite, operational capacity, and the impact that excessive changes may have on stability and performance.

Article 53: Change prioritization and approval process

(1) A RI establishes a process for evaluating and prioritizing change requests to ensure that the most critical changes are given priority while maintaining the established limit.

(2) A RI defines criteria for assessing the urgency, impact, and risk associated with each change request.

(3) A RI implements an approval mechanism that involves relevant stakeholders, including IT, business units, and third-party vendors, to ensure proper evaluation and decision-making.

Article 62: Review and adjustments

(1) A RI reviews periodically the established limit in light of changing business needs, technology advancements, or industry best practices.

(2) A RI considers conducting post-implementation reviews to evaluate the impact of changes and identify opportunities for improvement.

(3) A RI revises, if necessary, the maximum number of changes permitted per year based on the institution's evolving requirements and the lessons learned from previous change management experiences.

Article 63: Monitoring and reporting

(1) A RI puts in place a system to monitor and track the number of changes executed throughout the year, ensuring compliance with the policy and procedures.

(2) ARI generates regular reports on change activity, highlighting the number of changes performed, any exceptions to the limit, and the reasons for those exceptions. It shares these

reports with relevant stakeholders, including senior management and the parties involved in the SLA, to foster transparency and enable informed decision-making.

Article 64: Entry into force

This Directive comes into force on the date of its signature.

Done at Kigali on 22nd January 2024

Digitally
signed by
BNR(GOV
ERNOR)

RWANGOMBWA John
Governor

ANNEX TO THE DIRECTIVE Nº 4230/2024-00038 [613] OF 17/01/2024 ON CHANGE MANAGEMENT OF SYSTEMS IN REGULATED INSTITUTIONS

CHANGE MANAGEMENT REPORTING TEMPLATE TO THE CENTRAL BANK

Items	**Description**
Feasibility study/business case	
Change implementation plan	
Design and documentation	
Risk assessment & Business impact analysis documents	
Testing reports and sign offs	
Expected downtime	
CAB/CAC approval	
Board approval	
Rollback plan/strategy	
Rollback test report	

Seen to be annexed to the Directive Nº 4230/2024-00038 [613] of 17/01/2024 on change management of systems in regulated institutions

Done at Kigali on 22nd January 2024

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor