Rwanda

Regulation on Cyber Security in Regulated Institutions

Regulation 50 of 2022

Legislation as at 17 June 2022

FRBR URI: /akn/rw/act/reg/2022/50/eng@2022-06-17

Regulation on Cyber Security in Regulated Institutions
Contents

Rwanda

Regulation on Cyber Security in Regulated Institutions
Regulation 50 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 articles 6, 6bis, 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 articles 56, 57, 58, 60 and 82;

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

Law N° 061/2021 of 14/10/2021 governing the payment system, especially in its article 8;

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 the regulation N° 02/2018 of 24/01/2018 on cyber security;

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

Chapter One
General provisions

Article One – Purpose

The purpose of this regulation is to ensure that regulated institutions have resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the regulated institution's critical operations.

Article 2 – Scope

This Regulation shall apply to all regulated institutions unless provided otherwise by specific regulations or directives.

Article 3 – Definition of terms

In this regulation, the following words and expressions shall mean:

1° **a regulated institution**: any financial institution licensed and supervised by the Supervisory Authority;

2° **authorized user**: any employee, contractor, agent, or other person that participates in the business operations of a regulated institution and is authorized to access and use any Information Systems and non-public data of the regulated institution;

3° **Cyber incident**: A cyber event that:

a. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or

b. violates the security policies, security procedures or acceptable use policies,

Whether resulting from malicious activity or not.

4° **information system**: software, tools and equipment's for the production, storage or processing of data or information or management of data or information;

5° **multi-factor authentication**: authentication of a user's identity through the use and verification of at least two of the following types of identity factors:

a. knowledge factors, such as password, PIN;

b. possession factors, such as a card, token, text message on a mobile phone;

c. inherence factors, such as a user's biometrics.

6° **Nonpublic data**: all data that is not publicly available that is:

a. related to product and services of regulated institution or related statistics;

b. personal data as defined by specific laws

7° **penetration testing**: a test methodology in which assessors, using all available documentation and working under specific constraints, attempt to circumvent the security features of an information system

8° **publicly available information**: any information that a regulated institution has a reasonable basis to believe is lawfully made available to the general public;

9° **risk-based authentication**: any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

10° **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;

11° **Cyber security**: preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium;

12° **Cyber risk**: The combination of the probability of cyber incidents occurring and their impact;

13° **IT Infrastructure**: the hardware, software, network resources and services required for the existence, operation, and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and or customers and is usually internal to an organization and deployed within owned facilities;

14° **Threat profiles**: information about critical assets, threat actors, and details about how threat actors might attempt to compromise those critical assets;

15° **Threat modelling**: using a structured process to identify how critical assets might be compromised by a threat actor and why, what level of protection is needed for those critical assets, and what impact would be if that protection failed.

Chapter II
Regulatory requirements

Article 4 – Cyber security governance

Cyber security governance must be the responsibility of the Board of Directors and Senior Management.

A regulated institution must have a comprehensive cyber security governance framework consisting of the following:

1° cyber security strategy linked with business objectives;

2° governing security program that address each aspect of the strategy, controls and regulations;

3° a complete set of standards for each policy to ensure procedures and guidelines comply with the policy;

4° an effective organization structure void of conflict of interest with sufficient authority and adequate resources;

5° metrics and monitoring processes to ensure compliance, feedback on effectiveness and provide the basis for appropriate management decisions;

6° Adopt best practices that regulated institution should strive to attain globally accepted practices on information security management;

7° Develop crisis management practices, involving executive management and board of directors from pre-agreed thresholds onward;

8° Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed;

9° cyber risk management strategy that is incorporated into the overall business strategy and risk management of the institution.

Article 5 – IT Board Committee

Unless provided otherwise in a specific regulation, the Supervisory Authority may require or exempt a regulated institution to have IT Committee at the Board level depending on its nature of activity and complexity.

The IT Committee shall have the following powers and responsibilities:

1° give advice on strategic direction on IT and cyber security and to review IT investments on Board's behalf;

2° perform oversight functions over the IT steering committee (at a senior management level);

3° seek information from any employee;

4° obtain outside legal or professional advice;

5° secure attendance of outsiders with relevant expertise, if it considers necessary;

6° work in partnership with other board committees and senior management to provide input, review and amend the aligned corporate and IT strategies;

7° Ensure that internal and external auditors agree with the audit committee and management how information security should be covered in the audit;

8° inform the Board on an ongoing basis of the institution’s cyber risk exposure and risk management practices, including known and emerging threats and trends;

9° review the procedures for testing the effectiveness of the institution’s cyber security protocols and updating them as the threat landscape evolves;

The IT Committee members must be technically competent. At least one member must have substantial IT or cyber security expertise.

Article 6 – IT Steering Committee

A regulated institution must have an IT Steering Committee with representatives from the IT, HR, legal and business lines unless otherwise provided by supervisory authority.

The IT Committee shall at least have the following responsibilities:

1° assist the Executive Management in implementing IT Security Strategy that has been approved by the Board;

2° monitoring service levels and improvements, IT service delivery and projects;

3° Discuss on the implementation of plans and activities to reduce cyber risks, including business continuity planning matters;

4° Deliberate on lesson learning following cyber and information security incidents and implementation of relevant recommendations. Debriefing shall begin immediately after the end of the incidents.

5° Assess potential risks involved in activating the regulated institution's systems in a cloud environment;

6° Create a measurable and management transparent security strategy based on benchmarking, maturity models, gap analysis and continuous performance reporting that mirrors the operational processes;

7° Include security in job performance appraisals and apply appropriate rewards and disciplinary measures;

8° ensure the approved cyber risk management strategy articulates how the institution intends to address its inherent cyber risk and how it will maintain an acceptable level of residual cyber risk and maintain resilience on an ongoing basis;

The Steering Committee shall meet at least quarterly and when deem necessary.

Article 7 – IT Security Function

Unless provided otherwise in a specific regulation or Directive, each regulated Institution shall have an IT security Function with qualified staff in the IT or cyber security.

The IT security function's responsibilities shall include and not limited to:

1° designing cyber security strategy and IT program;

2° Implement and overseeing the regulated Institution's cyber security program execution;

3° recommending actions for addressing any noted program shortfalls and enforcing its cyber security policy;

4° perform regular information security internal assessments and audit;

5° detect cyber security incidents and regularly monitoring of abnormal and unauthorized access or use;

6° respond to identified or detected cyber security incidents to mitigate any negative effects;

7° recover from cyber-attacks and restore normal operations and services;

8° identify and assess internal and external cyber security risks that may threaten the security or integrity of non-public data stored on the regulated institution's information systems;

9° use preventive and detective infrastructure and implement policies and procedures to protect the regulated institution's information systems, and the financial data stored or in transit on those information systems, from unauthorized access, use or other malicious acts;

10° Establish and maintain threat profiles for identified threats to the institution;

11° establish and maintain threat modelling capabilities;

12° Conduct comprehensive penetration tests.

The head of the IT Security function or the staff in charge of IT Security shall report administratively to Chief Executive officer and functionally to the IT Board Committee.

Article 8 – Cyber security strategy

The regulated institution must maintain a cyber security strategy designed to protect the confidentiality, integrity and availability of the regulated institution's non-public data, systems and the underlying IT infrastructure.

The cyber security strategy must provide the basis for an action plan comprised of cyber security program that, as implemented, achieve the planned security objectives.

All documentation and information relevant to the regulated institution's cyber security strategy and program must be made available to the Supervisory Authority upon request.

Article 9 – Cyber security policy

A regulated institution must implement and maintain a written policy approved by the board.

The cyber security policy must be based on the regulated institution's risk assessment and address at least the following areas of the institution's operations:

1° Information security;

2° Data governance and classification;

3° Asset inventory and device management;

4° Access controls and identity management;

5° Systems operations and availability concerns;

6° Systems, applications and network security;

7° Application development, acquisition and quality assurance;

8° Physical security and environmental controls;

9° Customer data protection and privacy;

10° vendor and service provider management;

11° Cyber risk management;

12° penetration testing and vulnerability assessments;

13° Cyber incident management;

14° awareness of staff, customers and stakeholders with regard to cyber security;

15° integrity requirements of staff dealing with data, systems and networks including non-disclosure agreement;

16° controls to systems, physical locations containing customer information and tools to monitor access by authorized persons.

The policy shall be reviewed within a reasonable period.

Article 10 – Penetration testing and vulnerability assessments

A regulated institution is required to conduct at least:

1 ° Annual penetration tests: The penetration testing shall focus on testing preventive and detective cyber resilience capabilities as well as test response and recovery capabilities. Tests should not result in a pass or fail, rather they should provide the tested entity with insight into its strengths and weaknesses, and enable it to learn and evolve to improve their cyber security maturity;

2° Bi-annual vulnerability assessments: conduct vulnerability assessments that scan internal systems for known vulnerabilities, and review the implementation level of cyber security policies and procedures based on the risk assessment;

Any person entrusted to conduct penetration test or vulnerability assessment shall have at least one or some of the following qualification:

1° Certified Information Systems Security Professional (CISSP);

2° Certified Information Security Manager (CISM);

3° Certified Information Systems Auditor (CISA);

4° Certified Ethical Hacker (CEH);

5° Offensive Security Certified Professional (OSCP);

6° Licensed Penetration Tester (LPT);

7° Any other similar certification.

The regulated institution shall share with the Supervisory Authority an executive summary of the findings of the test within fifteen days (15) after the test.

Article 11 – Audit trail

A regulated institution must securely maintain systems that includes audit trails designed to detect and respond to cyber security incidents that have reasonable likelihood of materially harming any material part of the normal operations of the regulated institution.

Article 12 – Alternative Delivery Channels (ADC) Security Management

Regulated Institutions shall provide customers with information about the precautions required when using ADC regularly, inform customers about potential risks associated to the ADC, and recommended protection and privacy principles for minimizing these risks to the customer. This information shall be publicly available.

Regulated Institutions shall determine individual identification and authentication factors for online and other remote transactions based on Board-approved policies, risk assessments, and data protection and privacy guidelines.

Article 13 – Cyber risk management

A regulated institution shall conduct a periodic risk assessment of the regulated institution's information systems sufficient to inform the design of the cyber security strategy and policy as required by this regulation. Such risk assessment shall be updated as reasonably necessary to address changes to the regulated institution's information systems, no-public data or business operations.

A regulated institution risk assessment must allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the regulated institution's business

operations related to cyber security, non-public information collected or stored, information systems utilized and the availability and effectiveness of controls to protect non-public data and information systems.

The risk assessment must be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

1° Criteria for the evaluation and categorization of identified cyber security risks or threats facing the institution;

2° Criteria for the assessment of the confidentiality, integrity, and availability of the financial information systems and non-public data, including the adequacy of existing controls in the context of identified risks;

3° Acceptance criteria describing how identified risks will be treated or accepted based on the institution's risk appetite and how the cyber security strategy and policy will address the risks.

The regulated institution risk management function should include and not limited to the tasks below:

1° Assessing the risks and exposures related to cyber security and determining whether they are aligned to the regulated institution's risk appetite;

2° Monitoring current and emerging risks and changes to laws and regulations.;

3° Collaborating with system administrators and others charged with safeguarding the information assets of the regulated institution to ensure appropriate control design;

4° Maintain comprehensive cyber risk registers: Key risk indicators (KRI) should be regularly identified and assessed. Risk identification should be forward looking and include the security incident handling;

5° Ensure implementation of the cyber security strategy and program;

6° Safeguarding the confidentiality, integrity and availability of information and the underlying IT infrastructure;

7° Ensure that a comprehensive inventory of IT assets, classified by business criticality, is established and maintained;

8° A Business Impact Analysis process is in place to regularly assess the business criticality of IT assets;

9° Design and implement a risk quantification framework in order to effectively assess how well the institution is managing its aggregate cyber risk and mitigating the residual cyber risk of its sector-critical systems and therefore develop a robust cyber risk management plan;

10° Reporting all enterprise risks consistently and comprehensively to the board to enable the comparison of all risks equally in ensuring that they are prioritized correctly;

11° Conduct red team exercises.

12° Carry out a business impact analysis and risk assessment where they identify critical assets to their business processes and class the risks/impact pertaining to them. A risk treatment plan shall be developed to mitigate the risks identified.

Article 14 – Assessment of a service provider

A regulated institution must implement written policies and procedures designed to ensure the security of information systems and non-public data that are accessible to, or held by, service providers.

Such policies and procedures shall be based on the risk assessment of the regulated institution and shall address to the extent applicable:

1° the identification and risk assessment of service providers;

2° minimum cyber security practices required to be met by such third-party service providers in order for them to do business with the regulated institution;

3° due diligence processes used to evaluate the adequacy of cyber security practices of such service providers;

4° periodic assessment of such service providers based on the risk they present and the continued adequacy of their cyber security practices;

5° Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations;

6° Response and recovery planning and testing are conducted with suppliers and third-party providers;

7° Conduct specific testing that addresses external interdependencies, such as connectivity to payment systems, messaging services, delivery channels, markets, and other critical service providers or partners.

Article 15 – Role of Internal Audit function

A regulated Institution shall incorporate qualified information security auditors within their Internal Audit team. Information security audit activities can be outsourced or through internal placement. Internal audit systems shall be appropriate to the size of the institution and to the nature, scope and risk of its activities that provide for adequate testing and review of information systems.

The regulated institution internal information security auditors should therefore ensure that the audit scope includes and not limited to the tasks below:

1° Continuous review and report on cyber risks and controls of the ICT systems within the regulated institution and other related third-party connections;

2° Conduct up-front due diligence to mitigate risks associated with third parties;

3° Assess both the design and effectiveness of the cyber security framework implemented;

4° Conduct regular independent threat and vulnerability assessment tests;

5° Report to the board the findings of the assessments;

6° Ensure the development and testing environment are separate from the production environment;

7° Assess if the institution's cyber risk management framework is appropriate for its size, complexity, and scope of operations, interconnectedness, and risk profile;

8° Advise senior management on whether the institution's policies and procedures are adequate to keep up with emerging cyber risks and industry regulations.

Article 16 – Multi-factor authentication

Based on its risk assessment, a regulated institution must use effective controls, which will include risk-based multi-factor authentication, to protect against unauthorized access to non-public data or information systems.

Multi-factor authentication must be utilized for any individual accessing the regulated institution's internal networks from an external network, unless the head of IT Security function or relevant staff has approved in writing the use of reasonably equivalent or more secure access controls.

Article 17 – Limitations on data retention

A regulated institution must have a data retention policy for the secure keeping and disposal on a periodic basis of any non-public data identified as per their Risk assessment, except where such information is otherwise required to be retained by law or regulation.

Article 18 – Training and awareness

A regulated institution must:

1° design a consistent and updated security awareness program in line with institution's risk assessment, strategy and current cyber security threats and trends;

2° provide regular cyber security awareness training for board members, senior managers and all personnel that interacts with institution's information system including but not limited to staff, interns, third party;

3° evaluate the effectiveness of the awareness training through regular quizzes and test simulations.

Board/Senior Management shall allocate adequate funds for all required trainings and awareness.

Article 19 – Encryption of non-public data

A regulated institution must implement controls, including encryption, to protect data held or transmitted by the regulated institution both in transit over external networks and at rest.

To the extent a regulated institution determines that encryption of data in transit over external networks is infeasible, the regulated institution may instead secure such non-public data using effective alternative compensating controls reviewed and approved by the IT steering Committee.

To the extent that a regulated institution is utilizing compensating controls as mentioned above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the IT steering Committee.

Article 20 – Incident response and business continuity management

A regulated institution must establish a written incident response management plan designed to promptly respond to, contain, and recover from, disruptions caused by any cyber incident materially affecting the confidentiality, integrity or availability of the institution's information systems or the continuing functionality of any aspect of the institution's business or operations.

The incident response and business continuity management plan shall address the following areas:

1° the internal processes for responding to cyber security incident and disasters;

2° the goals of the incident response and business continuity plans;

3° the definition of clear roles, responsibilities, and levels of decision-making authority;

4° external and internal communications and information sharing;

5° identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

6° documentation and reporting on cyber incidents/attacks and related incident response activities;

7° the evaluation and revision as necessary of the incident response and business continuity plans following a cyber security event;

8° identification and mitigation of cyber risks posed through interconnectedness to sector partners, external stakeholders and other third parties to prevent cyber risk contagion;

9° Implementation of effective escalation protocols linked to organization decision levels, cyber contagion containment procedures, communication strategies, and processes to incorporate lessons learned into the cyber security program.

Article 21 – Notification and reporting of the cyber incident

A regulated institution must notify the Supervisory Authority as promptly as possible within a period not exceeding two (2) hours from the occurrence of the incident or from a determination that a cyber security incident has occurred that is either of the following:

1° Cyber security incident that may disrupt a regulated institution from continuing its normal operations for customer-facing transactions;

2° Cyber security events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the institution.

A regulated institution must submit to the Supervisory Authority the full incident report within 24 hours from the occurrence of the incident as per the annex on this regulation.

Specific reporting requirements on cyber security incident may be provided in the Directive.

A regulated institution shall submit to the Supervisory Authority on an annual basis a written statement as per the appendix certifying that the regulated institution cyber security program is in compliance with the requirements set forth in this Regulation. The statement shall be submitted not later than 15th January of each year.

Article 22 – Statement of self-assessment

A regulated institution must submit to the Supervisory Authority on annual basis a written statement of self-assessment per the appendix certifying that the regulated institution cyber security strategy is in compliance with the requirements set forth in this Regulation. The statement shall be submitted not later than 15th January of each year.

Chapter III
Miscellaneous and final provisions

Article 23 – Application of other laws

Without prejudice to the provisions of this regulation, a regulated institution shall abide with other legal and regulatory requirements applicable to cyber security and data protection and privacy.

Article 24 – Tailored requirements

Regulated institution shall comply with provisions of this regulation, unless the Supervisory authority issue by a Directive tailored requirement proportionate to the nature, size, complexity and maturity in its business operations.

Article 25 – 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 relevant specific regulations.

Article 26 – Transition period

Regulated institutions that do not comply with the provisions of this regulation are given a period of One year to comply with them from the publication in the Official *Gazette* of the Republic of Rwanda.

Article 27 – Drafting, consideration and approval of this Regulation

This regulation was prepared, considered and approved in English

Article 28 – Repealing provision

The regulation N° 02/2018 of 24/01/2018 on cyber security and any prior provisions contrary to this regulation are hereby repealed.

Article 29 – Commencement

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

Appendix 1

Cyber security incident report format

N°	Date of incident	Time of incident	Type/ nature of incident	Physical location/ branch	Action taken	Time of resolution	Estimated/ actual impact of the incident (Financial and operational)	Law enforcement authorities involved (if applicable)	Action taken to mitigate future incidents

Appendix 2

(Regulated Institution Name)

Date ___

Statement of self-assessment

The Board of Directors [or a Senior Officer(s) of the regulated institution] certifies:

(1) The Board of Directors (or name of Senior Officer(s)) have reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the Board of Directors [or name of Senior Officer(s)] knowledge, the Cyber security strategy or program of (name of a regulated institution) as of ___/ ___/___(date of the Board Resolution or Senior Officer(s)) Compliance Finding for the year ended ___ / ___/ ___(year for which Board Resolution or Compliance Finding is provided) complies with this Regulation (regulation number).

Signed by the Chairperson of the Board of Directors (or the CEO)

(Name) _____ Date: _____