AMABWIRIZA RUSANGE Nº 02/2018 YO KU WA 24/01/2018 YEREKEYE UMUTEKANO W'IBIJYANYE N'IKORANABUHANGA MU ITANGAZABUMENYI N'ITUMANAHO

REGULATION Nº 02/2018 OF 24/01/2018 ON CYBERSECURITY

REGLEMENT Nº 02/2018 DU 24/01/2018 SUR LA CYBERSECURITE

ISHAKIRO

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza agamije

Ingingo ya 2: Ibisobanuro by'amagambo

Ingingo ya 3: Kurinda amakuru y'amabanki

UMUTWE WA II: IBISABWA MU MATEGEKO

Ingingo ya 4: Inshingano z'Inama y'Ubutegetsi n'Ubuyobozi bukuru mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho

Ingingo ya 5: Ingamba na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho

TABLE OF CONTENTS

CHAPTER ONE: GENERAL PROVISIONS

Article one: Purpose

Article 2: Definition of terms

Article 3: Banking data protection

CHAPTER II: REGULATORY REQUIREMENTS

Article 4: Board and Senior Management Cybersecurity Responsibilities

Article 5: Cybersecurity strategy and program

TABLE DE MATIERES

CHAPITRE PREMIER: DISPOSITIONS GENERALES

Article premier: Objet

Article 2: Définition des termes

Article 3: Protection de données bancaires

CHAPITRE II: EXIGENCES REGLEMENTAIRES

Article 4: Les responsabilités du conseil d'administration et de la direction générale en matière de cybersécurité

Article 5: Stratégie et programme de cybersécurité

Ingingo ya 6: Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	**Article 6: Cybersecurity Policy**	**Article 6: Politique de cybersécurité**
Ingingo ya 7: Amasuzuma yo kugerageza kwinjira no kureba intege nke	**Article 7: Penetration Testing and Vulnerability Assessments**	**Article 7: Test d'intrusion et évaluations de vulnérabilité**
Ingingo ya 8: Inzira y'ubugenzuzi	**Article 8: Audit Trail**	**Article 8: Piste d'audit**
Ingingo ya 9: Gucunga umutekano w'imirongo itwara amakuru isimbura iyindi	**Article 9: Alternative Delivery Channels (ADC) Security Management**	**Article 9: Gestion de la sécurité des canaux de distribution alternatifs**
Ingingo ya 10 : Isuzuma ry'ibibazo bishobora kuvuka	**Article 10 : Risk Management**	**Article 10 : Evaluation des risques**
Ingingo ya 11: Undi muntu utanga serivisi	**Article 11: Third Party Service Provider**	**Article 11: Tiers prestataire de services**
Ingingo ya 12: Gusuzuma umwirondoro hakoreshejwe ibintu byinshi	**Article 12: Multi-Factor Authentication**	**Article 12: Authentification multi-factorielle**
Ingingo ya 13: Igabanywa ry'amakuru agomba kubikwa	**Article 13: Limitations on Data Retention**	**Article 13: Limitations sur la rétention des données**
Ingingo ya 14: Amahugurwa n'igenzurwa ry'ukoresha uburyo bukoresha ikoranabuhanga	**Article 14: User Training and Monitoring**	**Article 14: Formation et contrôle de l'utilisateur**
Ingingo ya 15: Kurinda amakuru atari rusange	**Article 15: Encryption of Non-public Information**	**Article 15: Cryptage des informations non publiques**

Ingingo ya 16 Gahunda yo gukemura ibibazo bivutse	**Article 16 Incident Response and business continuity management**	**Article 16 Plan d'intervention en cas d'incident**
Ingingo ya 17 Imenyesha rikorerwa Banki Nkuru	**Article 17 Notices to the Central Bank**	**Article 17 Notifications à la Banque Centrale**
Ingingo ya 18 Ibyerekeranye n'ibanga	**Article 18 Confidentiality**	**Article 18 Confidentialité**
UMUTWE WA III: INGINGO ZINYURANYE N'IZISOZA	**CHAPTER III: MISCELLANEOUS AND FINAL PROVISIONS**	**CHAPITRE III: DISPOSITIONS DIVERSES ET FINALES**
Ingingo ya 19 Ibihano n'ibyemezo byo mu rwego rw'ubutegetsi	**Article 19 Penalties and administrative sanctions**	**Article 19 Pénalités et sanctions administratives**
Ingingo ya 20 : Igihe ntarengwa cyo kubahiriza aya mabwiriza	**Article 20 : Deadline for conforming to the provisions of this regulation**	**Article 20 : Délai de conformité aux dispositions du présent règlement**
Ingingo ya 21: Ivanwaho ry'ingingo z'amabwiriza zinyuranyije n'aya amabwiriza	**Article 21: Repealing provisions**	**Article 21: Dispositions abrogatoires**
Ingingo ya 22: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange	**Article 22: Drafting, consideration and approval of this Regulation**	**Article 22: Initiation, examen et approbation du présent Règlement**
Ingingo ya 23: Igihe aya mabwiriza atangirira gukurikizwa	**Article 23: Commencement**	**Article 23: Entrée en vigueur**

AMABWIRIZA RUSANGE No 02/2018 YO KU WA /24/01/2018 YEREKEYE UMUTEKANO W'IBIJYANYE N'IKORANABUHANGA MU ITANGAZABUMENYI N'ITUMANAHO

Ishingiye ku Itegeko n° 48/2017 ryo kuwa 23/09/2017 rigenga Banki Nkuru y'u Rwanda, cyane cyane mu ngingo yaryo ya 6, iya 8, iya 9, n'iya 10;

Ishingiye ku Itegeko n° 47/2017 ryo ku wa 23/094/2017 rigena imitunganyirize y'imirimo y'amabanki, cyane cyane mu ngingo yaryo iya 37 n'iya 117 ;

Banki Nkuru y'u Rwanda, yitwa " Banki Nkuru" mu ngingo zikurikira itegetse:

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza agamije

Aya mabwiriza agamije :

1° gushyiraho ibigenderwaho by'ibanze ku mabanki hagamijwe gukumira ibishobora guhungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho; no

2° guteza imbere uburyo bwo kurinda amakuru ku bakiriya kimwe n'uburyo bw'ikoranabuhanga mu guhanahana amakuru bukoreshwa n'amabanki.

REGULATION Nº 02/2018 OF 24/01/2018 ON CYBERSECURITY

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

Pursuant to Law n° 47/2017 of 23/094/2017 governing the organization of banking, especially in its Article 37 and 117 ;

The National Bank of Rwanda hereinafter referred to as "Central Bank", decrees:

CHAPTER ONE: GENERAL PROVISIONS

Article one: Purpose

This regulation aims at :

1° establishing minimum prudent standards to banks for their protection against cybersecurity threats ; and

2° promoting the protection of customer information as well as the information technology systems of banks

REGLEMENT Nº 02/2018 DU 24/01/2018 SUR LA CYBERSECURITE

Vu la loi n ° 48/2017 du 23/09/2017 régissant la Banque Nationale du Rwanda, spécialement en ses articles 6, 8, 9 et 10 ;

Vu la loi n° 47/2017 du 23/094/2017 portant organisation de l'activité bancaire, en particulier en son article 37 et 117 ;

La Banque Nationale du Rwanda ci-après dénommée " Banque Centrale", édicte:

CHAPITRE PREMIER: DISPOSITIONS GENERALES

Article premier: Objet

Le présent règlement vise à:

1° établir pour des banques des normes de prudentiels minimales pour les protéger contre les menaces de cybersécurité ; et

2° promouvoir la protection des informations des clients ainsi que des systèmes de technologies d'informations des banques.

Ingingo ya 2: Ibisobanuro by'amagambo

Muri aya mabwiriza, amagambo akurikira asobanura:

1° **ukorana n'ikigo**: Umuntu uwo ari we wese ugenzura, ugenzurwa cyangwa ugenzurirwa hamwe n'undi muntu. Muri iki gisobanuro, kugenzura bisobanura kugira ububasha mu buryo buziguye cyangwa butaziguye bwo gutanga icyerekezo cyangwa kugira ijambo rikomeye mu gutanga icyerekezo ku micungire cyangwa kuri politiki z'umuntu byaba binyuze ku kuba afite ububiko bw'uwo muntu cyangwa mu bundi buryo ;

2° **ukoresha uburyo bukoresha ikoranabuhanga ubyemerewe:** umukozi uwo ari we wese, ufitanye amasezerano na banki, uyihagarariye cyangwa undi muntu uwo ari we wese ugira uruhare mu bikorwa by'ubucuruzi bya banki kandi akaba yemerewe kugera ku buryo bukoresha ikoranabuhanga no ku makuru yayo kimwe no kubikoresha ;

3° **ikibazo cy'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho:** igikorwa icyo ari cyo cyose cyangwa kugerageza gukora igikorwa cyaba cyagezweho cyangwa kitagezweho cyo kugera utabyemerewe, guhungabanya

Article 2: Definition of terms

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

1° **affiliate**: any person that controls, is controlled by or is under common control with another Person. In this definition , control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise ;

2° **authorized User**: any employee, contractor, agent or other person that participates in the business operations of a bank and is authorized to access and use any Information Systems and data of the bank ;

3° **cybersecurity incident**: any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

Article 2: Définition des termes

Dans le présent règlement, les termes et expressions suivants signifient:

1° **affilié :** toute personne qui contrôle, est contrôlée par ou se trouve sous le contrôle commun avec une autre personne. Aux fins de cette définition, contrôle signifie la possession directe ou indirecte du pouvoir de diriger ou d'influencer la direction de la gestion et des politiques d'une personne que ce soit à travers la possession des actions d'une telle personne ou d'une autre manière que ce soit ;

2° **utilisateur autorisé**: tout employé, contractant, agent ou toute autre personne qui participe aux opérations commerciales d'une banque et est autorisée à accéder aux systèmes d'informations et des données de la banque et à les utiliser ;

3° **incident de cybersécurité:** toute acte ou tentative ayant réussi ou non visant à avoir accès non autorisé, perturber ou abuser d'un système d'informations ou de l'information stockée sur ce système**.**

cyangwa gukoresha nabi uburyo bukoresha ikoranabuhanga cyangwa amakuru abitswe kuri bene ubwo buryo.

4° **uburyo bukoresha ikoranabuhanga:** Uburyo bw'ibanga bw'ibikenerwa byifashishwa mu guhanahana amakuru hifashishijwe ikoranabuhanga bwatunganyirijwe gukusanya, gutunganya, kubika, gukoresha, guhanahana, gusakaza cyangwa kugira amakuru mu buryo bw'ikoranabuhanga kimwe n'uburyo bwihariye nk'uburyo bwo kugenzura bukoreshwa mu nganda/itunganya ry'ibintu binyuranye, gushyiraho imirongo ya telefoni, uburyo bwo guhamagarana kuri telefoni ikigo kihariye, kimwe n'uburyo bwo kugenzura ibidukikije.

5° **gusuzuma umwirondoro hagendewe ku bintu byinshi:** gusuzuma umwirondoro w'umuntu ugendeye nibura ku bwoko bubiri bw'ibintu byifashishwa mu kumenya uwo ari we:

a) ibyo agomba kuba azi nk'ijambobanga;
b) ibyo agomba kuba afite nk'akarango cyangwa ubutumwa kuri telefoni igendanwa; cyangwa

4° **information System**: a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

5° **multi-Factor authentication**: authentication through verification of at least two of the following types of authentication factors:

a) knowledge factors, such as a password;
b) possession factors, such as a token or text message on a mobile phone; or

4° **iystème d'information:** un ensemble distinct de ressources électroniques d'information organisées pour la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou la disposition d'informations électroniques ainsi que tout système spécialisé tel que les systèmes de contrôle industriels/processus, commutation téléphonique ainsi les systèmes d'autocommutateurs téléphoniques privés , et des systèmes de contrôle de l'environnement.

5° **authentification multi-factorielle**: authentification par vérification d'au moins deux des types de facteurs d'authentification suivants:

a) facteurs de connaissance, tel un mot de passe ;
b) facteurs de possession, tel un jeton d'authentification ou un message text téléphonique sur un téléphone mobile ; ou

c) ibyerekeranye n'imiterere y'ibiranga umuntu nk'ibiranga imiterere y'umubiri.

6° **amakuru atari rusange:** amakuru ayo ari yo yose abantu bose badashobora kugeraho abitswe mu buryo bw'ikoranabuhanga kandi:

a) akaba afitanye isano n'ibikorwa by'ubucuruzi bya banki ku buryo kuyahindura mu buriganya, cyangwa kuyasakaza hanze, kuyageraho cyangwa kuyakoresha nta burenganzira byagira ingaruka mbi ku bucuruzi, ibikorwa cyangwa ku mutekano wa banki;

b) amakuru ayo ari yo yose yerekeranye n'umuntu biturutse ku izina rye, nomero ye, ikimenyetso cye bwite, cyangwa ikindi kintu kimuranga gishobora gukoreshwa mu kumenya uwo muntu hakoreshejwe kimwe cyangwa byinshi muri ibi bintu bikurikira: (i) nomero y'ubwiteganyirize ye, (ii) nomero y'uruhushya rwo gutwara ibinyabiziga ye cyangwa nomero y'ikarita ndangamuntu ku badafite uruhushya rwo gutwara ibinyabiziga, (iii) nomero ya konti, nomero y'ikarita yo kubikuriza amafaranga yemera

c) inherence factors, such as a biometric characteristic.

6° **nonpublic information**: all electronic information that is not Publicly Available Information and is:

a) business related information of the bank, the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the bank;

b) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security

c) facteurs d'inhérence e, tel un caractère biométrique.

6° **information non publique**: toute information électronique qui n'est pas disponible au public et qui est :

a) l'information commerciale de la banque, dont la falsification ou la divulgation, l'accès ou l'utilisation non autorisés auraient un impact négatif sérieux sur l'activité, les opérations ou la sécurité de la banque;

b) toute information concernant un individu qui du fait du nom, du numéro, de la marque personnelle, ou d'un autre signe d'identification peut être utilisée pour identifier cet individu en combinaison avec un ou plusieurs des éléments de données suivants : : (i) le numéro de la sécurité sociale, (ii) le numéro du permis de conduire ou le numéro de la carte d'identification du non conducteur, (iii) le numéro de compte, le numéro de la carte de

inguzanyo cyangwa iy'ikarita yo kubikiriza amafaranga itemera inguzanyo, (iv) ubundi buryo bwose bwo kurinda umutekano, uburyo bwo kugera ku makuru cyangwa ijambobanga rituma umuntu agera ku makuru yamufasha kugera kuri konti y'umuntu ku giti cye, cyangwa (v) amakuru ku miterere y'umubiri;

code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

crédit ou de débit, (iv) tout code de sécurité, code d'accès ou mot de passe qui permettrait d'accéder à un compte financier d'un individu' ou (v) les données biométriques ;

c) amakuru ayo ari yo yose, usibye imyaka cyangwa igitsina uko yaba ateye kose cyangwa uburyo abitswemo, yateguwe n'umukozi wo mu rwego rw'ubuvuzi yerekeranye n'umuntu ku giti cye avuga ku byerekeranye (i) n'ubuzima bw'umubiri we , ubuzima bwo mu mutwe cyangwa imyitwarire ye mu gihe cyahise, ubungubu cyangwa igihe kizaza cyangwa uburwayi bw'umuntu ku giti cye cyangwa bw'umwe mu bagize umuryango we (ii) itangwa rya serivisi z'ubuzima ku muntu uwo ari we wese, cyangwa (iii) ubwishyu bwa serivisi z'ubuzima ku muntu uwo ari we wese.

c) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

c) toute information ou données, à l'exception de l'âge ou du genre, sous quelque forme ou support que ce soit, créés par ou provenant d'un prestataire de services de santé ou d'une personne et qui sont relatives (i) à la santé ou l'état physique, mental ou comportemental passé, présent ou futur de toute personne ou d'un membre de safamille, ou (ii) à la fourniture de soins de santé à tout individu, ou (iii) au paiement de soins de santé à tout individu.

7° **kugerageza kwinjira nta burenganzira**: uburyo bukoreshwa mu kugerageza aho abakora isuzuma bagerageza gukwepa cyangwa kuganza ibigize umutekano w'uburyo bukoresha ikoranabuhanga

7° **penetration Testing**: a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or

7° **test d'intrusion**: une méthodologie de test dans laquelle les évaluateurs tentent de contourner ou de déjouer les caractéristiques de sécurité d'un système d'information en essayant de

bagerageza kwinjira mu bubiko bw'amakuru cyangwa ahakorerwa igenzura binjiriye imbere cyangwa inyuma y'uburyo bukoresha ikoranabuhanga bukoreshwa na banki.

8° **amakuru rusange**: amakuru ayo ari yo yose banki ishobora gutekereza ko abantu bose bashobora kumenya mu buryo bwemewe n'amategeko : ni ukuvuga amakuru aturuka mu nzego za Leta cyangwa mu nzego z'ibanze; ibitangazamakuru bigera ku bantu benshi; cyangwa amakuru agomba gutangarizwa rubanda hakurikijwe amategeko.

9° **isuzuma ry'umwirondoro rishingiye ku byateza ingorane:** Uburyo ubwo ari bwo bwose bwo gusuzuma umwirondoro bushingiye ku ngorane zishobora kuba butahura ibintu bidasanzwe cyangwa impinduka mu bijyanye n'imikoreshereze isanzwe kandi bugasaba ko habaho irindi genzura ry'ibiranga umuntu igihe ibyo bintu bidasanzwe cyangwa izo mpinduka zigaragaye nko kumubaza ibibazo byo kureba niba uwo muntu ari we koko.

10° **undi muntu utanga serivisi:** Umuntu (i) utari usanzwe akorana na banki, (ii) uha banki serivisi, kandi (iii) ufata neza, utunganya cyangwa wemerewe kugera ku makuru atari rusange binyuze muri serivisi ayiha.

controls from outside or inside the bank's information systems.

8° **publicly Available Information**: any information that a bank has a reasonable basis to believe is lawfully made available to the general public from: the Government or local government records; widely distributed media; or disclosures to the general public that are required to be made by the law.

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° **third party service provider(s)**: a Person that (i) is not an Affiliate of the bank, (ii) provides services to the bank, and (iii) maintains, processes or otherwise is permitted access to

pénétrer les banques de données ou les contrôles de l'extérieur ou à l'intérieur des Systèmes d'Informations de la banque.

8° **informations publiques:** toute information dont la banque a toute raison de croire qu'elle est légalement disponible au grand public à partir : des archives de l'Etat ou d'une collectivité locale; des organes médiatiques de large diffusion; ou des révélations au grand public qui sont exigées par la loi.

9° **authentification basée sur le risque**: tout système d'authentification basée sur le risque qui détecte des anomalies ou des changements dans la manière d'utilisation normale d'une personne et qui requiert une vérification supplémentaire de l'identité de la personne lorsque de telles déviations ou changements sont détectés notamment par le biais de l'utilisation des questions secrètes.

10° **tiers prestataire (s) de services:** une personne qui (i) n'est pas un affilié de la banque, (ii) donne des services à la banque, et (iii) maintient, traite ou est autrement autorisée d'accéder aux

Nonpublic Information through its provision of services to the bank.

informations non publiques par le biais de prestation de services à la banque.

Ingingo ya 3: Kurinda amakuru y'amabanki

Banki iyo ariyo yose yemewe na Banki Nkuru itegetswe kubika amakuru yayo y'ibanze ku butaka bwa Repubulika y'u Rwanda.

Article 3: Banking primary data location

Any bank lincensed by the Central Bank must maintain its primary data on the territory of the Republic of Rwanda.

Article 3: Protection de données bancaires

Toute banque agréer par la Banque Centrale doit maintainir ses données primaires sur le territoire de la République du Rwanda.

UMUTWE WA II: IBISABWA MU MATEGEKO

CHAPTER II: REGULATORY REQUIREMENTS

CHAPITRE II: EXIGENCES REGLEMENTAIRES

Ingingo ya 4: Inshingano z'Inama y'Ubutegetsi n'Ubuyobozi bukuru mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho

(4.1) Imiyoborere y'umutekano w'amakuru ni inshingano y'Inama y'Ubutegetsi n'ubuyobozi bukuru. Buri banki igomba kugira uburyo rusange bw'imiyoborere y'umutekano w'amakuru bugizwe n'ibi bikurikira:

a) ingamba z'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho zijyanye n'intego z'ibikorwa ;

b) gahunda y'umutekano y'ibanze itanga igisubizo kuri buri cyiciro cy'ingamba, cy'igenzura n'icy'amabwiriza ;

Article 4: Board and Senior Management Cybersecurity Responsibilities

(4.1) Information Security Governance must be the responsibility of the Board of Directors and Senior Management. Each bank must have a comprehensive information security governance framework consisting of the following:

a) cybersecurity strategy linked with business objectives;

b) governing security program that address each aspect of the strategy, controls and regulations;

Article 4: Les responsabilités du conseil d'administration et de la direction générale en matière de cybersécurité

(4.1) La Gouvernance de la sécurité de l'information est la responsabilité du conseil d'administration et de la direction générale. Chaque banque doit disposer d'une structure globale de gouvernance de la sécurité de l'information qui consiste de ce qui suit :

a) une stratégie de cybersécurité ayant trait aux objectifs opérationnels;

b) un programme régissant la sécurité applicable à chaque aspect de la stratégie, des contrôles et du règlement ;

c) urutonde rwuzuye rw'ibigenderwaho muri buri politiki kugira ngo uburyo bukurikizwa n'imirongo ngenderwaho bijyanye na politiki iriho ;

d) imiterere y'ikigo ikora neza izira kugongana kw' inyungu bwite, ifite ububasha buhagije n'ibyangombwa byuzuye ;

e) ibipimo n'uburyo bwo kugenzura ko amabwiriza yubahirizwa kimwe no kumenya uko abandi babona imikorere y'urwo rwego ndetse no gushyiraho ibyashingirwaho mu ifatwa ry'ibyemezo mu rwego rw'imicungire ;

(4.2) **Inzobere mu by'ikoranabuhanga ku rwego rw'Inama y'Ubuyobozi:** Buri banki igomba kugira komite ishinzwe ikoranabuhanga mu itumanaho ku rwego rw'Inama y'Ubuyobozi yayo kugira ngo iyigire inama ku byerekeranye n'icyerekezo kigomba gufatwa mu rwego rw'Ikoranabuhanga mu itumanaho no gukora ishoramari muri urwo rwego ibikorera Inama y'Ubutegetsi.

(4.3) **Ububasha bwa komite ishinzwe ikoranabuhanga n'itumanahano:** komite ifite ububasha bukurikira:

a) kugenzura komite nyobozi ishinzwe

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

d) an effective organization structure void of conflict of interest with sufficient authority and adequate resources;

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

(4.2) **Expertise at the Board Level**: Each bank must have IT Committee at the Board level to give advice on strategic direction on IT and to review IT investments on Board's behalf.

(4.3) **Powers of IT Committee**: the committee must have the following powers:

a) perform oversight functions

c) une série complète des normes de chaque politique visant à garantir la conformité des procédures et des Principes directeurs à la politique ;

d) une structure organisationnelle efficace dépourvue de conflit d'intérêts avec une autorité suffisante et des ressources appropriées.

e) des indicateurs et les processus de contrôle en vue d'assurer la conformité, les réactions sur l'efficacité et de fournir la base de prise de décisions de gestion appropriées ;

(4.2) **Expertise au niveau du conseil d'administration:** Chaque banque doit disposer d'un comité chargé de l' informatique sein du conseil d'administration pour donner conseil sur l' orientation stratégique en matière de la technologie d'information et pour revoir les investissements en la matière pour le compte du conseil d'administration.

(4.3) **Compétences du Comité chargé de l'informatique:** le comité dispose des compétences suivantes:

a) exercer des fonctions de

Ikoranabuhanga n'itumanaho ;

b) gukora amaperereza ku bikorwa muri urwo rwego ;

c) gushakisha amakuru ku mukozi uwo ari we wese ;

d) gushaka ubufasha bwo mu rwego rw'amategeko n'urw'umwuga hanze y'ikigo ;

e) kunoza uruhare rw'abo hanze bafite ubuzobere bukwiye mu gihe ari ngombwa ;

f) gufatanya n'izindi komite z'Inama y'ubutegetsi n'ubuyobozi bukuru mu gutanga ibitekerezo, gusubiramo no guhindura ingamba za sosiyete n'ingamba zo mu rwego rw'ikoranabuhanga mu itangazabumenyi.

(4.4) Gushyira mu bikorwa, kugerageza no kuvugurura ingamba zo kubungabunga umutekano w'amakuru bigomba gutegurwa nk'igice cy'ishyirwaho rya gahunda y'umutekano w'amakuru. Komite nshingwabikorwa n'Inama y'Ubuyobozi

over the IT steering committee at managerial level ;

b) investigate activities within this scope ;

c) seek information from any employee ;

d) obtain outside legal or professional advice ;

e) secure attendance of outsiders with relevant expertise, if it considers necessary ;

f) work in partnership with other board committees and senior management to provide input, review and amend the aligned corporate and IT strategies.

(4.4) Information security strategy implementation, testing and reviews should be planned as part of the Information security program development. The executive committee and the Board must review the security

supervision du comité direction en charge de l'informatique ;

b) faire des investigations dans ce cadre ;

c) s'informer auprès de tout employé ;

d) obtenir des conseils juridiques ou professionnels de l'extérieur ;

e) assurer la présence des personnes de l'extérieur ayant l'expertise voulue s'il le juge nécessaire ;

f) travailler en partenariat avec les autres comités du conseil d'administration et la direction générale en vue de donner des commentaires, revoir et modifier les stratégies organisationnelles et informatique alignées.

(4.4) La mise en œuvre, les tests et les révisions de la stratégie de la sécurité de l'information, doivent être planifiés dans le cadre de l'élaboration du programme de la sécurité de l'information. Le comité exécutif et le

zigomba gusubiramo ingamba z'umutekano zifatanyije na serivisi ishinzwe umutekano w'amakuru, zikumva ibisobanuro n'ingaruka, zikagira icyo zivuga kuri buri gikorwa kigamije kugera ku ntego y'imikorere no guha umukuru wa serivisi ishinzwe umutekano w'amakuru igihe cyo kugira icyo avuga ku byavuzwe no kuzohererereza ingamba zisubiwemo komite ifata ingamba zerekeranye n'ikoranabuhanga ngo izunguraneho ibitekerezo, izinononsore inazemeze.

strategy with the IT Security Unit, understand the implications and effects, provide feedback on each initiative to achieve strategic objective and allow time for the IT Security Unit representative to respond to the comments and send the next version to the strategic committee for discussion, refinement and approval.

conseil d'administration doivent revoir la stratégie de sécurité avec l'unité chargé de la sécurité des systèmes d'information, en comprendre les implications et les effets, donner des réactions sur chaque initiative visant à réaliser l'objectif stratégique et donner du temps au responsable de la sécurité des systèmes d'information pour réagir aux commentaires et d'envoyer la prochaine version au comité stratégique pour discussion, finalisation et approbation.

Umukuru wa serivisi ishinzwe umutekano w'amakuru n'umuyobozi mukuru bagomba gusubiramo, kwemeza no gutangariza abo bireba inyandiko ya nyuma yerekeranye n'ingamba zafatwa mu rwego rw'umutekano w'ikoranabuhanga.

The head of the information security or the Chief Executive Officer (CEO) must review, approve and communicate the final security strategy document to the intended audience.

Le responsable de la sécurité des systèmes d'information et le directeur général doivent revoir, approuver, et communiquer le document final de la stratégie de sécurité au public visé.

(4.5) **Komite nyobozi ishinzwe ikoranabuhanga:** Banki igomba kugira komite nyobozi ishinzwe ikoranabuhanga igizwe n'abahagarariye serivisi y'ikoranabuhanga, serivisi ishinzwe abakozi, n'inzego zishinzwe amategeko n'ubucuruzi. Inshingano zayo ni ugufasha ubuyobozi bukuru mu gushyira mu bikorwa ingamba mu byerekeranye n'umutekano w'ikoranabuhanga zemejwe n'Inama y'ubuyobozi. Izo ngamba zikubiyemo ishyirwaho ry'ibyihutirwa mu ishoramari mu

(4.5) **IT Steering Committee:** The bank must have an IT Steering Committee with representatives from the IT, HR, legal and business lines. Its role must be to assist the Executive Management in implementing IT Security Strategy that has been approved by the Board. It includes prioritization of IT-enabled security investment, reviewing the status of projects (including, resource conflict), monitoring service levels and

(4.5) **Le comité de direction chargé de l'informatique :** La banque doit avoir un comité **de direction chargé de l'**informatique composé des représentants provenant des services informatique, ressources humaines, juridique et commercial. Son rôle est d'assister la direction exécutive dans la mise en œuvre de la stratégie de la sécurité des systèmes d'information qui a été adoptée par le conseil d'administration. Cette stratégie

rwego rw'umutekano w'ikoranabuhanga mu itangazabumenyi, gusubiramo imishinga (harimo no gukemura ibitumvikanwaho mu rwego rw'ibikenewe), kugenzura ibipimo n' impinduka nziza bya serivisi , itangwa rya serivisi z'ikoranabuhanga ndetse n'imishinga.

(4.6) **Urwego rushyinzwe serivisi y'umutekano w'amakuru (ISU):** Banki igomba gushyiraho umuntu w'inzobere ushinzwe gutegura ingamba na gahunda y' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, gushyira mu bikorwa no kugenzura imikoreshereze y'iyo gahunda, gutanga inama ku bigomba gukorwa mu rwego rwo gukemura ibibazo bigenda bigaragara muri iyo gahunda no gushyira mu bikorwa politiki yayo y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho. Urwego rugomba kandi guhora rukora isesengura n'ubugenzuzi k'umutekano w'amakuru mu ikoranabuhanga.

Inshingano za serivisi y'umutekano w'amakuru zishobora gukorwa na na banki, umwe mu bakorana nayo kimwe n'undi muntu utanga serivisi muri urwo rwego. Iyo ibisabwa muri urwo rwego byuzujwe hifashishijwe undi muntu utanga serivisi cyangwa ikigo gishamikiye kuri banki, banki igomba:

improvements, IT service delivery and projects.

(4.6) **IT Security Unit (ISU) :** The bank must establish an IT Security Unit and designate a qualified individual responsible for designing cybersecurity strategy and program, implementing and overseeing the bank's cybersecurity program execution, recommending actions for addressing any noted program shortfalls and enforcing its cybersecurity policy. The unit must also perform regular information security internal assessments and audit.

The responsabilities of the Unit may be undertaken by the bank, one of its affiliates or a third party service provider. To the extent this requirement is met using a third party service provider or an affiliate, the bank must:

comprend la définition des priorités des investissements en matière de la sécurité informatique, l'exam de l'état des projets (y compris le conflit des ressources), le suivi des niveaux et des améliorations des services, la fourniture des services ainsi que des projets informatiques.

(4.6) **L'unité chargé de la sécurité des systèmes d'information (ISU) :** La banque doit désigner un individu qualifié chargé de concevoir la stratégie et le programme de cybersécurité, de mettre en œuvre et de contrôler l'exécution du programme de cybersécurité de la banque, de recommander des actions pour remédier aux défaillances observées dans le programme et de mettre en œuvre sa politique de cybersécurité. L'unité doit également effectuer régulièrement des évaluations internes de sécurité de l'information et des audits.

Les responsabilités de l'unité chargé de la sécurité des systèmes d'information peuvent être employé par la banque, l'un de ses affiliés ou par un tiers prestataire de services. Si cette exigence est remplie en faisant recours à un prestataire de services ou un affilié, la banque doit :

a) kwishingira ko aya mabwiriza azubahirizwa;

b) gushyiraho umwe mu bakozi bakuru ba banki ushinzwe kuyobora no kugenzura utanga serivisi; no

c) gusaba utanga serivisi gukomeza gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho irinda banki nk'uko bisabwa muri aya mabwiriza.

(4.7) **Gutanga raporo:** Ukuriye ISU atanga raporo k'Umuyobozi Mukuru cyangwa ku muyobizi ufite mu nshingano ze umutekano. ISU itanga raporo ku ngamba z'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho rya banki no ku ishyirwa mu bikorwa rya gahunda y'umutekano; akagaragaza ibibazo bishobora kuvuka muri urwo rwego areba nibura ibi bikurikira:

a) Ibanga ku makuru atari rusange n'ubudakemwa n'umutekano w'uburyo bukoresha ikoranabuhanga bukoreshwa na banki;

a) retain responsibility for compliance with this regulation;

b) designate a senior member of the bank's personnel responsible for direction and oversight of the third party service provider; and

c) require the third party service provider to maintain a cybersecurity program that protects the bank in accordance with the requirements of this regulation.

(4.7) **Reporting:** The head of the ISU must report the Chief Executive Officer (CEO) or the senior manager in charge of the cyber security. The Unit must report on the bank's cybersecurity strategy and program execution identifying emerging material cybersecurity risks and must consider at least the following:

a) the confidentiality of nonpublic information and the integrity and security of the bank's information systems;

a) retenir la responsabilité de conformité au présent règlement;

b) désigner un cadre supérieur parmi son personnel chargé de diriger et de contrôler le tiers prestataire de services ; et

c) exiger le tiers prestataire de services de maintenir un programme de cybersécurité qui protège la banque conformément aux exigences du présent règlement.

(4.7) **Des rapports:** Le chargé de ISU de chaque banque relève de CEO ou du cadre superieur chargé de la sybersecurité. Il doit rendre compte de la stratégie de cybersécurité de la banque et l'exécution du programme en identifiant les risques émergents importants en matière de cybersécurité et considérer au moins les aspects suivants :

a) la confidentialité des informations non publiques et l'intégrité et la sécurité des systèmes d'information de la banque ;

b) Politiki n'inzira zikurikizwa na banki mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho;

c) Ibyateza ingorane byigaragaza bishobora kuvuka mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho muri banki;

d) Ubushobozi muri rusange bwa gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bwo kugera ku ngamba y'umutekano; na

e) Ibikorwa bifatika by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho banki yagizemo uruhare mu gihe kirebwa n'iyo raporo.

b) the bank's/ cybersecurity policies and procedures;

c) emerging material cybersecurity risks to the bank;

d) overall effectiveness of the bank's cybersecurity program achieving security strategy; and

e) material cybersecurity events involving the bank during the time period addressed by the report ;

b) les politiques et procédures de la banque en matière de cybersécurité ;

c) les risques sérieux et émergents de cybersécurité pour la banque;

d) l'efficacité globale du programme de cybersécurité de la banque dans la réalisation de la stratégie de sécurité ; et

e) des événements importants de cybersécurité qui ont impliqué la banque au cours de la période couverte par le rapport.

Ingingo ya 5: Ingamba na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho

(5.1) Banki igomba gushyiraho ingamba na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho yo kurinda amabanga, ubudakemwa, n'ukuboneka k'uburyo

Article 5: Cybersecurity strategy and program

(5.1) The bank must maintain a cybersecurity strategy and program designed to protect the confidentiality, integrity and availability of the bank's information systems.

Article 5: Stratégie et programme de cybersécurité

(5.1) La banque doit maintenir une stratégie et un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de la banque.

bukoresha ikoranabuhanga bukoreshwa na banki.

(5.2) Ingamba y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanahoitanga intango ya gahunda y'ibigomba gukorwa igizwe na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, ituma intego ziteganyijwe mu rwego rw'umutekano zishobora kugerwaho iyo ishyizwe mu bikorwa. Ingamba na gahunda z'ibigomba gukorwa zigomba guteganya uburyo igenzura kimwe n'ibipimo bishobora kwerekana urugero rw'ibyagezweho.

(5.3) Ingamba na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanahobigomba kuba bishingiye ku isuzuma ry'ibyateza ingorane ryakozwe na banki kandi bigomba kuba bigamije gukora nibura ibi bikurikira:

a) gutahura no gusuzuma ibyateza ingoranemu rwego y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho by'imbere mu kigo cyangwa hanze yacyo bishobora kubangamira umutekano cyangwa ubudakemwa bw'amakuru abitswe mu buryo bukoresha ikoranabuhanga bukoreshwa na banki;

(5.2) The cybersecurity strategy must provide the basis for an action plan comprised of cybersecurity program that as implemented, achieve the planned security objectives. The strategy and action plans must contain provision for monitoring as well as defined metrics to determine the level of success.

(5.3) The cybersecurity strategy and program must be based on the Bank's risk assessment and designed to perform at least the following core cybersecurity functions:

a) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the bank's information systems;

(5.2) La stratégie de cybersécurité doit servir de base à un plan d'action comprenant un programme de cybersécurité qui, une fois mise en œuvre, permet de réaliser les objectifs de sécurité planifiés. La stratégie et les plans d'action doivent prévoir des dispositions pour le contrôle ainsi que des indicateurs définis en vue de déterminer le niveau de réussite.

(5.3) La stratégie et le programme de cybersécurité doivent être basés sur l'évaluation des risques de la banque et être conçus pour remplir au moins les principales fonctions de cybersécurité reprises ci-après :

a) identification et évaluation des risques de cybersécurité internes et externes susceptibles de porter atteinte à la sécurité ou l'intégrité des informations non publiques stockées sur les systèmes d'information de la banque ;

b) gukoresha ibikorwa remezo by'ubwirinzi no gushyira mu bikorwa politiki n'inzira zikurikizwa mu kurinda uburyo bukoresha ikoranabuhanga bukoreshwa na banki hamwe n'amakuru atari rusange abitswe kuri ubwo buryo, habuzwa kuyageraho nta burenganzira, kuyakoresha cyangwa kuyakoraho ibindi bikorwa by'ubugome;

b) use defensive infrastructure and the implementation of policies and procedures to protect the bank's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;

b) utilisation de l'infrastructure de défense et mise en œuvre des politiques et procédures de protection des systèmes d'information de la banque et des informations non publiques stockées sur ces systèmes d'information contre tout accès ou utilisation non autorisés, ou d'autres actes malveillants ;

c) gutahura ibikorwa bihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;

c) detect cybersecurity incidents and regularly monitoring of abnormal and unauthorized access or use;

c) détection des incidents de cybersécurité;

d) gukemura ibibazo bikomoka ku bikorwa bihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho byagaragaye cyangwa byatahuwe mu rwego rwo kugabanya ubukana bw'ingaruka zabyo;

d) respond to identified or detected cybersecurity incidents to mitigate any negative effects;

d) réaction aux incidents de cybersécurité identifiés ou détectés afin de mitiger tous les effets négatifs ;

e) gusana ibyangijwe n'ibikorwa by'ihungabana ry'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho no gusubukura ibikorwa n'itangwa rya serivisi zisanzwe; na

e) recover from cybersecurity events and restore normal operations and services; and

e) reprise après les incidents de cybersécurité et restauration du fonctionnement normal des opérations et des services ; et

f) kuzuza inshingano zo gutanga raporo ziteganywa n'amabwiriza.

f) fulfill applicable regulatory reporting obligations.

f) accomplissement des applicables obligations réglementaires en mstière d'information.

(5.4) Banki igomba gukora ibisabwa byose muri aya mabwiriza ishyiraho ingingo zikwiye za gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho y'umuntu ukorana na banki; izo ngingo zipfa gusa kuba zuzuza ibisabwa muri aya mabwiriza bireba banki.

(5.4) The bank must meet the requirement(s) of this regulation by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this regulation, as applicable to the bank.

(5.4) La banque doit remplir les exigences du présent règlement en adoptant des dispositions appropriées et applicables d'un programme de cybersécurité maintenu par un affilié, pourvu que de telles dispositions satisfessent aux exigences du présent règlement autant que cela est applicable pour la banque.

(5.5) Banki Nkuru igomba gushyikirizwa inyandiko zose kimwe n'amakuru yerekeranye n'ingamba na gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho igihe ibisabye.

(5.5) All documentation and information relevant to the bank's cybersecurity strategy and program must be made available to the Central Bank upon request.

(5.5) Toute documentation et informations relatives à la stratégie et au programme de cybersécurité de la banque doivent être rendues disponibles à la Banque Centrale sur sa demande.

<u>Ingingo ya 6</u>: Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho

<u>Article 6</u>: Cybersecurity Policy

<u>Article 6</u>: Politique de cybersécurité

(6.1) Banki igomba gushyira mu bikorwa no kubika politiki yanditse yemewe n'Inama y'Ubuyobozi igaragaza politiki yayo mu byerekeranye no kurinda uburyo bukoresha ikoranabuhanga kimwe n'amakuru atari rusange abitswe kuri ubwo buryo. Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho igomba gushingira ku isuzuma ry'ibyateza ingorane banki muri kandi ikagira icyo ivuga nibura kuri ibi bikurikira bijyanye n'ibikorwa bya banki:

(6.1) The bank must implement and maintain a written policy approved by the bank board of directors, setting forth the bank's policy for the protection of its information systems and nonpublic information stored on those information systems. The cybersecurity policy must be based on the Bank's risk assessment and address at least the following areas of the bank's operations:

(6.1) La banque doit mettre en œuvre et maintenir une politique écrite approuvée par le conseil d'administration qui expose sa politique de protection de ses systèmes d'information ainsi que des informations non publiques stockées sur ces systèmes d'information. La politique de cybersécurité doit être basée sur l'évaluation des risques de la banque et doit considérer au moins les aspects des opérations de la banque repris ci-après :

a) Umutekano w'amakuru;	a) Information security ;	a) Sécurité de l'information ;
b) Imiyoborere no gushyira mu byiciro amakuru;	b) Data governance and classification ;	b) Gouvernance et classification des données ;
c) Ibarura ry'umutungo no gucunga ibikoresho;	c) Asset inventory and device management ;	c) Inventaire des biens et gestion des appareils
d) Kugenzura uburyo bwo kugera ku makuru no gucunga imyirondoro y'abantu;	d) Access controls and identity management ;	d) Contrôles d'accès et gestion de l'identité ;
e) Gukora gahunda y'ikomeza ry'ibikorwa by'ubucuruzi no gusubukura imirimo nyuma y'amage no gutegura ibikenewe muri urwo rwego;	e) Business continuity and disaster recovery planning and resources ;	e) Planification et ressources pour la continuité 'd'activité et la reprise après sinistre ;
f) Imikorere y'uburyo bukoresha ikoranabuhanga n'ibibazo bijyanye n'uko ubwo buryo buboneka;	f) Systems operations and availability concerns ;	f) Opérations des systèmes et problèmes de disponibilité
g) Umutekano w'uburyo bukoresha ikoranabuhanga n'uw'umuyoboro;	g) Systems, applications and network security;	g) Sécurité des systèmes et du réseau;
h) Kugenzura uburyo bukoresha ikoranabuhanga n'muyoboro;	h) Systems, applications and network monitoring;	h) Contrôle des systèmes et du réseau;
i) Gutunganya uburyo bukoresha ikoranabuhanga no kunoza imikorere yabwo;	i) Application development, acquisition and quality assurance;	i) développement des systèmes et d'applications et assurance de qualité ;
j) Umutekano w'ahantu hakorerwa no gukora amagenzura mu rwego rw'ibidukikije;	j) Physical security and environmental controls;	j) Sécurité physique et conditionnement de l'environnement ;
k) Ibanga ry'amakuru yerekeye abakiriya;	k) Customer data privacy ;	k) La confidentialité des données des clients ;
l) Imicungire y'ugurisha n'iy'utanga serivisi;	l) vendor and third party service provider management;	l) Gestion du vendeur et du tiers prestataire de services ;

m) Isuzuma ry'ibyateza ingorane ; no

n) Igisubizo ku bikorwa byo guhungabanya umutekano ;

o) Ubukangurambaga ku bakozi ku bijyanye n'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;

p) Ibisabwa k'ubunyangamugayo bw'abakozi bakoresha amakuru n'imiyoboro ;

q) Ubugenzuzi bw'imiyoboro, bw'ahabikwa amakuru y'umukiliya n'uburyo agerwaho ;

m) Risk management ; and

n) Incident management ;

o) Awerness of staff with regard to sybersecurity ;

p) Integrity requirements requirments of staff dealing with data, systems and networks ;

q) Controls to systems, physical locations containing customer information and tools to monitor access by authorized persons.

m) Evaluation des risques ; et

n) Réponse aux incidents ;

o) Sensibilition du personnel en matière de sybersécurité;

p) Exigences relatives aux exigences d'intégrité du personnel traitant les données, les systèmes et les réseaux ;

q) Contrôles aux systèmes, emplacements physiques contenant des informations sur les clients et outils pour surveiller l'accès par des personnes autorisées

Ingingo ya 7: Amasuzuma yo kugerageza kwinjira no kureba intege nke

Gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ya buri banki igomba guteganya ibikorwa by'igenzura n'iby'igerageza; bigategurwa hashingiwe ku isuzuma ry'ibyateza ingorane rikozwe na banki, bigashyirwaho hagamijwe gukora isuzuma ry'ubushobozi bw'iyo gahunda. Ibikorwa by'igenzura n'igerageza bigizwe n'igenzura rihoraho cyangwa kugerageza kwinjira mu buryo bukoresha ikoranabuhanga n'amasuzuma ngarukagihe y'intege nke zabwo. Mu gihe hatariho igenzura rikwiye rihoraho cyangwa hatariho ubundi buryo bwo

Article 7: Penetration Testing and Vulnerability Assessments

The cybersecurity program for each bank must include monitoring and testing, developed in accordance with the bank's risk assessment, designed to assess the effectiveness of the bank's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities, bank's must conduct:

Article 7: Test d'intrusion et évaluations de vulnérabilité

Le programme de cybersécurité de chaque banque doit comprendre les mécanismes de contrôle et des tests développés conformément à l'évaluation des risques de la banque et conçus pour évaluer l'efficacité du programme de cybersécurité de la banque. Le contrôle et les tests doivent inclure un contrôle continu ou des tests d'intrusion périodiques ainsi que des évaluations de vulnérabilité. En l'absence d'un contrôle efficace continu ou d'autres systèmes de détection continue des changements au sein des systèmes d'information qui pourraient créer

gutahura ku buryo buhoraho impinduka mu buryo bukoresha ikoranabuhanga zishobora kubutera intege nke cyangwa kuzigaragariza ibimenyetso, amabanki agomba gukora ibi bikurikira:

a) **Kugerageza kwinjira** mu buryo bukoresha ikoranabuhanga bwa banki bikorwa buri mwaka hashingiwe ku byateza ingorane byatahuwe mu isuzuma ry'ibyateza ingorane ryakozwe; na

b) Amasuzuma y'ahari intege nke akorwa kabiri mu mwaka arimo ibikorwa byo kugenzura no gusubiramo neza uburyo bukoresha ikoranabuhanga biteguwe neza hagamijwe gutahura ibibazo byerekeranye n'intege nke mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho zigaragara mu buryo bukoresha ikoranabuhanga bukoreshwa na banki zizwi na bose hashingiwe ku isuzuma ry'ibyateza ingorane ryakozwe.

<u>Ingingo ya 8</u>: Inzira y'ubugenzuzi

Ishingiye ku isuzuma ry'ibyateza ingorane ryakozwe, buri banki igomba kugira, mu gihe bishoboka, uburyo butekanye:

les vulnérabilités ou en donner des indications, les banques doivent mener :

a) **Annual penetration testing** of the bank's information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

b) **Bi-annual vulnerability assessments**, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the bank's information systems based on the risk assessment.

<u>Article 8</u>: Audit Trail

Each bank must securely maintain systems that, to the extent applicable and based on its risk assessment:

a) **des tests d'intrusion annuels** des systèmes d'information de la banque déterminés chaque année en fonction des risques identifiés selon l'évaluation des risques ; et

b) **Des évaluations de vulnérabilité semi-annuelles,** y compris des examens systématiques ou des révisions des systèmes d'information raisonnablement conçus pour identifier les vulnérabilités de cybersécurité connues du public dans les systèmes d'information de la banque sur base de l'évaluation des risques.

<u>Article 8</u>: Piste d'audit

Chaque banque doit maintenir en toute sécurité des systèmes qui, dans la mesure du possible et sur base de son évaluation des risques:

a) bukoze ku rwego bushobora kugarura ibikorwa by'imari kandi bufatika bihagije kugira ngo bushobore gushyigikira ibikorwa n'ishingano zisanzwe za banki; no

b) Gushyiraho inzira z'igenzura zigomba gutahura no gutanga ibisubizo ku bikorwa bihungabanya y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bishobora guhungabanya igice kimwe gifatika cy'ibikorwa bisanzwe bya banki.

Ingingo ya 9: Gucunga umutekano w'imirongo itwara amakuru isimbura iyindi

(9.1) Banki igomba kwita ku nzira zikurikizwa mu kumenya umwirondoro w'umukiriya uko bikwiye (KYC)igihe yandika umukiriya muri serivisi z'imari zitangwa hakoreshejwe interineti cyangwa uburyo bwimuka, ikarinda uko bikwiye amakuru akwiye kwitonderwa cyane, ikarinda umutekano w'ibyimukanwa uko bikwiye kandi igaha amahugurwa abakoresha uburyo bw'ikoranabuhanga.

(9.2) Ikoranabuhanga rya banki rigomba guhuzwe r'iry'urwego ry'irangamuntu kugirango abeho uburyo bwo gutahura umukiriya.

a) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the bank; and

b) include audit trails designed to detect and respond to cybersecurity incidents that have reasonable likelihood of materially harming any material part of the normal operations of the bank.

Article 9: Alternative Delivery Channels (ADC) Security Management

(9.1) The bank must ensure adequate Know Your Customer (KYC) procedures during customer registration for online and Mobile Financial Services, adequate sensitive data protection, adequate mobile security protection and user training.

(9.2) the core banking systems must be intergeted with National Identification system for the customer identity verification mechanism.

a) sont conçus de façon à reconstruire les transactions financières importantes suffisant pour supporter les opérations et obligations normales de la banque ; et

b) incluent des pistes d'audit conçus pour détecter et répondre aux incidents de cybersécurité qui vraisemblablement peuvent porter atteinte sérieuse à une partie considérable des activités normales de la banque.

Article 9: Gestion de la sécurité des canaux de distribution alternatifs

(9.1) La banque doit veiller à ce qu'il y ait des procédures adéquates de « Connaissance de son Client (KYC) » lors de l'inscription des clients pour les services financiers en ligne ou mobiles, une protection appropriée des données sensibles, une protection appropriée de la sécurité mobile et la formation des utilisateurs.

(9.2) les systèmes bancaires de base doivent être intervertis avec le système national d'identification pour le mécanisme de vérification de l'identité du client.

(9.3) Banki igomba gukoresha uburyo bw'umutekano butuma umuntu uwo ari we wese atemererwa kugera ku makuru akwiye kwitonderwa cyane yaba abitswe cyangwa ari mu nzira aherererekanywa nk'uko biteganywa n'aya mabwiriza.

(9.3) The bank shall employ security mechanisms that prevent unauthorized access to sensitive data at rest or in transit as contained in this regulation.

(9.3) La banque doit employer des mécanismes de sécurité qui préviennent un accès non autorisé aux données sensibles en repos ou en transit tels que prévus dans le présent règlement.

Ingingo ya 10 : Isuzuma ry'ibibazo bishobora kuvuka

Article 10 : Risk Management

Article 10 : Evaluation des risques

(10.1) Buri banki igomba gukora isuzuma ngarukagihe rihagije ry'ibyateza ingorane mu rwego rw'uburyo bukoresha ikoranabuhanga kugira ngo habashe gutunganywa gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho nk'uko biteganywa n'aya mabwiriza. Bene iryo suzuma ry'ibyateza ingorane rigomba kugenda rihuzwa n'igihe uko bishoboka kose mu rwego rwo gukemura ibibazo bijyanye n'impinduka zibonetse mu buryo bukoreshwa na banki bukoresha ikoranabuhanga, mu makuru atari rusange kimwe no mu bikorwa by'ubucuruzi byayo.

10.1) Each bank shall conduct a periodic risk assessment of the bank's information systems sufficient to inform the design of the cybersecurity program as required by this regulation. Such risk assessment shall be updated as reasonably necessary to address changes to the bank's information systems, non public information or business operations.

(10.1) Chaque banque doit mener une évaluation périodique des risques auxquels ses systèmes d'information font face suffisante pour informer la conception du programme de cybersécurité tel que requis par le présent règlement. Cette évaluation des risques doit être mise à jour aussi raisonnablement que nécessaire en vue de répondre aux changements des systèmes d'information de la banque, des informations non publiques ou des opérations commerciales.

(10.2) Isuzuma ry'ibyateza ingorane banki rigomba guteganya ivugururwa ry'amagenzura kugira ngo uburyo bukoreshwa bubashe kujyana n'iterambere ry'ikoranabuhanga kimwe no gukemura ibibazo biba byugarije uburyo bukoresha ikoranabuhanga kandi rigomba kwita ku byateza ingorane byihariye mu bikorwa bya banki bifite aho bihuriye

10.2) The bank's risk assessment must allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the bank's business operations related to cybersecurity, non public information collected or stored, information systems utilized and the

(10.2) L'évaluation des risques de la banque doit prévoir des possibilités de révision des contrôles en vue de répondre aux développements technologiques et aux menaces évolutives et doit considérer les risques particuliers des opérations commerciales de la banque relatifs à la cybersécurité, aux informations non

y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, amakuru atari rusange yakusanyijwe cyangwa abitswe, uburyo bukoresha ikoranabuhanga bukoreshwa cyangwa no kuba uburyo bwo kugenzura buboneka kandi bukora neza mu rwego rwo kurinda amakuru atari rusange cyangwa uburyo bukoresha ikoranabuhanga.

(10.3) Isuzuma ry'ibyateza ingorane rikorwa hakurikijwe politiki n'inzira zikurikizwa zanditswe kandi ibirivuyemo bikandikwa. Izo politiki n'izo nzira zikurikizwa ziba zikubiyemo:

a) ibigenderwaho mu gusuzuma no gushyira mu byiciro ibyateza ingorane mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho byabonetse cyangwa ibibazo byugarije banki muri urwo rwego;

b) ibigenderwaho mu gusuzuma ibanga, ubudakemwa, umutekano n'iboneka ry'uburyo bukoresha ikoranabuhanga bukoreshwa na banki kimwe n'amakuru atari rusange harimo no kuba uburyo bwo kugenzura bukwiye hakurikijwe ibyateza ingorane byagaragaye; no

availability and effectiveness of controls to protect nonpublic information and information systems.

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

a) Criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the bank;

b) Criteria for the assessment of the confidentiality, integrity, security and availability of the bank's/FI information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and

publiques collectées ou stockées, aux systèmes d'information utilisés et à la disponibilité et l'efficacité des contrôles en vue de la protection des informations non publiques et des systèmes d'information.

(10.3) L'évaluation des risques doit être menée conformément aux politiques et procédures écrites et doit être documentée. De telles politiques et procédures doivent comprendre:

a) les critères d'évaluation et de catégorisation des risques de cybersécurité identifiés ou de menaces auxquelles la banque est confrontée;

b) les critères d'évaluation de la confidentialité, de l'intégrité, de la sécurité et de la disponibilité des systèmes d'information de la banque et des informations non publiques comprenant l'adéquation des contrôles existants dans le contexte des risques identifiés ; et

c) ibisabwa bigaragaza uburyo ubukana bw' ibyateza ingorane byagaragaye bushobora kugabanywa cyangwa kwakirwa hashingiwe ku isuzuma ry' ibyateza ingorane ryakozwe n'uburyo gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho izabasha gukemura izo ngorane.

Ingingo ya 11: Undi muntu utanga serivisi

(11.1) Banki igomba gushyira mu bikorwa politiki n'inzira zikurikizwa zanditswe hagamijwe kubungabunga umutekano w'uburyo bukoresha ikoranabuhanga n'amakuru atari rusange ashobora kugerwaho cyangwa abitswe n'abandi batanga serivisi. Izo politiki n'izo nzira zikurikizwa zigomba gushingira ku isuzuma ry'ibyateza ingorane ryakozwe na banki kandi, aho bishoboka hose, zigomba kugira icyo ziteganya kuri ibi bikurikira:

a) Itahurwa n'isuzuma ry'ibyateza ingorane byerekeranye n'abandi bantu batanga serivisi;

b) Imigenzereze y'ibanza ishoboka yo mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi

c) Acceptance criteria describing how identified risks will be treated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Article 11: Third Party Service Provider

(11.1) The bank must implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers. Such policies and procedures shall be based on the risk assessment of the bank and shall address to the extent applicable:

a) the identification and risk assessment of third party service providers;

b) minimum cybersecurity practices required to be met by such third

c) les exigences qui décrivent comment les risques identifiés seront mitigés ou acceptés compte tenu de l'évaluation des risques et la façon dont le programme de cybersécurité traitera ces risques.

Article 11: Tiers prestataire de services

(11.1) La banque doit mettre en exécution des politiques et des procédures écrites conçues pour assurer la sécurité des systèmes d'information et des informations non publiques qui sont accessibles aux tiers prestataires de services ou détenues par eux. De telles politiques et procédures doivent être basées sur l'évaluation des risques de la banque et doivent porter, dans la mesure du possible, sur :

a) l'identification et l'évaluation des risques des tiers prestataires de services ;

b) le minimum de pratiques de cybersécurité exigées aux tiers prestataires de service pour faire des affaires avec la banque;

n'itumanaho isabwa kuba yujujwe n'abandi bantu batanga serivisi kugira ngo babashe gukorana na banki muri urwo rwego;

party service providers in order for them to do business with the bank;

c) Inzira zo kugenzura mu bushishozi zikoreshwa mu gusuzuma niba imigenzereze y'abo bantu bandi batanga serivisi mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ikwiye;

c) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers; and

c) les processus de diligence raisonnable utilisés pour évaluer l'efficacité des pratiques de cybersécurité de ces tiers prestataires de service ; et

d) Gukorera isuzuma ngarukagihe abo bandi batanga serivisi hashingiwe ku ngorane bigaragara ko bashobora guteza no ku kuba imigenzereze yabo mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ihora ikwiye.

d) periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

d) l'évaluation périodique de ces tiers prestataires de services sur base des risques qu'ils présentent et l'efficacité continue de leurs pratiques de cybersécurité.

(11.2) Izo politiki n'inzira zikurikizwa zigomba kuba zikubiyemo imirongo ngenderwaho yo kumenya imyifatire ndetse no kurinda amasezerano yerekeranye n'abandi batanga serivisi harimo uko bishoboka kose imirongo ngenderwaho mu gusuzuma:

(11.2) Such policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to third party service providers including to the extent applicable guidelines addressing:

(11.2) De telles politiques et procédures doivent comprendre les principes directeurs appropriés d'identification et/ou les protections contractuelles en rapport avec les tiers prestataires de services y compris, dans la mesure du possible, des principes directeurs qui traitent :

a) politiki n'inzira zikurikizwa n'undi muntu utanga serivisi mu kugenzura uburyo bwo kugera ku makuru harimo imikoreshereze y'uburyo bwo gusuzuma umwirondoro

a) the third party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by

a) les politiques et les procédures de contrôles d'accès du tiers prestataire de services y compris son utilisation d'authentification multi- factorielle

hagendewe ku bintu byinshi nk'uko biteganywa mu ngingo ya 12 y'aya mabwiriza, hagamije kugabanya abashobora kugera ku buryo bukoresha ikoranabuhanga bukoreshwa kimwe no ku makuru atari rusange;

b) politiki n'inzira zikurikizwa n'undi muntu utanga serivisi mu gukoresha uburyo bw'ibanga nk'uko bisabwa mu ngingo ya 12 y'aya mabwiriza hagamijwe kurinda amakuru atari rusange ari mu nzira ahererekanywa cyangwa abitswe;

c) Imenyesha rigomba gukorerwa banki mu gihe habayeho ikibazo cy'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho gifite ingaruka zitaziguye ku buryo bukoresha ikoranabuhanga bwa banki cyangwa ku makuru yayo atari rusange abitswe n'undi muntu utanga serivisi; na

d) amamenyekanisha n' ubwiyemeze bitangwa kuri politiki n'inzira zikurikizwa n'undi muntu utanga serivisi mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ku byerekeranye n'umutekano w'uburyo bukoresha ikoranabuhanga bukoreshwa na banki cyangwa uw'amakuru yayo atari rusange.

Article 12 of this Regulation, to limit access to relevant Information systems and non-public information;

b) the third party service provider's policies and procedures for use of encryption as required by Article 12 of this Regulation to protect non-public information in transit and at rest;

c) notice to be provided to the bank in the event of a cybersecurity incident directly impacting the bank's/FI information systems or the bank's non-public information being held by the third party service provider; and

d) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the bank's/FI information systems or non-public information.

conformément à l'article 12 du présent Règlement en vue de limiter l'accès aux systèmes d'information et aux informations non publiques concernés ;

b) les politiques et les procédures du tiers prestataire de services pour l'utilisation du chiffrement conformément à l'Article 12 du présent Règlement en vue de protéger des informations non publiques en transit ou en repos ;

c) une notification à donner à la banque en cas d'incident de cybersécurité qui a un impact direct sur les systèmes d'information de la banque ou sur des informations non publiques de la banque détenues par le tiers prestataire de services ; et

d) les déclarations et garanties concernant les politiques et les procédures de cybersécurité du tiers prestataire de services ayant trait à la sécurité des systèmes d'information ou aux informations non publiques de la banque.

Ingingo ya 12: Gusuzuma umwirondoro hakoreshejwe ibintu byinshi

(12.1) Ishingiye ku isuzuma ry'ibyayiteza ingorane yakoze, buri banki igomba gukoresha amagenzura akwiye ashobora kuba akubiyemo gusuzuma umwirondoro w'abantu hakoreshejwe ibintu byinshi bibaranga cyangwa gusuzuma umwirondoro w'abantu hashingiwe ku byateza ingorane hagamijwe kubakumira kugera ku makuru atari rusange cyangwa k'uburyo bukoresha ikoranabuhanga banki ikoresha.

(12.2) Gusuzuma umwirondoro w'umuntu hakoreshejwe ibintu byinshi bimuranga bigomba gukorwa ku muntu uwo ari we wese winjira mu miyoboro ya banki y'imbere anyuze mu miyoboro yo hanze cyeretse gusa iyo ukuriye ISU yemeye mu nyandiko ikoreshwa ry'ubundi buryo bumeze nk'ubwo cyangwa ubundi buryo bw'igenzura bufite umutekano kurusha ubwongubwo.

Article 12: Multi-Factor Authentication

(12.1) Based on its risk assessment, each bank shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems.

(12.2) Multi-factor authentication shall be utilized for any individual accessing the bank's internal networks from an external network, unless the bank's head of ISU has approved in writing the use of reasonably equivalent or more secure access controls.

Article 12: Authentification multi-factorielle

(12.1) Sur base de son évaluation des risques, chaque banque doit utiliser des outils de contrôle efficaces qui peuvent comprendre une authentification multi – factorielle ou une authentification basée sur des risques en vue de se protéger contre l'accès non autorisé aux informations non publiques ou systèmes d'information.

(12.2) L'authentification multifactorielle doit être utilisée pour toute personne qui accède aux réseaux internes de la banque à partir d'un réseau externe, à moins que le chargé de ISU de la banque n'ait approuvé par écrit l'utilisation des outils de contrôle d'accès raisonnablement équivalents ou plus sécurisés.

Ingingo ya 13: Igabanywa ry'amakuru agomba kubikwa

Mu rwego rwa gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, buri banki igomba gushyiraho politiki n'inzira zikurikizwa mu gushyingura mu buryo bwizewe kandi mu buryo buhoraho amakuru yose atari rusange, cyeretse gusa iyo ayo makuru agomba

Article 13: Limitations on Data Retention

As part of its cybersecurity program, each bank must have a data retention policy for the secure keeping and disposal on a periodic basis of any nonpublic information identified as per their Risk assessment, except where such information is otherwise required to be retained by law or regulation.

Article 13: Limitations sur la rétention des données

Dans le cadre de son programme de cybersécurité, chaque banque doit inclure des politiques et des procédures de disposition sécurisée, de façon périodique, de toute information non publique, sauf là où ces informations doivent être conservées en vertu de la loi ou d'un règlement.

kubikwa hakurikijwe ibisabwa n'itegeko cyangwa amabwiriza.

Ingingo ya 14: Amahugurwa n'igenzurwa ry'ukoresha uburyo bukoresha ikoranabuhanga

(14.1) Mu rwego rwa gahunda yayo y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, buri banki igomba:

a) gushyira mu bikorwa politiki, inzira zikurikizwa n'amagenzura ashingiye ku byateza ingorane hagamijwe kugenzura ibikorwa by'abakoresha uburyo bukoresha ikoranabuhanga babyemerewe no gutahura abagera cyangwa abakoresha ubu buryo batabyemerewe ;

b) Guha buri gihe abakozi bose amahugurwa ajyanye n'igihe agaragaza ibyateza ingorane byagaragajwe mu isuzuma ry'ibyateza ingoraneryakozwe na banki kugira ngo babashe kugira imyumvire ikwiye ku umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;

c) Kugenzura akamaro k'amahugurwa biciye mu bibazo n'igeerageza ;

Article 14: User Training and Monitoring

(14.1) As part of its cybersecurity program, each bank must:

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

b) provide regular cybersecurity awareness training for all personnel that interacts with institution's information system including but not limited to staff, interns, third party ;

c) evaluate the effectiveness of the awareness training through regular quizes and test simulations.

Article 14: Formation et contrôle de l'utilisateur

(14.1) Dans le cadre de son programme de cybersécurité, chaque banque doit :

a) mettre en œuvre des politiques, des procédures et des contrôles basés sur des risques conçus pour contrôler les activités des utilisateurs autorisés et pour détecter l'accès ou l'utilisation non autorisés ;

b) donner à tout le personnel une formation régulière de prise de conscience sur la cybersécurité qui est à jour pour refléter les risques identifiés par la banque dans son évaluation des risques ;

c) évaluer l'efficacité de la sensibilisation au moyen de tests réguliers et de test de simulations.

<u>Ingingo ya 15</u>: Kurinda amakuru atari rusange

(15.1) Nka kimwe mu bigize gahunda yayo y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho kandi ishingiye ku isuzuma ry' ibyateza ingorane, buri banki igomba gushyira mu bikorwa uburyo bwo kugenzura burimo gusobeka hagamijwe kurinda amakuru atari rusange abitswe cyangwa yoherejwe na banki yaba ari mu nzira mu miyoboro yo hanze cyangwa abitswe.

(15.2) Mu gihe cyose banki isanze bidashoboka gusobeka makuru atari rusange ari mu nzira mu miyoboro yo hanze, ishobora kurinda bene ayo makuru yifashishije amagenzura asimbura ubwo buryo akora neza yasubiwemo kandi yemewe n'ukuriye ISU wa banki.

(15.3) Mu gihe cyose banki isanze bidashoboka gusobeka amakuru atari rusange abitswe, ishobora kurinda bene ayo makuru yifashishije amagenzura asimbura ubwo buryo akora neza yasubiwemo kandi yemewe n'ukuriye ISU wa banki.

<u>Article 15</u>: Encryption of Non-public Information

(15.1) As part of its cybersecurity program, based on its risk assessment, each bank shall implement controls, including encryption, to protect nonpublic information held or transmitted by the bank both in transit over external networks and at rest.

(15.2) To the extent a bank determines that encryption of nonpublic information in transit over external networks is infeasible, the bank may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the bank's head of ISU.

(15.3) To the extent a bank determines that encryption of Nonpublic Information at rest is infeasible, the bank may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the bank's head of ISU.

<u>Article 15</u>: Cryptage des informations non publiques

(15.1) Dans le cadre de son programme de cybersécurité et sur base de son évaluation des risques, chaque banque doit mettre en œuvre des contrôles, y compris le cryptage, pour protéger des informations non publiques gardées ou transmises par la banque qu'elles soient en transit sur des réseaux externes ou au repos.

(15.2) Dans la mesure où la banque estime que le cryptage des informations non publiques en transit sur des réseaux externes n'est pas faisable, celle ci peut par contre sécuriser de telles informations non publiques en utilisant des contrôles compensatoires efficaces examinés et approuvés par le chargé de ISU de la banque.

(15.3) Dans la mesure où la banque estime que le cryptage des informations non publiques en repos n'est pas faisable, celle ci peut par contre sécuriser de telles informations non publiques en utilisant des contrôles compensatoires efficaces examinés et approuvés par le chargé de ISU la banque.

(15.4) Mu gihe cyose banki ikoresha amagenzura asimbura uburyo bw'ibanga nk'uko byavuzwe haruguru, ISU agomba kongera gusuzuma niba irindamakuru rikoresha isobeka rishoboka n'imikorere y'amagenzura arisimbura nibura buri mwaka .

(15.4) To the extent that a bank is utilizing compensating controls as mentioned above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by ISU at least annually.

(15.4) Dans la mesure où une banque est en train d'utiliser des contrôles compensatoires tels que mentionnés ci-haut, le ISU doit passer en revue au moins une fois par an la faisabilité du cryptage et l'efficacité des contrôles compensatoires.

<u>Ingingo ya 16</u> Gahunda yo gukemura ibibazo bivutse

(16.1) Mu rwego rwa gahunda yayo y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, buri banki igomba gushyiraho gahunda yo gukemura ibibazo bivutse yanditse igamije gukemura ibyo bibazo ako kanya no kuyikura mu kibazo icyo aricyo cyose cyerekeranye n'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho kibangamira ibanga , ubudakemwa cyangwa ukuboneka k'uburyo bukoresha ikoranabuhanga bukoreshwa na banki cyangwa imikorere ihoraho y'ubwoko ubwo ari bwo bwose bw'ubucuruzi cyangwa bw'ibikorwa bya banki.

<u>Article 16</u> Incident Response and business continuity management

(16.1) As part of its cybersecurity program, each bank shall establish a written incident response and business continuity management plan designed to promptly respond to, and recover from, any cybersecurity incident materially affecting the confidentiality, integrity or availability of the bank's information systems or the continuing functionality of any aspect of the bank's business or operations.

<u>Article 16</u> Plan d'intervention en cas d'incident

(16.1) Dans le cadre de son programme de cybersécurité, chaque banque doit élaborer un plan écrit d'intervention en cas d'incident conçu pour réagir et sortir ponctuellement d'un incident de cybersécurité qui affecte matériellement la confidentialité, l'intégrité ou la disponibilité des systèmes d'information de la banque ou la fonctionnalité continue d'un aspect quelconque de ses activités ou de ses opérations.

(16.2) Iyo gahunda yo gukemura ibibazo bivutse igomba kwita kuri ibi bintu bikurikira:

(16.2) Such incident response and business continuity management plan shall address the following areas:

(16.2) Ce plan d'intervention en cas d'incident doit porter sur les aspects repris ci-après:

a) Inzira zikurikizwa muri banki imbere zo gukemura ikibazo cyerekeranye n'igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;

b) Intego za gahunda yo gukemura ibibazo bivutse;

c) Gusobanura mu buryo bwumvikana uruhare, inshingano n'inzego z'ubuyobozi zifatirwamo ibyemezo;

d) Itumanaho no guhanana amakuru imbere muri banki no hanze yayo ;

e) Kumenya ibikenewe mu rwego rwo kongera ingufu ahagaragaye intege nke mu buryo bwo guhanahana amakuru bukoreshwa n'ubugenzuzi bijyana;

f) Gukora inyandiko na raporo ku bikorwa bihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho no ku bikorwa byerekeranye no gukemura ibibazo byavutse; no

g) Gusuzuma no gusubiramo gahunda yo gukemura ibibazo bivutse uko bibaye ngombwa hakurukijwe

a) the internal processes for responding to cybersecurity incident and disasters;

b) the goals of the incident response and business continuity plans;

c) the definition of clear roles, responsibilities and levels of decision-making authority;

d) external and internal communications and information sharing;

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

f) documentation and reporting regarding cybersecurity events and related incident response activities; and

g) the evaluation and revision as necessary of the incident response

a) les processus internes de réponse à un incident de cybersécurité;

b) les objectifs du plan d'intervention en cas d'incidents;

c) la définition claire des rôles, responsabilités et niveaux d'autorité de prise de décision;

d) communications et échange d'information externes et internes;

e) Identification des besoins pour remédier à toutes les faiblesses identifiées dans les systèmes d'information ainsi que les contrôles associés ;

f) la documentation et production de rapports concernant les événements de cybersécurité ainsi que les activités connexes d'intervention en cas d'incident ; et

g) l'évaluation et la révision au tant que nécessaire du plan d'intervention

igikorwa gihungabanya y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho cyabaye.

Ingingo ya 17 Imenyesha rikorerwa Banki Nkuru

(17.1) Banki igomba kumenyesha Banki Nkuru ako kanya uko bishoboka mu gihe kitarenze amasaha abiri (2) uhereye igihe icyo gikorwa cyibereyeho cyangwa igihe hamenyekanye ko habayeho igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho gishobora kuba kiri muri bumwe muri ubu bwoko bukurikira:

a) Igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho gishobora kubuza ishami runaka rya banki gukomeza ibikorwa byaryo bisanzwe byo guha serivisi z'imari abakiriya baryo, cyangwa

b) Ibikorwa bihungabanya y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho uko bigaragara bishobora guhungabanya kuburyo bugaragara igice gifatika cy'ibikorwa bisanzwe bya banki.

and business continuity plans following a cybersecurity event.

Article 17 Notices to the Central Bank

(17.1) The bank must notify Central Bank as promptly as possible within a period not exceeding two (2) hours from the occurrence of the incident or from a determination that a cybersecurity incident has occurred that is either of the following:

a) cybersecurity incident that may prevent a specific bank branch from continuing its normal operations for customer-facing transactions, and

b) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the bank.

en cas d'incident à la suite d'un événement de cybersécurité.

Article 17 Notifications à la Banque Centrale

(17.1) La banque doit notifier à la Banque Centrale aussi rapidement que possible endéans une période ne dépassant pas deux (2) heures à compter de la survenance de l'incident ou de la constatation qu'il s'est produit un incident de cybersécurité qui peut revêtir l'un des aspects suivants :

a) un incident de cybersécurité qui peut empêcher une succursale bancaire donnée de continuer ses activités normales dans le cadre des opérations avec les clients, et

b) des événements de cybersécurité qui peuvent vraisemblablement porter atteinte sérieuse à une partie importante des activités normales de la banque.

(17.2) Banki igomba gushyikiriza Banki Nkuru raporo yuzuye y'igikorwa gihungabanya umutekano mu gihe cy'amasaha 24 kuva igikorwa kibaye.

(17.3) Banki igomba gushyikiriza Banki Nkuru inyandiko nk'uko igaragara ku mugereka yemeza ko gahunda ya banki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho yubahiriza ibyo isabwa n'aya mabwiriza. Iyo nyandiko igomba gushyikirizwa Banki Nkuru mu gihe kitarenze itariki ya 15 Mutarama buri mawaka.

(17.2) The Bank must submit to the Central Bank the full incident report within 24 hours from the occurrence of the incident.

(17.3) The bank shall submit to the Central Bank on annual basis a written statement as per the appendix certifying that the bank cyber securtiy 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.

(17.2) La Banque doit soumettre à la Banque Centrale le rapport d'incident complet dans les 24 heures suivant la survenance de l'incident.

(17.3) La banque doit transmettre annuellent à la Banque Central une déclaration écrite certifiant que le programme de cybersecurité se conforme aux exigences du présent Règlement. Cette declaration doit etre tramsmit au plus tard le 15 janvier de chaque année

Ingingo ya 18 Ibyerekeranye n'ibanga

Amakuru atangwa na banki hakurikijwe aya mabwiriza ntarebwa n'ingingo z'itangaza ry'amakuru z'Itegeko rigena imitunganyirize y'imirimo y'amabanki cyangwa irindi tegeko bijyanye.

Article 18 Confidentiality

Information provided by a bank pursuant to this Regulation is subject to exemptions from disclosure under the Banking Law or any other applicable law.

Article 18 Confidentialité

Les informations fournies par une banque conformément au présent Règlement sont sujettes à des dispenses de divulgation conformément à la Loi portant organisation de l'activité bancaire ou à toute autre loi applicable.

UMUTWE WA III: INGINGO ZINYURANYE N'IZISOZA

Ingingo ya 19 Ibihano n'ibyemezo byo mu rwego rw'ubutegetsi

Iyo banki itabashije kubahiriza ibisabwa muri aya mabwiriza, Banki Nkuru ishobora kuyifatira ibihano biteganywa n'Itegeko rigena imitunganyirize

CHAPTER III: MISCELLANEOUS AND FINAL PROVISIONS

Article 19 Penalties and administrative sanctions

Where the bank fails to satisfy any of the requirements of this Regulation, the Central Bank may apply any sanctions available under relevant provisions of the Law concerning

CHAPITRE III: DISPOSITIONS DIVERSES ET FINALES

Article 19 Pénalités et sanctions administratives

Lorsqu' une banque ne parvient pas à répondre aux exigences du présent Règlement, la Banque Centrale peut appliquer toute sanction prévue par les dispositions applicables de la Loi portant

y'imirimo y'amabanki cyangwa mu ngingo z'amabwiriza akurikizwa.

Ingingo ya 20 : Igihe ntarengwa cyo kubahiriza zimwe mu ngingo z' aya mabwiriza

Amabanki ahawe igihe kitarenze amezi icumi n'umunane (18) uhereye igihe iri tegeko ritangarijwe mu Igazeti ya Leta ya Repubulika y'u Rwanda kugira ngo abe yahuje imikorere yayo n'ibiteganywa mu ngingo ya 3 y'aya mabwiriza.

Amabanki ahawe igihe cy'amazi atandatu (6) kugirango zubahiruze ibikubiye muri ngo ya 4, iya 4 n'iya 6 y'aya mabwiriza, uhereye igihe uhereye igihe atangarijwe mu Igazeti ya Repubulika y'u Rwanda

Ingingo ya 21: Ivanwaho ry'ingingo z'amabwiriza zinyuranyije n'aya amabwiriza

Ingingo zose zinyuranye n'aya mabwiriza zivanyweho.

Ingingo ya 22: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange

Aya mabwiriza rusange yateguwe, asuzumwa kandi yemezwa mu rurimi rw'icyongereza.

organization of banking and/or provisions of a relevant regulation.

Article 20 : Deadline for conforming to certain provisions of this regulation

Banks shall have eighteen (18) months as from the entry into force of this regulation to conform their functioning with the provisions of article 3 of this regulation.

Banks are given a maximun of six (6) months to comply with provisions of Article 4, 5 and 6 of this regulation, starting from the date of its publication in the Official Gazette of the Republic of Rwanda.

Article 21: Repealing provisions

All previous provisions contrary to this Regulation are hereby repealed.

Article 22: Drafting, consideration and approval of this Regulation

This Regulation was drafted, considered and approved in English.

organisation de l'activité bancaire et/ou les dispositions d'un règlement applicable.

Article 20 : Délai de conformité aux certain dispositions du présent règlement

Les banques disposent d'un delai de dix huit (18) mois pour se conformer aux exigences de l'article 3 de present règlement, suivant la date la date d'entrée en vigueur du présent reglement.

Les banques disposent d'un maximum de six (6) mois pour se conformer aux dispositions des article 4,5 et 6 du present règlement, suivant la date de sa publication au Journal Officiel de la République du Rwanda.

Article 21: Dispositions abrogatoires

Toutes les dispositions antérieures contraires au présent règlement sont abrogées.

Article 22: Initiation, examen et approbation du présent Règlement

Le présent Règlement a été initié, examiné et approuvé en anglais.

Ingingo ya 23: Igihe aya mabwiriza atangirira gukurikizwa

Aya mabwiriza atangira gukurikizwa ku umunsi atangarijweho mu igazeti ya Leta ya Repubulika y'u Rwanda.

Bikorewe i Kigali, ku wa 24/01/2018

(sé)
RWANGOMBWA John
Guverineri

Article 23: Commencement

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

Done at Kigali, on 24/01/2018

(sé)
RWANGOMBWA John
Governor

Article 23: Entrée en vigueur

Le présent règlement entre en vigueur le jour de sa publication au Journal Officiel de la République du Rwanda.

Fait à Kigali, le 24./01/2018

(sé)
RWANGOMBWA John
Gouverneur

APPENDIX A

_____

(**Bank Name)**

Date_ _ _____

Certification of Compliance with National Bank of Rwanda Cybersecurity Regulation

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

(1) The Board of Directors (or name of Senior Officer(s)) has 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 Cybersecurity Program of (name of Bank) 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 nymber).

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

(Name)_____Date: _____