AMABWIRIZA RUSANGE Nº 50/2022 YO KU WA 02/06/2022 YEREKEYE UMUTEKANO W'IBIJYANYE N'IKORANABUHANGA MU ITANGAZABUMENYI N'ITUMANAHO MU BIGO BIGENZURWA	REGULATION Nº 50 /2022 OF 02/062022 ON CYBER SECURITY IN REGULATED INSTITUTIONS	REGLEMENT Nº 50/2022 DU 02/06/2022 SUR LA CYBERSECURITE DANS LES INSTITUTIONS REGLEMENTEES
ISHAKIRO	**TABLE OF CONTENTS**	**TABLE DES MATIÈRES**
UMUTWE WA MBERE: INGINGO RUSANGE	**CHAPTER ONE: GENERAL PROVISIONS**	**CHAPITRE PREMIER: DISPOSITIONS GÉNÉRALES**
Ingingo ya mbere: Icyo aya mabwiriza rusange agamije	**Article one: Purpose**	**Article premier: Objet**
Ingingo ya 2: Abarebwa n'aya mabwiriza rusange	**Article 2: Scope**	**Article 2: Champ application**
Ingingo ya 3: Ibisobanuro by'amagambo	**Article 3: Definition of terms**	**Article 3: Définition des termes**
UMUTWE WA II: IBISABWA BIGOMBA KUBAHIRIZWA	**CHAPTER II: REGULATORY REQUIREMENTS**	**CHAPITRE II: EXIGENCES RÉGLEMENTAIRES**
Ingingo ya 4: Imiyoborere mu by'umutekano w'ibijyanye	**Article 4: Cyber security governance**	**Article 4: Gouvernance de la cybersécurité**

n'ikoranabuhanga mu itangazabumenyi n'itumanaho		
Ingingo ya 5: Komite y'Inama y'Ubutegetsi ishinzwe ikoranabuhanga	**Article 5: IT Board Committee**	**Article 5: Comité du conseil d'administration des technologies de l'information**
Ingingo ya 6: Komite nyobozi ishinzwe ikoranabuhanga	**Article 6: IT Steering Committee**	**Article 6: Comité de pilotage informatique**
Ingingo ya 7: Urwego rushyinzwe umutekano w'ikoranabuhanga	**Article 7: IT Security Function**	**Article 7: Fonction de sécurité informatique**
Ingingo ya 8: Ingamba zo gucunga umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	**Article 8: Cyber security strategy**	**Article 8: Stratégie de cybersécurité**
Ingingo ya 9: Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	**Article 9: Cyber security Policy**	**Article 9: Politique de cybersécurité**
Ingingo ya 10: Amasuzuma yo kugerageza kwinjira no kureba intege nke	**Article 10: Penetration Testing and Vulnerability Assessments**	**Article 10: Tests de pénétration et évaluations de la vulnérabilité**
Ingingo ya 11: Inzira y'ubugenzuzi	**Article 11: Audit Trail**	**Article 11: Piste d'audit**

Ingingo ya 12: Gucunga umutekano w'imirongo itwara amakuru isimbura iyindi	**Article 12: Alternative Delivery Channels (ADC) Security Management**	**Article 12: Gestion de la sécurité des canaux de distribution alternatifs (ADC)**
Ingingo ya 13: Gucunga ibyateza ingorane biturutse ku ikoranabuhanga	**Article 13: Cyber Risk Management**	**Article 13: Gestion des cyber risques**
Ingingo ya 14: Isuzuma ry'abatanga serivisi bavuye hanze	**Article 14: Assessment of a Service Provider**	**Article 14: Évaluation d'un fournisseur de services**
Ingingo ya 15: Uruhare rw'urwego rw'ubugenzuzi bw'imbere	**Article 15: Role of Internal Audit Function**	**Article 15: Rôle de la fonction d'audit interne**
Ingingo ya 16: Gusuzuma umwirondoro hakoreshejwe ibintu byinshi	**Article 16: Multi-Factor Authentication**	**Article 16: Authentification multifactorielle**
Ingingo ya 17: Igabanywa ry'amakuru agomba kubikwa	**Article 17: Limitations on Data Retention**	**Article 17: Limitations de la conservation des données**
Ingingo ya 18: Amahugurwa no kumenyekanisha	**Article 18: Training and awareness**	**Article 18: Formation et sensibilisation**
Ingingo ya 19: Guhisha amakuru y'imari	**Article 19: Encryption of non-public data**	**Article 19: Cryptage des données financières**
Ingingo ya 20: Gahunda yo gukemura ibibazo bivutse	**Article 20: Incident Response and business continuity management**	**Article 20: Réponse aux incidents et gestion de la continuité des activités**

Ingingo ya 21: Kumenyesha no gutanga raporo kubyabaye ku bijyanye n'ikoranabuhanga	**Article 21: Notification and reporting of the cyber incident**	**Article 21: Notification et signalement du cyber incident**
Ingingo ya 22: Inyandiko yo kwisuzuma	**Article 22: Statement of self assessment**	**Article 22: Déclaration d'auto-évaluation**
UMUTWE WA III: INGINGO ZINYURANYE N'IZISOZA	**CHAPTER III: MISCELLANEOUS AND FINAL PROVISIONS**	**CHAPITRE III: DISPOSITIONS DIVERSES ET FINALES**
Ingingo ya 23: Ikurikizwa ry'andi mategeko	**Article 23: Application of other laws**	**Article 23: Application d'autres lois**
Ingingo ya 24: Ibisabwa byihariye	**Article 24: Tailored requirements**	**Article 24: Exigences adaptées**
Ingingo ya 25: Ibihano n'ibyemezo byo mu rwego rw'ubutegetsi	**Article 25: Penalties and administrative sanctions**	**Article 25: Pénalités et sanctions administratives**
Ingingo ya 26: Igihe cy'inzibacyuho	**Article 26: Transition period**	**Article 26: Période de transition**
Ingingo ya 27: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange	**Article 27: Drafting, consideration and approval of this Regulation**	**Article 27: Initiation, examen et approbation du présent règlement**
Ingingo ya 28: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza rusange	**Article 28: Repealing provision**	**Article 28 : Disposition abrogatoire**
Ingingo ya 29: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza rusange	**Article 29 : Commencement**	**Article 29: Entrée en vigueur**

AMABWIRIZA RUSANGE Nº 50/2022 YO KU WA 02/06/2022 YEREKEYE UMUTEKANO W'IBIJYANYE N'IKORANABUHANGA MU ITANGAZABUMENYI N'ITUMANAHO MU BIGO BIGENZURWA	**REGULATION Nº 50 /2022 OF 02/06/2022 ON CYBER SECURITY IN REGULATED INSTITUTIONS**	**REGLEMENT Nº 50/2022 DU 02/06/2022 SUR LA CYBERSECURITE DANS LES INSTITUTIONS REGLEMENTEES**
Ishingiye ku Itegeko N° 48/2017 ryo kuwa 23/09/2017 rigenga Banki Nkuru y'u Rwanda nk'uko ryavuguruwe kugeza ubu, cyane cyane mu ngingo zaryo, iya 6, iya 6bis, iya 8, iya 9, iya 10 n'iya 15	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;	Vu la Loi N° 48/2017 du 23/09/ 2017 régissant la Banque Nationale du Rwanda telle que modifiée à ce jour, spécialement en ses articles, 6, 6bis, 8,9 ;10 and 15 ;
Ishingiye ku Itegeko N° 47/2017 ryo ku wa 23/09/2017 rigena imitunganyirize y'imirimo y'amabanki, cyane cyane mu ngingo zaryo, iya 37 n'iya 117;	Pursuant to Law N° 47/2017 of 23/09/2017 governing the organization of banking, especially in its Articles 37 and 117;	Vu la Loi N° 47/2017 du 23/09/2017 portant organisation de l'activité bancaire, spécialement en ses articles 37 et 117 ;
Ishingiye ku Itegeko N° 030/2021 ryo ku wa 30/06/2021 rigenga imitunganyirize y'umurimo w'ubwishingizi cyane cyane mu ngingo zaryo, iya 56, iya 57 n'iya 60 n'iya 82;	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;	Vu la Loi N° 030/2021 du 30/06/2021 régissant l'organisation d'activité d'assurance, spécialement en ses articles 56, 57, 58 60 et 82 ;
Ishingiye ku Itegeko N° 072/2021 ryo ku wa 05/11/2021 rigenga ibigo by'imari icyiriritse	Pursuant to Law N° 072/2021 of 05/11/2021 governing deposit-taking microfinance institutions, especially in its articles 23 and 24;	Vu Loi N° 072/2021 du 05/11/2021 régissant les institutions de microfinance de dépôt, spécialement en ses articles 23 et 24 ;

byakira amafaranga abitswa, cyane cyane mu ngingo zaryo, iya 23 n'iya 24;		
Ishingiye ku Itegeko N° 061/2021 ryo ku wa 14/10/2021 rigenga uburyo bwo kwishyurana, cyane cyane mu ngingo yaryo ya 8 ;	Law N° 061/2021 of 14/10/2021 governing the payment system, especially in its article 8;	Vu la Loi N° 061/2021 du 14/10/2021 régissant le système de paiement, spécialement en son article 8 ;
Ishingiye ku Itegeko Nº 73/2018 ryo ku wa 31/08/2018 rigena uburyo bw'ihererekanya makuru ku myenda cyane cyane mu ngingo iya 9, iya 13 n'iya 23;	Pursuant to Law Nº 73/2018 of 31/08/2018 governing credit reporting system, especially in its articles 9, 13 and 23;	Vu la Loi Nº 73/2018 du 31/08/2018 régissant le système d'information sur les crédits, , spécialement en ses articles 9,13 et 23 ;
Ishingiye ku Itegeko N° 05/2015 ryo ku wa 30/03/2015 rigenga imitunganyirize y'ubwiteganyirize bwa pansiyo cyane cyane mu ngingo yaryo ya 3;	Pursuant to Law N° 05/2015 of 30/03/2015 governing the Organization of Pension Schemes, especially in its article 3;	Vu la Loi N° 05/2015 du 30/03/2015 régissant l'organisation des régimes de pensions spécialement en son article 3 ;
Isubiye ku mabwiriza rusange Nº 02/2018 yo ku wa 24/01/2018 yerekeye umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ;	Having reviewed the regulation Nº 02/2018 of 24/01/2018 on cyber security;	Revu le règlement N ° 02/2018 du 24/01/2018 sur la cybersécurité;
Banki Nkuru y'u Rwanda, mu ngingo zikurikira yitwa «**Urwego rw'ubugenzuzi**» ishyizeho aya mabwiriza rusange akurikira :	The National Bank of Rwanda hereinafter referred to as the **«Supervisory Authority»,** issues the following regulation:	La Banque Nationale du Rwanda, ci-après dénommée « **Autorité de contrôle**;», édicte le présent règlement :

UMUTWE WA MBERE: INGINGO RUSANGE	**CHAPTER ONE: GENERAL PROVISIONS**	**CHAPITRE PREMIER: DISPOSITIONS GÉNÉRALES**
Ingingo ya mbere: Icyo aya mabwiriza rusange agamije Aya mabwiriza rusange agamije kugena uburyo ibigo bigenzurwa bigira sisitemu n'uburyo bw'ikoranabuhanga buhamye hakubiyemo umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bigamije kurinda, kugaragarza, gusubiza gahunda zo kuzahura zigeragezwa ku buryo buhoraho, gushyiraho uburyo bw'ubukangurambaga no gutanga amakuru ku gihe mu rwego rwo gucunga ingorane n'ifatwa ry'ibyemezo mu rwego rwo gufasha mu mirimo y'ingenzi y'ikigo kigenzurwa.	**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 premier: Objet** Le but de ce règlement est de veiller à ce que les institutions réglementées disposent de ICT résilientes, y compris la cybersécurité, soumises à des programmes de protection, de détection, de réponse et de récupération régulièrement testés, intègrent une connaissance appropriée de la situation et transmettent des informations pertinentes en temps opportun pour la gestion des risques et les processus de prise de décision afin de soutenir et de faciliter pleinement la livraison des opérations critiques de l'institution règlementée
Ingingo ya 2: Abarebwa n'aya mabwiriza rusange Aya Mabwiriza rusange akurikizwa mu bigo bigenzurwa byose keretse aho biteganyijwe ukundi mu mabwiriza rusange cyangwa mu mabwiriza yihariye.	**Article 2: Scope** This Regulation shall apply to all regulated institutions unless provided otherwise by specific regulations or directives.	**Article 2: Champ application** Le présent règlement s'applique à tous les institutions réglementées, sauf disposition contraire des règlements ou des directives spécifiques.

Ingingo ya 3: Ibisobanuro by'amagambo	**Article 3: Definition of terms**	**Article 3: Définition des termes**
Muri aya mabwiriza rusange, amagambo akurikira asobanura:	In this regulation, the following words and expressions shall mean:	Dans ce règlement, les mots et expressions suivants signifient:
1° **Ikigo kigenzurwa:** ikigo cyemerewe gukora kandi kigenzurwa kigenzurwa n' Urwego rw'Ubugenzuzi;	1° **a regulated institution**: any financial institution licensed and supervised by the Supervisory Authority;	1° **Une institution réglementée :** toute institution agrée et supervisée par l'Autorité de contrôle ;
2° **ukoresha uburyo bukoresha ikoranabuhanga ubyemerewe:** umukozi uwo ari we wese, ufitanye amasezerano n'ikigo kigenzurwa, ugihagarariye cyangwa undi muntu uwo ari we wese ugira uruhare mu bikorwa by'ubucuruzi by'ikigo kigenzurwa kandi akaba yemerewe kugera ku buryo bukoresha ikoranabuhanga no ku makuruatagenewe rubanda yacyo kimwe no kubikoresha;	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;	2° **Utilisateur autorisé:** tout employé, entrepreneur, agent ou autre personne qui participe aux opérations commerciales d'une institution réglementé et est autorisé à accéder et à utiliser les Systèmes d'Information et les données non publique de l'institution réglementée;
3° **ikibazo cy'umutekano w'ibijyanye n'ikoranabuhanga:** Ni igikorwa iyo kibaye	3° **Cyber incident:** A cyber event that:	3° **Cyber incident:** Un cyber-événement qui :

a. Gishyira mu ngorane umutekano w'ikoranabuhanga mu itangazabumenyi n'itumanaho bya sisitemu y'amakuru cyangwa amakuru sistemu itunganya, ibitse cyangwa yohereza, cyangwa	a. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or	a. met en danger la cybersécurité d'un système d'information ou des informations que le système traite, stocke ou transmet ; ou
b. Byica politiki 'umutekano w'amakuru, uburyo bwo gucunga umutekano w'amakuru cyangwa politiki yemewe yo gukoresha amakuru ;	b. violates the security policies, security procedures or acceptable use policies,	b. viole les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptables,
Bishobora kuvamo cyangwa kutavamo igikorwa kibi.	Whether resulting from malicious activity or not.	Qui résultent ou non d'une activité malveillante.
4° **uburyo bukoresha ikoranabuhanga:** porogaramu zose za mudasobwa n'ibikoresho byo gutunganya amakuru, kuyabika cyangwa kuyacukumbura cyangwa byo kuyacunga;	4° **information system**: software, tools and equipments for the production, storage or processing of data or information or management of data or information;	4° **Système d'information:** tous les logiciels, outils et équipements pour la production, le stockage or le traitement de données ou d'informations ou la gestion des données ou d'information ;
5° **gusuzuma umwirondoro hagendewe ku bintu byinshi:** gusuzuma umwirondoro w'umuntu ugendeye nibura ku bwoko bubiri bw'ibintu byifashishwa mu kumenya uwo ari we:	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:	5° **authentification multifactorielle:** authentification de l'identité d'un utilisateur par l'utilisation et la vérification d'au moins deux des types de facteurs d'identité suivants:

a. ibyo agomba kuba azi nk'ijambobanga; Umubare w'ibanga;	a. knowledge factors, such as password, PIN;	a. facteurs de connaissance, tels que mot de passe, code PIN;
b. ibyo agomba kuba afite nk'ikirango cyangwa ubutumwa kuri telefoni igendanwa;	b. possession factors, such as a card, token, text message on a mobile phone;	b. les facteurs de possession, tels qu'une carte, un jeton, un message texte sur un téléphone mobile;
c. ibyerekeranye n'imiterere y'ibiranga umuntu nk'ibiranga imiterere y'umubiri.	c. inherence factors, such as a user's biometrics.	c. facteurs d'héritage, tels que la biométrie d'un utilisateur.
6° **Amakuru atagenewe rubandawese:** amakuru yose ataboneka k'umugaragaro ariyo:	6° **Nonpublic data:** all data that is not publicly available that is:	6° **Données non publiques:** toutes les données non accessibles au public qui sont:
a. yerekeranye n'ibicuruzwa na serivisi byikigo kigenzurwa cyangwa imibare;	a. related to product and services of regulated institution or related statistics;	a. liés aux produits et services d'une institution réglementé ou aux statistiques connexes;
b. amakuru yihariye ya buri muntu nkuko abasonurwa n'amategeko yihariye;	b. personal data as defined by specific laws	b. données personnelles telles que définies par des lois spécifiques.

7° **kugerageza kwinjira:** uburyo bw'isizuma aho abasuzuma bakoresha inyandiko zose zihari bakora ku mpungenge bakagerageza kwinjira mu birango bya sistemu y'amakuru acungiwe umutekano **;**	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	7° **test de pénétration:** une méthodologie de test dans laquelle les évaluateurs, utilisant tous les documentations et travaillant sous des contraintes spécifiques, tenter de contourner les éléments de sécurité d'un système d'information
8° **amakuru rusange:** amakuru yose ikigo kigenzurwa gishobora kwizera ko ashobora gushyirwa aho buri wese yayabona	8° **publicly available information:** any information that a regulated institution has a reasonable basis to believe is lawfully made available to the general public;	8° **Informations accessibles au public:** toute information qu'une institution réglementée a des motifs raisonnables de croire qu'elle est légalement rendue accessible au grand public;
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.	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.	9° **authentification basée sur les risques:** tout système d'authentification basé sur les risques qui détecte des anomalies ou des changements dans les schémas d'utilisation normaux d'une personne et nécessite une vérification supplémentaire de l'identité de la personne lorsque de tels écarts ou changements sont détectés, par exemple par l'utilisation d'un défi des questions;

10° **Utanga serivisi:** umuntu wo hanze ukora ibikorwa mu izina ry'ikigo kigenzurwa kandi harimo umunyamuryango witsinda ikigo kigenzurwa kibarizwamo, isosiyete ifitanye isano yaba iyo mu Rwanda cyangwa hanze;	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;	10° **prestataire de services:** une personne qui entreprend l'activité externalisée pour le compte de l'institution réglementé et comprend un membre du groupe auquel appartient l'institution réglementé, société liée qu'elle soit située au Rwanda ou à l'extérieur;
11° **umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho:**kubika, kugira ibanga , ubunyangamugayo, no kugaragaza amakuru na/cyangwa sisitemu y'amakuru binyuze mu muyoboro w'ikoranabuhanga mu itangazabumenyi;	11° **Cyber security**: preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium;	11° **Cybersécurité:** préservation de la confidentialité, de l'intégrité et de la disponibilité des informations et/ou des systèmes d'information par le biais du cybermédia ;
12° **Ibyateza ingorane biturutse ku ikoranabuhanga mu itangazabumenyi n'itumanaho:** Uruhurirane rw'ibishobora kuba biturutse ku bibazo byaterwa n''ikoranabuhanga mu itangazabumenyi n'itumanaho n'ingaruka zabyo;	12° **Cyber risk**: The combination of the probability of cyber incidents occurring and their impact;	12° **Cyber-risque:** La combinaison de la probabilité que des cybers incidents se produisent et de leur impact;

13° **Ibikorwa remezo by'ikoranabuhanga:** ibyuma, software, ibikoresho by'urusobe na serivisi bisabwa kugirango habeho, imikorere no gucunga imishinga y'ikoranabuhanga ibikikije. Iyemerera ishyirahamwe gutanga ibisubizo bya serivisi na serivisi ku bakozi bayo, abafatanyabikorwa ndetse nabakiriya kandi mubisanzwe imbere mumuryango kandi byoherejwe mubikoresho bifite;	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;	13° **Infrastructure informatique:** désigne le matériel, les logiciels, les ressources réseau et les services nécessaires à l'existence, au fonctionnement et à la gestion d'un environnement informatique d'entreprise. Il permet à une organisation de fournir des solutions et des services informatiques à ses employés, partenaires et / ou clients et est généralement interne à une organisation et déployé dans des installations détenues;
14° **Ingano y'ibiteye ibyago:** Amakuru ku mitungo y'ingenzi, abateza ibyago, n'amakuru y'uburyo abateza ibyago bashobora guhungabanya iyo mitungo y'ingenzi;	14° **Threat profiles:** information about critical assets, threat actors, and details about how threat actors might attempt to compromise those critical assets;	14° **Profils de menaces:** informations sur les actifs critiques, les acteurs de la menace et détails sur la manière dont les acteurs de la menace pourraient tenter de compromettre ces actifs critiques;
15° **Gupima ibiteye ubwoba:** ukoresheje inzira itunganijwe kugirango umenye uburyo umutungo w'ingenzi ushobora guhungabanywa n'umuntu, impamvu, n'uburyo bwo kurinda bukenewe kuri iyo mitungo ikomeye, n'ingaruka byagira mu gihe ubwo burinzi bunaniranye.	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.	15° **Modélisation des menaces:** utiliser un processus structuré pour identifier comment les actifs critiques pourraient être compromis par un acteur de la menace et pourquoi, quel niveau de protection est nécessaire pour ces actifs critiques et quel serait l'impact si cette protection échouait.

UMUTWE WA II: IBISABWA BIGOMBA KUBAHIRIZWA	**CHAPTER II: REGULATORY REQUIREMENTS**	**CHAPITRE II: EXIGENCES RÉGLEMENTAIRES**
Ingingo ya 4: Imiyoborere mu by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	**Article 4: Cyber security governance**	**Article 4: Gouvernance de la cybersécurité**
Umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ni inshingano z'abagize inama y'ubutegetsi n'ubuyobozi bukuru.	Cyber security governance must be the responsibility of the Board of Directors and Senior Management.	La gouvernance de la cybersécurité doit relever de la responsabilité du conseil d'administration et de la haute direction.
Ikigo kigenzurwa kigomba kugira uburyo bw'imiyoborere buhamye ku bijyanye n' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bukubiyemo nibura ibi bukurikira:	A regulated institution must have a comprehensive cyber security governance framework consisting of the following:	Une institution réglementée doit disposer d'un cadre de gouvernance de cybersécurité complet comprenant les éléments suivants:
1° Ingamba mu by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho zihuye n'intego z'ubucuruzi;	1° cyber security strategy linked with business objectives;	1° stratégie de cybersécurité liée aux objectifs commerciaux;
2° Gahunda y'imiyoborere mu by'umutekano wa interineti icyemura buri rwego rw'ingamba. ubugenzuzi n'amabwiriza;	2° governing security program that address each aspect of the strategy, controls and regulations;	2° régir le programme de sécurité qui aborde chaque aspect de la stratégie, des contrôles et des règlements;

3° urutonde rwuzuye rwibipimo kuri buri politiki kugirango harebwe inzira n'ibigenderwaho byubahiriza politiki;	3° a complete set of standards for each policy to ensure procedures and guidelines comply with the policy;	3° un ensemble complet de normes pour chaque politique afin de s'assurer que les procédures et les lignes directrices sont conformes à la politique;
4° imiterere y'ikigo ihamye kandi itarangwamo kugongana kw'inyungu z'abayobozi n'ububasha buhagije;	4° an effective organization structure void of conflict of interest with sufficient authority and adequate resources;	4° une structure organisationnelle efficace sans conflit d'intérêts avec une autorité et des ressources suffisantes;
5° ibipimo no gukurikirana inzira kugirango habeho iyubahirizwa, ibitekerezo ku mikorere no gutanga ishingiro ry'aho ubuyobozi buhera mu gufata ibyemezo;	5° metrics and monitoring processes to ensure compliance, feedback on effectiveness and provide the basis for appropriate management decisions;	5° des mesures et des processus de surveillance pour assurer la conformité, le retour d'information sur l'efficacité et fournir la base de décisions de gestion appropriées;
6° Gushyiraho imikorere myiza ikigo kigenzurwa kigomba kwihatira kugeraho yemewe ku rwego mpuzamahanga ku bijyanye no gucunga amakuru	6° Adopt best practices that regulated institution should strive to attain globally accepted practices on information security management;	6° Adopter les meilleures pratiques que l'institution réglementée devrait s'efforcer d'atteindre des pratiques mondialement acceptées en matière de gestion de la sécurité de l'information
7° Guteza imbere uburyo bwo gukemura ibibazo, bugaragaramo ubuyobozi bukuru n'inama y'ubutegetsi kuva ku mbibi zumvikanyweho mbere;	7° Develop crisis management practices, involving executive management and board of directors from pre-agreed thresholds onward;	7° Développer des pratiques de gestion de crise, impliquant la direction générale et le conseil d'administration à partir de seuils préalablement convenus;

8° Ibisabwa n'amategeko n’amabwiriza yerekeye umutekano w’ibijyanye n’ikoranabuhanga mu itangazabumenyi n’itumanaho, harimo n’ibanga n’inshingano k’uburenganzira bw’umuntu, birasobanuka kandi bigacungwa;	8° Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed;	8° Les exigences légales et réglementaires en matière de cybersécurité, y compris les obligations en matière de confidentialité et de libertés civiles, sont comprises et gérées ;
9° ingamba zo gucunga ibyateza ingorane z’ikoranabuhanga byinjijwe mu bikorwa rusange by’ubucuruzi no gucunga ibyateza ingorane ku kigo.	9° cyber risk management strategy that is incorporated into the overall business strategy and risk management of the institution.	9° stratégie de gestion des cyberrisques intégrée à la stratégie commerciale globale et à la gestion des risques de l'établissement.
<u>Ingingo ya 5:</u> Komite y'Inama y'Ubutegetsi ishinzwe ikoranabuhanga	**<u>Article 5:</u> IT Board Committee**	**<u>Article 5:</u> Comité du conseil d’administration des technologies de l'information**
Uretse aho byaba biteganyijwe ukundi mu mabwiriza rusange, Urwego rw’ubugenzuzi rushobora gusaba cyangwa gusonera ikigo kigenzurwa kugira komite ishinzwe ikoranabuhanga ku rwego rw’inama y’ubutegetsi bitewe n’ubwoko cyangwa urusobe rw’ibikorwa by’ikigo kigenzurwa.	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.	Sauf disposition contraire dans une réglementation spécifique, l'Autorité de contrôle peut exiger ou dispenser une institution réglementée d'avoir un Comité Informatique au niveau du Conseil en fonction de la nature de son activité et de sa complexité.
Komite ishinzwe ikoranabuhanga ifite ububasha n’inshingano bikurikira:	The IT Committee shall have the following powers and responsibilities:	Le comité informatique a les pouvoirs et responsabilités suivants:

1° gutanga inama ku cyerekezo cyerekeranye n'ikoranabuhanga n'umutekano wa interineti no gusuzuma ishoramari ry'ikoranabuhanga mu izina ry'Inama y'Ubutegetsi;	1° give advice on strategic direction on IT and cyber security and to review IT investments on Board's behalf;	1° donner des conseils sur l'orientation stratégique de l'informatique et de la cybersécurité et examiner les investissements informatiques au nom du conseil d'administration;
2° kugenzura komite nyobozi ishinzwe Ikoranabuhanga n'itumanaho (Ku rwego rw'ubuyobozi bukuru);	2° perform oversight functions over the IT steering committee (at a senior management level);	2° exercer des fonctions de supervision du comité de pilotage informatique (au niveau de la direction générale);
3° gushakisha amakuru ku mukozi uwo ari we wese;	3° seek information from any employee;	3° rechercher des informations auprès de tout salarié;
4° gushaka ubufasha bwo mu rwego rw'amategeko n'urw'umwuga hanze y'ikigo;	4° obtain outside legal or professional advice;	4° obtenir des conseils juridiques ou professionnels externes;
5° kunoza uruhare rw'abo hanze bafite ubuzobere bukwiye mu gihe ari ngombwa;	5° secure attendance of outsiders with relevant expertise, if it considers necessary;	5° assurer la présence d'étrangers ayant une expertise pertinente, s'il le juge nécessaire;
6° 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;	6° work in partnership with other board committees and senior management to provide input, review and amend the aligned corporate and IT strategies;	6° travailler en partenariat avec d'autres comités du conseil et la haute direction pour fournir des commentaires, examiner et modifier les stratégies corporatives et informatiques harmonisées;

7° Kumenya neza ko abagenzuzi b'imbere n'abaturutse hanze bemeranya na komite y'ubugenzuzi n'ubuyobozi k'uburyo umutekano w'amakuru ugomba kwitabwaho mu igenzura;	7° Ensure that internal and external auditors agree with the audit committee and management how information security should be covered in the audit;	7° S'assurer que les auditeurs internes et externes conviennent avec le comité d'audit et la direction de la manière dont la sécurité de l'information doit être couverte dans l'audit ;
8° Kumenyesha inama y'ubutegetsi k'uburyo burambye ibyateza ikigo ingorane biturutse ku ikoranabuhanga gishobora guhura nabyo n'uburyo bwo kubibungabunga hakubiyemo ibiteye ubwoba bizwi n'ibiteganywa n'aho ibintu byerekera;	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;	8° informer le conseil en permanence de l'exposition aux cyberrisques et des pratiques de gestion des risques de l'établissement, y compris les menaces et tendances connues et émergentes;
9° gusubiramo uburyo bwo gusuzuma imikorere ya gahunda y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho w'ikigo no kuyivugurura hakurikije uko imiterere y'iterabwoba igenda ihinduka;	9° review the procedures for testing the effectiveness of the institution's cyber security protocols and updating them as the threat landscape evolves;	9° revoir les procédures de test de l'efficacité des protocoles de cybersécurité de l'institution et les mettre à jour au fur et à mesure de l'évolution du paysage des menaces;
Abagize Komite y'ikoranabuhanga bagomba kuba bafite ubuhanga. Nibura umwe muri bo agomba kuba afite ubumenyi buhagije mu by'ikoranabuhanga cyangwa mu by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho.	The IT Committee members must be technically competent. At least one member must have substantial IT or cyber security expertise.	Les membres du comité informatique doivent être techniquement compétents. Au moins un membre doit avoir une solide expertise en informatique ou en cybersécurité.

Ingingo ya 6: Komite nyobozi ishinzwe ikoranabuhanga:	**Article 6: IT Steering Committee**	**Article 6: Comité de pilotage informatique**
Ikigo kigenzurwa kigomba kugira komite nyobozi ishinzwe ikoranabuhanga igizwe n'abahagarariye serivisi y'ikoranabuhanga, serivisi ishinzwe abakozi, n'inzego zishinzwe amategeko keretse bigenwe ukundi n'urwego rw'ubugenzuzi.	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.	Une institution réglementée doit disposer d'un comité de pilotage informatique composé de représentants des secteurs informatique, RH, juridique et métier sauf disposition contraire l'autorité de contrôle.
Komite nyobozi ishinzwe ikoranabuhanga igomba kugira nibura inshingano zikurikira:	The IT Committee shall at least have the following responsibilities:	Le comité informatique aura au moins les responsabilités suivantes:
1° gufasha ubuyobozi bukuru gushyira mu bikorwa ingamba z'umutekano mu by'ikoranabuhanga zemejwe n'inama y'ubutegetsi;	1° assist the Executive Management in implementing IT Security Strategy that has been approved by the Board;	1° assister la direction générale dans la mise en œuvre de la stratégie de sécurité informatique approuvée par le conseil d'administration;
2° gukurikirana urwego rwa serivisi no kunoza, gutanga serivisi z'ikoranabuhanga n'imishinga;	2° monitoring service levels and improvements, IT service delivery and projects;	2° surveiller les niveaux de service et les améliorations, la prestation des services informatiques et les projets;
3° Kuganira ku ishyirwa mu bikorwa rya gahunda n'ibikorwa byo kugabanya ingorane zaturuka ku ikoranabuhanga, harimo n'ibikorwa byo gukomeza ubucuruzi;	3° Discuss on the implementation of plans and activities to reduce cyber risks, including business continuity planning matters;	3° Discuter de la mise en œuvre de plans et d'activités visant à réduire les cyberrisques, y compris les questions de planification de la continuité des activités;

4° Kujya inama ku masomo akurikira ikibazo cyabaye mu rwego rw'ikoranabuhanga n'umutekano w'amakuru no gushyira mu bikorwa ingamba zifatika. Gutanga ibitekerezo bikorwa ako kanya nyuma yo kubona ikibazo kibaye;	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.	4° Délibérer sur l'apprentissage des leçons suite à des incidents de cybersécurité et de sécurité de l'information et mise en œuvre des recommandations pertinentes. Le compte rendu doit commencer immédiatement après la fin des incidents.
5° gusuzuma ingaruka zishobora kubaho mu gusubiza ku murongo gahunda y'ikigo kigenzurwa yo gukorera ahantu hatagaragara;	5° Assess potential risks involved in activating the regulated institution's systems in a cloud environment;	5° Évaluer les risques potentiels liés à l'activation des systèmes de l'institution réglementé dans un environnement cloud;
6° gushyiraho ingamba zapimwe kandi zicungirwa ahagaragara muri gahunda y'umutekano zishingiye ku bipimo ngenderwaho, imiterere yo gukura, gusesengura icyuho no gutanga raporo ihoraho yerekana ibikorwa;	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;	6° Créer une stratégie de sécurité mesurable et transparente de gestion basée sur des analyses comparatives, des modèles de maturité, une analyse des écarts et des rapports de performance continus qui reflètent les processus opérationnels;
7° gushyiraho gahunda y'umutekano mu gusuzuma imikorere kandi hagashyirwaho ibihembo bikwiye hamwe n'ibihano;	7° Include security in job performance appraisals and apply appropriate rewards and disciplinary measures;	7° Inclure la sécurité dans les évaluations du rendement au travail et appliquer des récompenses et des mesures disciplinaires appropriées;

8° kumenya neza ko ingamba zemewe zo gucunga ibyago bituruka ku ikoranabuhanga byerekana uburyo ikigo giteganya gukemura ibibazo byacyo by'ikoranabuhanga ndetse n'uburyo bizakomeza urwego rwemewe rw'ibisigisigi by'ibisigisigi kandi bigakomeza guhangana k'uburyo buhoraho; Komite Nyobozi iterana byibura buri gihembwe ndetse n'ikindi gihe bibaye ngombwa.	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.	8° veiller à ce que la stratégie approuvée de gestion des cyberrisques indique comment l'établissement entend faire face à son cyber-risque inhérent et comment il maintiendra un niveau acceptable de cyberrisque résiduel et maintiendra sa résilience de façon continue; Le comité directeur se réunit au moins une fois par trimestre et lorsque cela est jugé nécessaire.
<u>Ingingo ya 7</u>: Urwego rushyinzwe umutekano w'ikoranabuhanga Uretse iyo biteganijwe ukundi mu mabwiriza rusange cyangwa mu mabwiriza yihariye, buri kigo kigenzurwa kigomba kugira urwego rushinzwe umutekano w'ikoranabuhanga n'abakozi babishoboye bafite ubumenyi mu ikoranabuhanga cyangwa mu by'umutekano wa interineti. Inshingano z'umutekano w'ikoranabuhanga zirimo, ariko ntabwo zigarukira kuri:	**<u>Article 7:</u> 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:	**<u>Article 7:</u> Fonction de sécurité informatique** Sauf disposition contraire dans un règlement ou une directive spécifique, chaque institution réglementée dispose d'une fonction de sécurité informatique dotée d'un personnel qualifié dans le domaine de l'informatique ou de la cybersécurité. Les responsabilités de la fonction de sécurité informatique comprennent, sans s'y limiter:

1° gutegura ingamba z'umutekano w'ikoranabuhangana gahunda y'ikoranabuhanga;	1° designing cyber security strategy and IT program,	1° conception de la stratégie de cybersécurité et du programme informatique;
2° Gushyira mu bikorwa no kugenzura ishyirwa mu bikorwa rya gahunda y'umutekano w'ikigo kigenzurwa;	2° Implement and overseeing the regulated Institution's cyber security program execution;	2° Mettre en œuvre et superviser l'exécution du programme de cybersécurité de l'Institution réglementé;
3° Gushyiraho gahunda zo gukemura ibitaragenze neza mu ngamba zari muri gahunda no gushyira mu bikorwa politiki y'umutekano wa interineti;	3° recommending actions for addressing any noted program shortfalls and enforcing its cyber security policy;	3° recommander des actions pour remédier à toute insuffisance constatée du programme et faire appliquer sa politique de cybersécurité;
4° Gusuzuma ku buryo buhoraho iby'umutekano n'igenzura;	4° perform regular information security internal assessments and audit;	4° effectuer régulièrement des évaluations et audits internes de la sécurité de l'information;
5° gutahura ibibazo by'umutekano wa interineti no gukurikirana buri gihe uburyo budasanzwe kandi butemewe bwo kugera kuri interineti cyangwa kuyikoresha;	5° detect cyber security incidents and regularly monitoring of abnormal and unauthorized access or use;	5° détecter les incidents de cybersécurité et surveiller régulièrement les accès ou utilisations anormaux et non autorisés;
6° gusubiza ibibazo byagaragaye cyangwa byagaragaye ko umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	6° respond to identified or detected cyber security incidents to mitigate any negative effects;	6° répondre aux incidents de cybersécurité identifiés ou détectés pour en atténuer les effets négatifs;

wagabanijwe kugirango ugabanye ingaruka mbi zose;		
7° gukira ibitero byifashisha ikoranabuhanga no kugarura ibikorwa na serivisi bisanzwe mu buryo busanzwe;	7° recover from cyber-attacks and restore normal operations and services;	7° se remettre des cyberattaques et rétablir les opérations et services normaux;
8° kumenya no gusuzuma ibyateza ingorane biturutse ku mutekano wa interineti imbere cyangwa hanze zishobora guhungabanya umutekano cyangwa ubusugire bw'amakuru atagenewe rubanda abitswe kuri sisitemu y'amakuru y'ikigo kigenzurwa;	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;	8° identifier et évaluer les risques de cybersécurité internes et externes susceptibles de menacer la sécurité ou l'intégrité des données financières stockées dans les systèmes d'information no-publiques de l'établissement réglementé;
9° gukoresha ibikorwa remezo byo gukumira no gutahura no gushyira mu bikorwa politiki n'uburyo bwo kurinda sisitemu y'amakuru y'ikigo kigenzurwa, hamwe n'amakuru y'imari yabitswe cyangwa muri ategerejwe kuri sisitemu y'amakuru, kutinjira, gukoresha cyangwa ibindi bikorwa bibi;	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;	9° utiliser une infrastructure de prévention et de détection et mettre en œuvre des politiques et des procédures pour protéger les systèmes d'information de l'institution réglementé, ainsi que les données financières stockées ou en transit sur ces systèmes d'information, contre tout accès, utilisation ou autres actes de malveillance non autorisés;

10° Gushyiraho no kubungabunga uburyo bwo guhangana n'ibiteye ubwoba ikigo;	10° Establish and maintain threat profiles for identified threats to the institution;	10° Établir et maintenir des profils de menaces pour les menaces identifiées à l'institution;
11° gushyiraho no gukomeza ubushobozi bwo kwerekana ibiteye ubwoba;	11° establish and maintain threat modelling capabilities**;**	11° établir et maintenir des capacités de modélisation des menaces;
12° gukora isuzuma ryimbitse.	12° Conduct comprehensive penetration tests.	12° Effectuer des tests de pénétration complets.
Umuyobozi w'urwego rw'umutekano w'ikoranabuhanga cyangwa abakozi bashinzwe umutekano w'ikoranabuhanga bagomba gutanga raporo k'ubuyobozi bukuru ndetse no kuri komite y'inama y'ubutegetsi ishinzwe ikoranabuhanga.	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.	Le responsable de la fonction Sécurité informatique ou le personnel en charge de la sécurité informatique rend compte administrativement au directeur général et fonctionnellement au comité du conseil informatique.
<u>Ingingo ya 8</u>: Ingamba zo gucunga umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho	**<u>Article 8:</u> Cyber security strategy**	**<u>Article 8:</u> Stratégie de cybersécurité**
Ikigo kigenzurwa kigomba gukomeza ingamba z'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho cyashyizeho mu kurinda ibanga, ubunyangamugayo no kuboneka kw'amakuru atagenwe rubanda y'ikigo	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.	L'institution réglementée doit maintenir une stratégie de cybersécurité conçue pour protéger la confidentialité, l'intégrité et la disponibilité des données non publiques, des systèmes et de l'infrastructure informatique sous-jacente de l'institution réglementé.

kigenzurwa, sisitemu n'ibikorwa remezo by'ikoranabuhanga. Ingamba z'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho zigomba gutanga ishingiro rya gahunda y'ibikorwa igizwe na gahunda y' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, nk'uko yashyizwe mu bikorwa, igera ku ntego z'umutekano ziteganijwe. Inyandiko zose n'amakuru ajyanye n'ingamba na gahunda y'ikigo kigenzurwa ku mutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bigomba gushyikirizwa Urwego rw'ubugenzuzi igihe bisabwe.	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.	La stratégie de cybersécurité doit fournir la base d'un plan d'action comprenant un programme de cybersécurité qui, tel qu'il est mis en œuvre, permet d'atteindre les objectifs de sécurité prévus. Tous les documents et informations concernant la stratégie et le programme de cybersécurité de l'institution réglementé doivent être mis à la disposition de l'Autorité de contrôle sur demande.
<u>Ingingo ya 9</u>: Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho Ikigo kigenzurwa kigomba gushyira mu bikorwa no kubika politiki yanditse yemewe n'inama y'ubutegetsi.	**<u>Article 9:</u> Cyber security Policy** A regulated institution must implement and maintain a written policy approved by the board.	**<u>Article 9</u>: Politique de cybersécurité** Une institution réglementée doit mettre en œuvre et maintenir une politique écrite approuvée par le conseil.

Politiki y'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho igomba kuba ishingiye ku gusuzuma ibyateza ingorane ku kigo kigenzurwa no gukemura byibuze ibice bikurikira by'ibikorwa by'ikigo:	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:	La politique de cybersécurité doit être fondée sur l'évaluation des risques de l'institution réglementé et aborder au moins les domaines suivants des opérations de l'institution:
1° Umutekano w'amakuru;	1° Information security;	1° Sécurité de l'information;
2° Imiyoborere no gushyira mu byiciro amakuru;	2° Data governance and classification;	2° Gouvernance et classification des données;
3° Ibarura ry'umutungo no gucunga ibikoresho;	3° Asset inventory and device management;	3° Inventaire des actifs et gestion des appareils;
4° Kugenzura uburyo bwo kugera ku makuru no gucunga imyirondoro y'abantu;	4° Access controls and identity management;	4° Contrôle d'accès et gestion des identités;
5° Imikorere y'uburyo bukoresha ikoranabuhanga n'ibibazo bijyanye n'uko ubwo buryo buboneka;	5° Systems operations and availability concerns;	5° Problèmes d'exploitation et de disponibilité des systèmes;
6° Kugenzura uburyo bukoresha ikoranabuhanga n'muyoboro;	6° Systems, applications and network security;	6° Sécurité des systèmes, des applications et des réseaux;

7° Gutunganya uburyo bukoresha ikoranabuhanga, kubugura no kunoza imikorere yabwo;	7° Application development, acquisition and quality assurance;	7° Développement d'applications, acquisition et assurance qualité;
8° Umutekano w'ahantu hakorerwa no gukora amagenzura mu rwego rw'ibidukikije;	8° Physical security and environmental controls;	8° Sécurité physique et contrôles environnementaux;
9° Kurinda amakuru y'abakiriya no kubagirira ibanga;	9° Customer data protection and privacy;	9° Protection des données et confidentialité des clients;
10° Imicungire y'ugurisha n'iy'utanga serivisi;	10° vendor and service provider management;	10° la gestion des vendeurs et des prestataires de services;
11° Isuzuma ry'ibyateza ingorane biturutse ku ikoranabuhanga;	11° Cyber risk management;	11° Gestion des cyberrisques;
12° Isuzuma ryimbitse no kugenzura ahari intege nkeya;	12° penetration testing and vulnerability assessments;	12° tests de pénétration et évaluations de vulnérabilité;
13° Gusuzuma neza ibyaterza ibibazo biturutse ku ikoranabuhanga;	13° Cyber incident management;	13° Gestion des cyberincidents;
14° kumenyesha abakozi, abakiriya n'abafatanyabikorwa ibijyanye n' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho;	14° awareness of staff, customers and stakeholders with regard to cyber security;	14° sensibilisation du personnel, des clients et des parties prenantes à la cybersécurité;

15° ibisabwa ubunyangamugayo bw'abakozi baba bagira ho bahurira n'amakuru, sisitemu n'umuyoboro harimo amasezerano yo kutamena ibanga;	15° integrity requirements of staff dealing with data, systems and networks including non-disclosure agreement;	15° Exigences en matière d'intégrité du personnel traitant des données, des systèmes et des réseaux, y compris l'accord de non-divulgation;
16° igenzura kuri sisitemu, ahantu hagaragara harimo amakuru y'abakiriya n'ibikoresho byo kugenzura bikorwa n'ababiherewe uburenganzira.	16° controls to systems, physical locations containing customer information and tools to monitor access by authorized persons.	16° des contrôles aux systèmes, aux emplacements physiques contenant des informations sur les clients et des outils pour surveiller l'accès des personnes autorisées.
Politiki igomba gusubirwamo mu gihe gikwiye.	The policy shall be reviewed within a reasonable period.	La politique doit être réexaminée dans un délai raisonnable.
<u>Ingingo ya 10:</u> Amasuzuma yo kugerageza kwinjira no kureba intege nke	**<u>Article 10:</u> Penetration Testing and Vulnerability Assessments**	**<u>Article 10:</u> Tests de pénétration et évaluations de la vulnérabilité**
Ikigo kigenzurwa kigomba gukora byibuze:	A regulated institution is required to conduct at least:	Une institution réglementée est tenue d'effectuer au moins:
1° **Isuzuma ryinjira buri mwaka:** isuzuma ryo kwinjira rigomba kwibanda ku gupima ubushobozi bwo gukumira no kubona ubudahangarwa mu by'ikoranabuhanga hamwe n'ubushobozi bwo gusubiza no gusubira	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	1° **Des tests de pénétration annuels:** Les tests de pénétration doivent se concentrer sur le test des capacités de cyber-résilience préventive et de détection ainsi que sur les capacités de réponse aux tests et de récupération. Les tests ne doivent pas

ku murongo. Isuzuma ntirigomba kuvamo gutsinda cyangwa gutsindwa, ahubwo rigomba guha urwego rwageragejwe gushishoza ku mbaraga n'intege nke zarwo, kandi bikabasha kwiga no gutera imbere kugirango hatezwe imbere umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho;	tested entity with insight into its strengths and weaknesses, and enable it to learn and evolve to improve their cyber security maturity;	aboutir à une réussite ou à un échec, ils doivent plutôt fournir à l'entité testée un aperçu de ses forces et faiblesses, et lui permettre d'apprendre et d'évoluer pour améliorer sa maturité en matière de cybersécurité;
2° **Amasuzuma y'ahari intege nke akorwa kabiri mu mwaka:** gukora isuzuma ry'intege nke zisikana sisitemu y'imbere ku mbogamizi zizwi, no gusuzuma urwego rw'ishyirwa mu bikorwa rya politiki y' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho n'uburyo bushingiye ku gusuzuma ingaruka;	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;	2° **Évaluations bi-annuelles de la vulnérabilité:** effectué des évaluations de vulnérabilité qui analysent les systèmes internes pour détecter les vulnérabilités connues et examiner le niveau de mise en œuvre des politiques et procédures de cybersécurité en fonction de l'évaluation des risques;
Umuntu wese wemerewe gukora isuzuma ryo kwinjira cyangwa gusuzuma ahari intege nke agomba kuba afite nibura bumwe mu bumenyi bukurikira:	Any person entrusted to conduct penetration test or vulnerability assessment shall have at least one or some of the following qualification:	Toute personne chargée d'effectuer un test de pénétration ou une évaluation de la vulnérabilité doit posséder au moins une ou certaines des qualifications suivantes:
1° impamyabumenyi yizewe y'umutekano y'umwuga (CISSP);	1° Certified Information Systems Security Professional (CISSP);	1° Professionnel certifié de la sécurité des systèmes d'information (CISSP);

2° impamyabumenyi mu gucunga umutekano w'amakuru (CISM);	2° Certified Information Security Manager (CISM);	2° Professionnel certifié de la sécurité de l'information (CISM);
3° Ufite imyamyabumenyi mu kugenzura sisitimu z'amakuru (CISA)	3° Certified Information Systems Auditor (CISA);	3° Auditeur Certifié des Systèmes d'Information (CISA);
4° Imyamyabumenyi m'ubwirinzi no kugenzura ibikoresho n'imiyoboro y'ikoranabuhanga(CEH);	4° Certified Ethical Hacker (CEH);	4° Hacker éthique certifié (CEH);
5° Ushinzwe gucunga ibyateza umutekano mucye wizewe wabigize umwuga (OSCP);	5° Offensive Security Certified Professional (OSCP);	5° Professionnel certifié en sécurité offensive (OSCP);
6° Uwemererwe gukora isuzuma ryimbitse (LPT);	6° Licensed Penetration Tester (LPT);	6° Testeur de pénétration agréé (LPT);
7° Indi mpamyabumenyi yo mu rwego rumwe nazo.	7° Any other similar certification.	7° Toute autre certification similaire.
Ikigo kigenzurwa kigomba ishyikiriza Urwego rw'ubugenzuzi incamake y'ibyavuye mu igenzura mu gihe cy'iminsi icumi n'itanu (15) igenzura rimaze gukorwa.	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.	L'institution réglementé partage avec l'autorité de contrôle un résumé des conclusions du test dans un délai de quinze jours(15) après le test.

Ingingo ya 11: Inzira y'ubugenzuzi Ikigo cyigenzurwa kigomba kubungabunga neza sisitemu zirimo inzira z'ubugenzuzi zagenewe gutahura no gukemura ibibazo umutekano mucye w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bifite amahirwe menshi yo kwangiza ibintu byose bigize ibikorwa bisanzwe by'ikigo kigenzurwa.	**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 11: Piste d'audit** Une institution réglementée doit maintenir en toute sécurité des systèmes comprenant des pistes d'audit conçues pour détecter et répondre aux incidents de cybersécurité qui ont une probabilité raisonnable de nuire sensiblement à tout élément important des opérations normales de l'institution réglementée.
Ingingo ya 12: Gucunga umutekano w'imirongo itwara amakuru isimbura iyindi Ibigo bigenzurwa bigomba guha abakiriya amakuru yerekeye ingamba zisabwa mu gihe ukoresha imirongo itwara amakuru isimbura iyindi buri gihe, kumenyesha abakiriya ingaruka zishobora guterwa n'imirongo itwara amakuru isimbura iyindi kandi bigasaba gukingira no gukurikiza amahame y'ibanga yo kugabanya izo ngaruka ku bakiriya. Aya makuru agomba kuboneka ku mugaragaro. Ibigo bigenzurwa bigomba kugena ibintu byerekana umuntu ku giti cye no kwemeza	**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	**Article 12: Gestion de la sécurité des canaux de distribution alternatifs (ADC)** Les institutions réglementées doivent fournir aux clients des informations sur les précautions requises lors de l'utilisation régulière de l'ADC, informer les clients des risques potentiels associés à l'ADC et des principes de protection et de confidentialité recommandés pour minimiser ces risques pour le client. Ces informations sont accessibles au public. Les institutions réglementées déterminent les facteurs d'identification et d'authentification

ibintu ku rubuga rwa interineti no mu bindi bikorwa bya kure hashingiwe kuri politiki yemejwe n'inama y'ubutegetsi, gusuzuma ingaruka, no kurinda amakuru ndetse n'amabwiriza yerekeye ubuzima bwite.	factors for online and other remote transactions based on Board-approved policies, risk assessments, and data protection and privacy guidelines.	individuels pour les transactions en ligne et autres transactions à distance sur la base des politiques approuvées par le Conseil, des évaluations des risques et des directives en matière de protection des données et de confidentialité.
Ingingo ya 13: Gucunga ibyateza ingorane biturutse ku ikoranabuhanga Ikigo kigenzurwa kigomba gusuzuma buri gihe ingaruka ziterwa na sisitemu y'amakuru y'ikigo cy bihagije kugirango hakorwe igenamigambi ry'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho nk'uko bisabwa n'aya mabwiriza. Isuzuma ry'ibyateza ingorane rigomba kuvugururwa igihe cyose bikenewe kugirango hakemurwe impinduka kuri sisitemu y'amakuru y'ikigo kigenzurwa, amakuru atagenewe rubanda cyangwa ibikorwa by'ubucuruzi. Isuzuma ry'ikigo kigenzurwa rigomba kwemerera gusubiramo ubugenzuzi kugira ngo hasubizwe ibijyanye n'iterambere ry'ikoranabuhanga n'iterabwoba rigenda	**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	**Article 13: Gestion des cyber risques** Une institution réglementée procède à une évaluation périodique des risques des systèmes d'information de l'institution réglementé, suffisante pour éclairer la conception de la stratégie et de la politique de cybersécurité, conformément au présent règlement. Cette évaluation des risques est mise à jour si cela est raisonnablement nécessaire pour tenir compte des modifications apportées aux systèmes d'information, aux données non-publiques ou aux opérations commerciales de l'institution réglementé. Une évaluation des risques des établissements réglementés doit permettre de réviser les contrôles pour répondre aux développements technologiques et aux menaces en évolution

ryiyongera kandi harebwa ibyateza ingorane zishobora guterwa n'ibikorwa by'ubucuruzi by'ikigo kigenzurwa bijyanye n'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho, amakuru atari rusange yakusanyijwe cyangwa abitswe, sisitemu y'amakuru yakoreshejwe; kuboneka no gukora neza kugenzura no kurinda amakuru atagenewe rubanda na sisitemu y'amakuru.	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.	et doit prendre en compte les risques particuliers des opérations commerciales de l'établissement financier liés à la cybersécurité, les informations non publiques collectées ou stockées, les systèmes d'information utilisés et les disponibilité et efficacité des contrôles pour protéger les données non-publiques et les systèmes d'information.
Isuzuma ry'ibyateza ingorane rigomba gukorwa hakurikijwe politiki n'uburyo byanditse kandi bigomba kwandikwa. Politiki n'inzira bigomba kuba bikubiyemo:	The risk assessment must be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:	L'évaluation des risques doit être effectuée conformément aux politiques et procédures écrites et doit être documentée. Ces politiques et procédures doivent inclure:
1° ibigenderwaho mu gusuzuma no gushyira mu byiciro ibyateza ingorane mu rwego rw'umutekano wa interineti naho byabonetse cyangwa ibibazo byugarije ikigo muri urwo rwego;	1° Criteria for the evaluation and categorization of identified cyber security risks or threats facing the institution;	1° Critères d'évaluation et de catégorisation des risques ou menaces de cybersécurité identifiée auxquels l'établissement est confronté;
2° ibigenderwaho mu gusuzuma ibanga, ubudakemwa, umutekano n'iboneka rya sisitimu y'amakuru atagenwe rubanda hakubiyemo n'ubugenzuzi bukwiye hakurikijwe ibyateza ingorane byagaragaye;	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;	2° Critères d'évaluation de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information financière et des données non -publiques, y compris l'adéquation des contrôles existants dans le contexte des risques identifiés;

3° ibisabwa bigaragaza uburyo ubukana bw' ibyateza ingorane byagaragaye bushobora kugabanywa cyangwa kwakirwa hashingiwe ku isuzuma ry' ibyateza ingorane ryakozwe n'uburyo gahunda y'umutekano wa interineti izabasha gukemura izo ngorane.	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.	3° Critères d'acceptation décrivant comment les risques identifiés seront traités ou acceptés en fonction de l'appétit pour le risque de l'établissement et comment la stratégie et la politique de cybersécurité aborderont les risques.
Urwego rw'ikigo kigenzurwa rushinzwe gucunga ibyateza ingorane rugomba kubamo kandi ntibirangirire k mirimo ikurikira:	The regulated institution risk management function should include and not limited to the tasks below:	La fonction de gestion des risques des institutions réglementé devrait inclure, sans s'y limiter, les tâches ci-dessous:
1° Gusuzuma ibyateza ingorane n'imikoreshereze ijyanye n'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanahono kumenya niba bihuje n'ibyifuzo by'ikigo kigenzurwa;	1° Assessing the risks and exposures related to cyber security and determining whether they are aligned to the regulated institution's risk appetite;	1° évaluer les risques et expositions liés à la cybersécurité et déterminer s'ils sont alignés sur l'appétit pour le risque de l'institution réglementé;
2° Gukurikirana ibyateza ingorane biriho kandi bigaragara n'impinduka ku mategeko n'amabwiriza.	2° Monitoring current and emerging risks and changes to laws and regulations.;	2° Surveiller les risques actuels et émergents et l'évolution des lois et règlements;
3° Gufatanya n'abayobozi ba sisitemu n'abandi bashinzwe kurinda umutungo w'amakuru w'ikigo kigenzurwa	3° Collaborating with system administrators and others charged with safeguarding the information assets of the regulated	3° Collaborer avec les administrateurs de système et autres personnes chargées de protéger les actifs informationnels de

kugirango habeho igishushanyo mbonera gikwiye;	institution to ensure appropriate control design;	l'institution réglementé pour assurer une conception de contrôle appropriée;
4° kubika ibitabo bihamye byerekeranye na interineti: Ibipimo byingenzi byerekana ibyateza ingorane (KRI) bigomba kumenyekana buri gihe kandi bigasuzumwa. Kumenya ibyateza ingorane bigomba kurebwa mbere kandi bikubiyemo gukemura ibibazo by'umutekano;	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;	4° Tenir à jour des registres complets des cyber risques: les indicateurs clés de risque (KRI) doivent être régulièrement identifiés et évalués. L'identification des risques doit être prospective et inclure la gestion des incidents de sécurité;
5° Kugenzura ishyirwa mu bikorwa ry'ingamba na gahunda by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho;	5° Ensure implementation of the cyber security strategy and program;	5° Assurer la mise en œuvre de la stratégie et du programme de cybersécurité;
6° Kurinda ibanga, ubunyangamugayo no kuboneka kw'amakuru n'ibikorwa remezo by' ikoranabuhanga;	6° Safeguarding the confidentiality, integrity and availability of information and the underlying IT infrastructure;	6° Préserver la confidentialité, l'intégrité et la disponibilité des informations et de l'infrastructure informatique sous-jacente;
7° kumenya neza ko ibarura ry'umutungo w'ikoranabuhanga ryuzuye, ryashyizwe mu rwego rwaryo no kunenga ubucuruzi, ryashyizweho kandi rikabungabungwa;	7° Ensure that a comprehensive inventory of IT assets, classified by business criticality, is established and maintained;	7° S'assurer qu'un inventaire complet des actifs informatiques, classés par criticité métier, est établi et maintenu;

8° Isesengura ry'ingaruka zihari k' ubucuruzi kugira ngo hasuzumwe buri gihe akamaro k'ubucuruzi ku mutungo w'ikoranabuhanga;	8° A Business Impact Analysis process is in place to regularly assess the business criticality of IT assets;	8° Un processus d'analyse d'impact sur l'activité est en place pour évaluer régulièrement la criticité métier des actifs informatiques;
9° Gutegura no gushyira mu bikorwa uburyo bwo gupima ibyateza ingorane kugira ngo harebwe neza uburyo ikigo gicunga neza ingorane rusange z'ikoranabuhanga no kugabanya ingorane zikomoka ku ikoranabuhanga zisigaye za sisitemu zikomeye z'urwego bityo hagashyirwaho gahunda ihamye yo gucunga ingorane z'ikoranabuhanga;	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;	9° Concevoir et mettre en œuvre un cadre de quantification des risques afin d'évaluer efficacement dans quelle mesure l'établissement gère son cyber-risque global et atténue le cyberrisque résiduel de ses systèmes sectoriels critiques et, par conséquent, élabore un solide plan de gestion des cyberrisques;
10° Kumenyekanisha ingorane zose z'ikigo buri gihe kandi byuzuye ku nama y'ubutegetsi kugirango bifashe mu kugereranya ingorane zose hagamijwe kureba iziza imbere kurusha izindi;	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;	10° rendre compte de tous les risques de l'entreprise de manière cohérente et complète au conseil d'administration afin de permettre la comparaison de tous les risques de manière égale en s'assurant qu'ils sont correctement hiérarchisés;
11° Gukora igeregageza ry'ibitagenda neza mu ikipe;	11° Conduct red team exercises.	11° Conduire des exercices de l'équipe rouge.
12° Gukora isesengura ry'ingaruka k' ubucuruzi no gusuzuma ingorane aho bagaragaza umutungo w'ingenzi mu	12° Carry out a business impact analysis and risk assessment where they identify critical assets to their business processes	12° Réaliser une analyse d'impact sur l'entreprise et une évaluation des risques où ils identifient les actifs critiques pour

bikorwa byabo by'ubucuruzi no gutondekanya ingorane / ingaruka zibareba. Gahunda yo kwirinda ingorane igomba gutegurwa kugirango hagabanuke ingorane zagaragaye.	and class the risks/impact pertaining to them. A risk treatment plan shall be developed to mitigate the risks identified.	leurs processus d'affaires et classent les risques / impacts les concernant. Un plan de traitement des risques doit être élaboré pour atténuer les risques identifiés.
Ingingo ya 14: Isuzuma ry'abatanga serivisi bavuye hanze	**Article 14: Assessment of a Service Provider**	**Article 14: Évaluation d'un fournisseur de services**
Ikigo kigenzurwa kigomba gushyira mu bikorwa politiki n'uburyo bwateganijwe bugamije kurinda umutekano wa sisitemu y'amakuru n'amakuru atagenewe rubanda ashobora kugerwaho, cyangwa afitwe n'abatanga serivisi.	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.	Une institution réglementée doit mettre en œuvre des politiques et des procédures écrites conçues pour assurer la sécurité des systèmes d'information et des données non-publiques qui sont accessibles ou détenus par des fournisseurs de services**.**
Izi politiki n'uburyo bigomba gushingira ku isuzuma ry'ingorane z'ikigo kigenzurwa kandi zigakemura ibikurikira:	Such policies and procedures shall be based on the risk assessment of the regulated institution and shall address to the extent applicable:	Ces politiques et procédures sont fondées sur l'évaluation des risques de l'institution réglementé et portent, dans la mesure du possible:
1° kumenya no gusuzuma ibyateza ingorane by'utanga serivisi;	1° the identification and risk assessment of service providers;	1° l'identification et l'évaluation des risques des prestataires de services;
2° ibikorwa bishoboka by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho bisabwa kuba byujujwe n'abatanga serivisi	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;	2° les pratiques minimales de cybersécurité que ces prestataires de services tiers doivent respecter pour pouvoir faire affaire avec l'institution réglementés;

baturutse hanze kugirango babashe gukorana n'ikigo kigenzurwa;		
3° Igenzura ryimbitse mu gusuzuma bihagije imikorere by'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho y'abatanga serivisi biturutse hanze;	3° due diligence processes used to evaluate the adequacy of cyber security practices of such service providers;	3° les processus de diligence raisonnable utilisés pour évaluer l'adéquation des pratiques de cybersécurité de ces prestataires de services;
4° isuzuma rigaruka mu gihe runaka ry'abatanga serivisi baturutse hanze hashingiwe ku ngorane bagaragaza ndetse no gukomeza guhaza ibikorwa byabo byo gucunga umutekano wa interineti;	4° periodic assessment of such service providers based on the risk they present and the continued adequacy of their cyber security practices;	4° évaluation périodique de ces prestataires de services en fonction du risque qu'ils présentent et de l'adéquation continue de leurs pratiques de cybersécurité ;
5° Abazana ibicuruzwa n'abandi bafatanyabikorwa basuzumwa buri gihe hakoreshejwe igenzura, ibisubizo by'isuzuma, cyangwa ubundi buryo bwo gusuzuma kugirango bemeze ko bubahiriza inshingano zabo;	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;	5° Les fournisseurs et partenaires tiers sont régulièrement évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluations pour confirmer qu'ils respectent leurs obligations contractuelles ;
6° Igisubizo n'igenamigambi ryo gusubiza ibintu k' umurongo no kugerageza ibikorwa by'abatanga ibicuruzwa hamwe n'abandi batanga serivise;	6° Response and recovery planning and testing are conducted with suppliers and third- party providers;	6° La planification et les tests de réponse et de reprise sont menés avec des fournisseurs et des fournisseurs tiers ;

7° Gukora isuzuma ryihariye rikemura ibibazo byuzuzanya, nko guhuza sisitemu yo kwishyura, serivisi zohererezanya ubutumwa, imiyoboro yo gutanga amasoko, n'abandi batanga serivise zikomeye cyangwa abafatanyabikorwa.	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.	7° Effectuer des tests spécifiques qui abordent les interdépendances externes, telles que la connectivité aux systèmes de paiement, aux services de messagerie, aux canaux de livraison, aux marchés et à d'autres fournisseurs de services ou partenaires critiques.
Ingingo ya 15: Uruhare rw'urwego rw'ubugenzuzi bw'imbere Ikigo kigenzurwa kigomba gushyira mu itsinda ryacyo ry'ubugenzuzi bw'imbere abagenzuzi b'umutekano w'amakuru babishoboye. Ibikorwa byo kugenzura umutekano w'amakuru bishobora gutangwa binyuze imbere. Sisitemu y'ubugenzuzi bw'imbere igomba kuba ikwiranye n'ubunini bw'ikigo ndetse na kamere, ingano n'ibyateza ingorane z'ibikorwa byacyo bitanga isuzuma rihagije no gusuzuma sisitemu y'amakuru. Abagenzuzi b'umutekano w'amakuru mu kigo kigenzurwa bagomba kwemeza igipimo cy'ubugenzuzi kitagarukira ku mirimo ikurikira:	**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:	**Article 15 : Rôle de la fonction d'audit interne** Une institution réglementée doit intégrer des auditeurs qualifiés en sécurité de l'information au sein de son équipe d'audit interne. Les activités d'audit de sécurité de l'information peuvent être externalisées ou par le biais d'un placement interne. Les systèmes d'audit interne doivent être adaptés à la taille de l'établissement et à la nature, à l'étendue et au risque de ses activités qui prévoient des tests et un examen adéquat des systèmes d'information. Les auditeurs internes de la sécurité de l'information des institutions réglementés devraient donc veiller à ce que la portée de l'audit comprenne et ne se limite pas aux tâches ci-dessous:

1° Gukomeza gusuzuma no gutanga raporo kubyerekeye ingorane zaturuka kuri interineti kugenzura sisitemu ya ICT mu kigo kigenzurwa n'ibindi bifitanye isano n'abandi bantu;	1° Continuous review and report on cyber risks and controls of the ICT systems within the regulated institution and other related third-party connections;	1° Examen et rapport continus sur les cyberrisques et les contrôles des systèmes ICT au sein de l'institution réglementé et autres connexions tierces connexes;
2° Gukorana umwete ukwiye hagamijwe kugabanya ingorane ziturutse ku bandi bantu;	2° Conduct up-front due diligence to mitigate risks associated with third parties;	2° Effectuer une due diligence initiale pour atténuer les risques associés aux tiers;
3° gusuzuma gahunda n'uburyo bukoreshwa mu rwego rw'umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanahoko byashyizwe mu bikorwa;	3° Assess both the design and effectiveness of the cyber security framework implemented;	3° évaluer à la fois la conception et l'efficacité du cadre de cybersécurité mis en œuvre;
4° Gukora isuzuma risanzwe ryigenga no gusuzuma ahari intege nke;	4° Conduct regular independent threat and vulnerability assessment tests;	4° Effectuer régulièrement des tests indépendants d'évaluation des menaces et des vulnérabilités;
5° Kumenyesha inama y'ubutegetsi ibyavuye mu isuzuma;	5° Report to the board the findings of the assessments;	5° Faire rapport au conseil d'administration des résultats des évaluations;
6° Kumenya neza ko ahakorerwa n'ahasuzumirwa hatandukanye n'aho ibikorwa bikorerwa;	6° Ensure the development and testing environment are separate from the production environment;	6° S'assurer que l'environnement de développement et de test est séparé de l'environnement de production ;

7° gusuzuma niba gahunda yo gucunga y'ikigo yo gucunga ibyateza ingorane ikwiranye n'ubunini bwacyo n'ubunini bw'ibikorwa, imikoranire, hamwe n'ingano y'ibyateza ingorane;	7° Assess if the institution's cyber risk management framework is appropriate for its size, complexity, and scope of operations, interconnectedness, and risk profile;	7° évaluer si le cadre de gestion des cyberrisques de l'institution est adapté à sa taille, à sa complexité et à son champ d'opérations, à son interconnexion et à son profil de risque;
8° Kugira inama ubuyobozi bukuru niba politiki n'ibikorwa by'ikigo bihagije kugira ngo igendane n'ibyateza ingorane bikomoka kuri interineti bigaragara n'ibisabwa n'amabwiriza y'urwego.	8° Advise senior management on whether the institution's policies and procedures are adequate to keep up with emerging cyber risks and industry regulations.	8° Conseiller la direction générale sur l'adéquation des politiques et procédures de l'institution pour suivre les cyberrisques émergents et les réglementations du secteur.
<u>Ingingo ya 16</u>: Gusuzuma umwirondoro hakoreshejwe ibintu byinshi	**<u>Article 16</u>: Multi-Factor Authentication**	**<u>Article 16:</u> Authentification multifactorielle**
Gishingiye ku isuzuma ry'ibyagiteza ingorane cyakoze, ikigo kigenzurwa kigomba gukoresha amagenzura akwiye ashobora kuba akubiyemo gusuzuma umwirondoro w'abantu hakoreshejwe ibintu byinshi bibaranga hagamijwe kubakumira kugera ku makuru atagenewe rubanda cyangwa kuri sisitemu y'amakuru.	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.	Sur la base de son évaluation des risques, une institution réglementée doit utiliser des contrôles efficaces, qui comprendront une authentification multifactorielle basée sur les risques, pour se protéger contre tout accès non autorisé aux données non-publiques ou aux systèmes d'information.
Gusuzuma umwirondoro w'umuntu hakoreshejwe ibintu byinshi bimuranga bigomba gukorwa k' umuntu uwo ari we	Multi-factor authentication must be utilized for any individual accessing the regulated institution's internal networks from an external	L'authentification multifacteur doit être utilisée pour toute personne accédant aux réseaux internes de l'institution réglementé à

wese winjira mu miyoboro y'ikigo kigenzurwa y'imbere anyuze mu miyoboro yo hanze cyeretse gusa iyo ukuriye urwego rw'ikoranabuhanga yemeye mu nyandiko ikoreshwa ry'ubundi buryo bumeze nk'ubwo cyangwa ubundi buryo bw'igenzura bufite umutekano kurusha ubwo ngubwo.	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.	partir d'un réseau externe, à moins que le responsable de la fonction de sécurité informatique ou le personnel concerné n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement équivalents ou plus sécurisés.
Ingingo ya 17: Igabanywa ry'amakuru agomba kubikwa Ikigo kigenzurwa kigomba kugira politiki yo kubika amakuru kugirango kibungabunge umutekano no gutangwa buri gihe hashingiwe ku makuru atagenewe rubanda yagaragajwe n'isuzuma ry'ibyateza ingorane, usibye aho ayo makuru asabwa n'amategeko cyangwa amabwiriza kubikwa.	**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 17: Limitations de la conservation des données** Une institution réglementée doit avoir une politique de conservation des données pour la conservation sécurisée et l'élimination périodique de toutes les données non-publiques identifiées conformément à leur évaluation des risques, sauf lorsque ces informations doivent par ailleurs être conservées par la loi ou la réglementation.
Ingingo ya 18: Amahugurwa no kumenyekanisha Ikigo kigenzurwa kigomba: 1° gushyira mu bikorwa politiki, inzira zikurikizwa n'amagenzura ashingiye ku	**Article 18: Training and awareness** A regulated institution must: 1° design a consistent and updated security awareness program in line with	**Article 18: Formation et sensibilisation** Une institution réglementée doit: 1° concevoir un programme de sensibilisation à la sécurité cohérent et

byateza ingorane hagamijwe kugenzura ibikorwa by'abakoresha; ingamba n'ibiteye ubwoba mu mutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho ndetse n'aho ibintu bigana;	institution's risk assessment, strategy and current cyber security threats and trends;	actualisé, conforme à l'évaluation des risques de l'institution, à sa stratégie et aux menaces et tendances actuelles en matière de cybersécurité;
2° gutanga amahugurwa ahoraho yo kumenyekanisha umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho kubagize inama y'ubutegetsi, abayobozi bakuru n'abakozi bose bakorana na sisitemu y'amakuru y'ikigo harimo abakozi, abimenyereza umwuga n'abandi bantu;	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;	2° dispenser régulièrement une formation de sensibilisation à la cybersécurité aux membres du conseil d'administration, aux cadres supérieurs et à tout le personnel qui interagit avec le système d'information de l'établissement, y compris, mais sans s'y limiter, le personnel, les stagiaires, les tiers;
3° gusuzuma akamaro k'amahugurwa yo kumenyekanisha binyuze mu bibazo bisanzwe no kwigana isuzuma.	3° evaluate the effectiveness of the awareness training through regular quizzes and test simulations.	3° évaluer l'efficacité de la formation de sensibilisation à travers des quiz et des simulations de tests réguliers;
Inama y'ubutegetsi/ubuyobozi bukuru bugenera amafaranga ahagije amahugurwa n'ubukangurambaga busabwa.	Board/ Senior Management shall allocate adequate funds for all required trainings and awareness.	Le conseil d'administration / la direction générale alloue des fonds adéquats pour toutes les formations et sensibilisations requises.

Ingingo ya 19: Guhisha amakuru atagenewe rubanda	**Article 19: Encryption of non-public data**	**Article 19: Cryptage des données non-publiques**
Ikigo kigenzurwa kigomba gushyira mu bikorwa igenzura, harimo no gushyira amakuru mu ibanga, kugira ngo birinde amakuru yatanzwe cyangwa yoherejwe n'ikigo kigenzurwa haba mu nzira zinyura mu miyoboro yo hanze ndetse no m' uburuhukiro.	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.	Une institution réglementée doit mettre en œuvre des contrôles, y compris le cryptage, pour protéger les données détenues ou transmises par l'institution réglementé à la fois en transit sur des réseaux externes et au repos.
Mu gihe ikigo kigenzurwa cyemeza ko kubika amakuru mu gutambuka ku miyoboro yo hanze bidashoboka, ikigo kigenzurwa gishobora ahubwo kubona ayo makuru atagenewe rubanda hakoreshejwe uburyo bunoze bwo guhwanisha bwasuzumwe kandi bwemejwe na komite nyobozi y'ikoranabuhanga.	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.	Dans la mesure où une institution réglementée détermine que le cryptage des données en transit sur des réseaux externes est irréalisable, l'institution réglementée peut à la place sécuriser ces données non-publiques à l'aide de contrôles compensatoires alternatifs efficaces examinés et approuvés par le comité de pilotage informatique.
Mu gihe ikigo kigenzurwa gikoresha igenzura rihuza nk'uko byavuzwe haruguru, uburyo bwo guhisha amakuru no gukoresha neza igenzura rihuza rizasuzumwa na komite ishinzwe ikoranabuhanga.	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.	Dans la mesure où une institution réglementée utilise les contrôles compensatoires mentionnés ci-dessus, la faisabilité du cryptage et l'efficacité des contrôles compensatoires seront examinées par le comité de pilotage informatique.

Ingingo ya 20: Gahunda yo gukemura ibibazo bivutse	**Article 20: Incident response and business continuity management**	**Article 20: Réponse aux incidents et gestion de la continuité des activités**
Ikigo kigenzurwa kigomba gushyiraho gahunda yo gukemura ibibazo bivutse yanditse igamije gukemura ibyo bibazo ako kanya no kuyikura mu kibazo icyo aricyo cyose cyerekeranye n'umutekano wa interineti bikibangamira ibanga, ubudakemwa cyangwa ukuboneka k' uburyo bukoresha ikoranabuhanga bukoreshwa n'ikigo cyangwa imikorere ihoraho y'ubwoko ubwo ari bwo bwose bw'ubucuruzi cyangwa bw'ibikorwa by'ikigo.	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.	Une institution réglementée doit établir un plan écrit de gestion des réponses aux incidents conçu pour répondre, contenir et récupérer rapidement les perturbations causées par tout cyberincident affectant matériellement la confidentialité, l'intégrité ou la disponibilité des systèmes d'information de l'institution ou la fonctionnalité continue de tout aspect de l'entreprise ou les opérations de l'institution.
Gahunda yo gukemura ibibazo bivutse igomba kwita kuri ibi bintu bikurikira:	The incident response and business continuity management plan shall address the following areas:	Le plan de gestion de la réponse aux incidents et de la continuité des activités doit aborder les domaines suivants:
1° Inzira z'imbere zikurikizwa mu gukemura ikibazo cyerekeranye n'igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho;	1° the internal processes for responding to cyber security incident and disasters;	1° les processus internes de réponse aux incidents et catastrophes de cybersécurité;
2° Intego za gahunda yo gukemura ibibazo bivutse;	2° the goals of the incident response and business continuity plans;	2° les objectifs des plans d'intervention en cas d'incident et de continuité des activités;

3° Gusobanura mu buryo bwumvikana uruhare, inshingano n'inzego z'ubuyobozi zifatirwamo ibyemezo;	3° the definition of clear roles, responsibilities and levels of decision-making authority;	3° la définition de rôles, de responsabilités et de niveaux de décision clairs;
4° Itumanaho no guhanahana amakuru imbere mu kigo no hanze yacyo;	4° external and internal communications and information sharing;	4° les communications externes et internes et le partage d'informations;
5° Kumenya ibikenewe mu rwego rwo kongera ingufu ahagaragaye intege nke mu buryo bwo guhanahana amakuru bukoreshwa n'ubugenzuzi bijyana;	5° identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;	5° l'identification des exigences pour la correction des faiblesses identifiées dans les systèmes d'information et les contrôles associés;
6° Gukora inyandiko na raporo ku bikorwa bihungabanya umutekano w'ibijyanye n' ikoranabuhanga no ku bikorwa byerekeranye no gukemura ibibazo byavutse;	6° documentation and reporting on cyber incidents / attacks and related incident response activities;	6° documentation et rapports sur les cyberincidents / attaques et les activités de réponse aux incidents connexes;
7° Gusuzuma no gusubiramo gahunda yo gukemura ibibazo bivutse uko bibaye ngombwa hakurikijwe igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho cyabaye;	7° the evaluation and revision as necessary of the incident response and business continuity plans following a cyber security event;	7° l'évaluation et la révision si nécessaire des plans de réponse aux incidents et de continuité d'activité suite à un événement de cybersécurité ;
8° kumenya no kugabanya ingorane zaterwa n' ikoranabuhanga no guhuza	8° identification and mitigation of cyber risks posed through interconnectedness to sector	8° identification et atténuation des cyberrisques posés par l'interconnexion

abafatanyabikorwa bo mu rwego rw'imari , abafatanyabikorwa bo hanze n'abandi bantu kugira ngo birinde ko ingorane zakwirakwira ;	partners, external stakeholders and other third parties to prevent cyber risk contagion;	avec les partenaires du secteur, les parties prenantes externes et d'autres tiers pour prévenir la contagion des cyberrisques;
9° ishyirwa mu bikorwa rya gahunda nziza yo kuzamura ifitanye isano n'inzego zifata ibyemezo, uburyo bwo kwirinda ingorane zikomoka kuri interineti zikwirakwiye, ingamba z'itumanaho, hamwe n'uburyo bwo kwinjiza amasomo yakuwe muri gahunda y' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho.	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.	9° mise en œuvre de protocoles d'escalade efficaces liés aux niveaux de décision de l'organisation, aux procédures de confinement de la cyber contagion, aux stratégies de communication et aux processus pour intégrer les leçons apprises dans le programme de cybersécurité.
<u>Ingingo ya 21</u>: Kumenyesha no gutanga raporo kubyabaye ku bijyanye n'ikoranabuhanga Ikigo kigenzurwa kigomba kumenyesha Urwego rw'ubugenzuzi byihuse bishoboka mu gihe kitarenze amasaha abiri (2) uhereye igihe ikibazo cyabereye cyangwa byemejwe ko habaye ikibazo gifitanye isano n'ikoranabuhanga cyaba ari kimwe muri ibi bikurikira:	**<u>Article 21</u>: 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:	**<u>Article 21</u>: Notification et signalement du cyberincident** Une institution réglementée doit informer l'Autorité de Contrôle le plus rapidement possible dans un délai ne dépassant pas deux (2) heures à compter de la survenance de l'incident ou à partir de la détermination qu'un incident de cybersécurité s'est produit qui est l'un des suivants**:**

1° Igikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho gishobora kubuza ikigo kigenzurwa gukomeza ibikorwa byacyo bisanzwe byo guha serivisi z'imari abakiriya bacyo;	1° Cyber security incident that may disrupt a regulated institution from continuing its normal operations for customer-facing transactions;	1° incident de cybersécurité pouvant empêcher une institution réglementée de poursuivre ses opérations normales pour les transactions avec les clients;
2° Ibikorwa bihungabanya umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho uko bigaragara bishobora guhungabanya k'uburyo bugaragara igice gifatika cy'ibikorwa bisanzwe by'ikigo.	2° Cyber security events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the institution.	2° les événements de cybersécurité qui ont une probabilité raisonnable de nuire matériellement à une partie importante du (des) fonctionnement (s) normal (s) de l'établissement.
Ikigo kigenzurwa kigomba gushyikiriza Urwego rw'ubugenzuzi raporo yuzuye y'igikorwa gihungabanya umutekano mu gihe cy'amasaha 24 kuva igikorwa kibaye nk; uko bikubiye k' umugereka w'aya mabwiriza rusange.	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.	Une institution réglementée doit soumettre à l'Autorité de contrôle le rapport d'incident complet dans les 24 heures suivant la survenance de l'incident conformément à l'annexe du présent règlement.
Ibyihariye byerekeye gutanga raporo ku gikorwa gihungabanya umutekano w'ibijyanye n'ikoranabuhanga bishobora kuganwa n'amabwiriza.	Specific reporting requirements on cyber security incident may be provided in the Directive.	Des exigences spécifiques en matière de rapports d'incident de cybersécurité peuvent être prévues dans la directive.

Ikigo kigenzurwa kigomba gushyikiriza Urwego rw'ubugenzuzi inyandiko nk'uko igaragara ku mugereka yemeza ko gahunda y'ikigo kigenzurwa y' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho cyubahiriza ibyo gisabwa n'aya mabwiriza. Iyo nyandiko igomba gushyikirizwa Urwego rw'ubugenzuzi mu gihe kitarenze itariki ya 15 Mutarama buri mwaka.	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.	Une institution Réglementée soumet à l'Autorité de contrôle sur une base annuelle une déclaration écrite conformément à l'annexe certifiant que le programme de cybersécurité de l'institution réglementée est conforme aux exigences énoncées dans le présent règlement. Le relevé doit être soumis au plus tard le 15 janvier de chaque année.
Ingingo ya 22: Inyandiko yo kwisuzuma Ikigo kigenzurwa kigomba gushyikiriza Urwego rw'ubugenzuzi buri mwaka inyandiko yanditse yo kwisuzuma ikubiye ku mugereka yemeza ko ingamba z' umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho z'ikigo kigenzurwa zubahiriza ibisabwa bivugwa muri aya mabwiriza. Inyandiko itangwa bitarenze ku ya 15 Mutarama ya buri mwaka.	**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.	**Article 22: Déclaration d'auto-évaluation** Une institution réglementée doit soumettre à l'Autorité de contrôle sur une base annuelle une déclaration écrite d'auto-évaluation conformément à l'annexe certifiant que la stratégie de cybersécurité de l'institution réglementée est conforme aux exigences énoncées dans le présent règlement. Le relevé doit être soumis au plus tard le 15 janvier de chaque année.

UMUTWE WA III: INGINGO ZINYURANYE N'IZISOZA	**CHAPTER III: MISCELLANEOUS AND FINAL PROVISIONS**	**CHAPITRE III: DISPOSITIONS DIVERSES ET FINALES**
Ingingo ya 23: Ikurikizwa ry'andi mategeko Bitabangamiye ibivugwa muri aya mabwiriza rusange, ikigo kigenzurwa kigomba kubahiriza ibindi bisabwa n'amategeko n'amabwiriza akurikizwa mu gucunga umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho no kurinda amakuru y'ibanga.	**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 23: Application d'autres lois** Sans préjudice des dispositions du présent règlement, une institution réglementée se conforme aux autres exigences légales et réglementaires applicables à la cybersécurité et à la protection des données et de la vie privée.
Ingingo ya 24: Ibisabwa byihariye Ibigo bigenzurwa byubahiriza ibikubiye muri aya mabwiriza rusange, keretse Urwego rw'ubugenzuzi rushizeho amabwiriza agena ibisabwa bikwiranye n'ikigo hashingiwe ku miterere, ingano, imikomerere n'iterambere ry'ibikorwa byacyo.	**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 24: Exigences adaptées** Les institutions réglementées doivent se conformer aux dispositions du présent règlement, l'autorité de contrôle peut par une directive émettre des exigences adaptées, proportionnelles à la nature, à la taille, à la complexité et à la maturité de ses activités.

Ingingo ya 25: Ibihano n'ibyemezo byo mu rwego rw'ubutegetsi Iyo ikigo kigenzurwa cyitabashije kubahiriza ibisabwa muri aya mabwiriza, Urwego rw 'ubugenzuzi ishobora kugifatira ibihano biteganywa n'amabwiriza rusange yihariye.	**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 25: Pénalités et sanctions administratives** Lorsqu'une institution réglementée ne satisfait pas à l'une des exigences du présent règlement, l'Autorité de contrôle peut appliquer les sanctions prévues par les dispositions pertinentes des règlements spécifiques concernés.
Ingingo ya 26: Igihe cy'inzibacyuho Ibigo bigenzurwa bitari bisanzwe bikurikiza aya mabwiriza rusange bihawe igihe cy'umwaka umwe ngo cyubahirize aya mabwiriza rusange uhereye igihe atangarijwe mu igazetti ya Republika y'u Rwanda.	**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 26: Période de transition** Les institutions réglementées qui ne respectent pas les dispositions de ce règlement disposent d'un délai d'un an pour s'y conformer à compter de la publication au Journal Officiel de la République du Rwanda.
Ingingo ya 27: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange Aya mabwiriza rusange yateguwe, asuzumwa kandi yemezwa mu rurimi rw'Icyongereza	**Article 27: Drafting, consideration and approval of this Regulation** This regulation was prepared, considered and approved in English	**Article 27: Initiation, examen et approbation du présent règlement** Le présent Règlement a été initié, examiné et approuvé en anglais.

<u>Ingingo ya 28</u>: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza rusange Amabwiriza rusange N^{o} 02/2018 yo ku wa 24/01/2018 yerekeye umutekano w'ibijyanye n'ikoranabuhanga mu itangazabumenyi n'itumanaho n'izindi ngingo zose zibanziriza aya mabwiriza rusange zinyuranye na yo zivanyweho.	**<u>Article 28:</u> Repealing Provision** The regulation N^{o} 02/2018 of 24/01/2018 on cyber security and any prior provisions contrary to this regulation are hereby repealed.	**<u>Article 28</u>: Disposition abrogatoire** Le règlement N ° 02/2018 du 24/01/2018 sur la cybersécurité et toute disposition antérieure contraire au présent règlement sont abrogés.
<u>Ingingo ya 29</u>: Igihe aya mabwiriza rusange atangirira gukurikizwa Aya mabwiriza rusange atangira gukurikizwa ku munsi atangarijweho mu Igazeti ya Leta ya Repubulika y'u Rwanda.	**<u>Article 29:</u> Commencement** This regulation comes into force on the date of its publication in the Official Gazette of the Republic of Rwanda.	**<u>Article 29</u>: Entrée en vigueur** Le présent règlement entre en vigueur le jour de sa publication au Journal Officiel de la République du Rwanda.

Kigali 02/06/2022

(sé)

RWANGOMBWA John
Guverineri
Governor
Gouverneur

Bibonywe kandi bishyizweho Ikirango cya Repubulika:
Seen and sealed with the Seal of the Republic:
Vu et scellé du Sceau de la République:

(sé)

Dr UGIRASHEBUJA Emmanuel
Minisitiri w'Ubutabera akaba n'Intumwa Nkuru ya Leta
Minister of Justice and Attorney General
Ministre de la Justice et Garde des Sceaux

UMUGEREKA WA MBERE: INYANDIKO IGARAGAZA RAPORO Y'IBYABAYE MU MUTEKANO W'IBIJYANYE N'IKORANABUHANGA

No	Itariki y'igikorwa	Isaha y'igikorwa	Ubwoko bw'igikorwa	Aho ibintu byabereye/ ishami	Icyakozwe	Igihe byakemukiye	Ikigereranyo cy'ingaruka byateje (Mu mafaranga cyangwa mu mikorere)	Abashinzwe kubahiriza amategeko bahageze	Ibyemezo byafashwe mu gukumira ibindi bikorwa mu hazaza

APPENDIX 1: CYBER SECURITY INCIDENT REPORT FORMAT

Nº	**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**

ANNEXE 1 : FORMULAIRE DE RAPPORT D'INCIDENT DE CYBERSECURITE

No	**date de l'incident**	**Heure de l'incident**	**Type / nature de l'incident (a)**	**Emplacement physique / succursale**	**Action prise**	**Temps de résolution**	**Estimé / réel impact de la incident (Financier et Opérationnel) (b)**	**ceux qui appliquent la loi impliqués**	**Mesures prises pour atténuer les incidents futurs**

UMUGEREKA WA 2

(Izina ry'ikigo kigenzurwa)

Itariki……..

Inyandiko igaragaza ukwisuzuma

Inama y'ubutegetsi [cyangwa Umuyobozi mukuru w'ikigo kigenzurwa] iremeza:

(1) Inama y'ubutegetsi (cyangwa izina ry'umuyobozi mukuru) yasuzumye inyandiko, raporo, impamyabumenyi n'ibitekerezo by'abo bakozi, abakozi, abahagarariye, abacuruzi bo hanze n'abandi bantu cyangwa bya ngombwa;

(2) Mu bumenyi bw'abagize inama y'ubutegetsi [Izina ry'umuyobozi mukuru] Gahunda y'umutekano wa interineti cyangwa gahunda [izina ry'ikigo kigenzurwa] ku itariki ya ……/……./….. [Itariki ibyemezo by'inama y'ubutegetsi byafatiweho cyangwa ubuyobozi bukuru mu kubahiriza ibyagaragajwe mu mwaka urangira……../…../ …….[Umwaka inama y'ubutegetsi yafatiyeho imyanzura cyangwa iyubahirizwa ry'ibyabonetse yatangiwe] byubahiriza aya mabwiriza rusange [Nimero y'amabwiriza]

(Amazina …….Itariki: _____

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: _____

ANNEXE 2

(Nom de l'institution réglementé)

Date……..

Déclaration d'auto-évaluation

Le conseil d'administration [ou un (des) dirigeant (s) supérieur (s) de l'institution réglementé] certifie:

(1) Le conseil d'administration (ou le nom du ou des hauts dirigeants) a examiné les documents, rapports, certifications et opinions de ces dirigeants, employés, représentants, fournisseurs externes et autres personnes ou entités, le cas échéant;

(2) Au meilleur de la connaissance du Conseil d'administration [ou nom du ou des hauts fonctionnaires], la stratégie ou le programme de cybersécurité de (Nom de l'institution réglementé) en date du ____ / _____ / _____ (date de la résolution du conseil ou du haut fonctionnaire (s)) La constatation de conformité pour l'année terminée le _____ / ____ / _____ (année pour laquelle la résolution du Conseil ou la constatation de conformité est fournie) est conforme au présent règlement (numéro de règlement).

Signé par le président du conseil d'administration (ou le chef de la direction)

(Nom …….date: _____

IBONYWE KUGIRANGO BISHYIRWE KU MUGEREKA W' AMABWIRIZA RUSANGE Nº 50/2022 YO KU WA 02/06/2022 YEREKEYE UMUTEKANO W'IBIJYANYE N'IKORANABUHANGA MU ITANGAZABUMENYI N'ITUMANAHO MU BIGO BIGENZURWA

SEEN TO BE ANNEXED ON REGULATION Nº50/2022 OF 02/06/2022 ON CYBER SECURITY IN REGULATED INSTITUTIONS

VU POUR ETRE ANNEXE AU REGLEMENT Nº50/2022 DU 02/06/2022 SUR LA CYBERSECURITE DANS LES INSTITUTIONS REGLEMENTEES

Kigali, 02/06/2022

(sé)

RWANGOMBWA John
Guverineri
Governor
Gouverneur

Bibonywe kandi bishyizweho Ikirango cya Repubulika:
Seen and sealed with the Seal of the Republic:
Vu et scellé du Sceau de la République:

(sé)

Dr UGIRASHEBUJA Emmanuel
Minisitiri w'Ubutabera akaba n'Intumwa Nkuru ya Leta
Minister of Justice and Attorney General
Ministre de la Justice et Garde des Sceaux