Ibirimo/Summary/Sommaire page/urup.

A. Amabwiriza / Regulations/ Règlements

Nº 2100 /2018 - 008[614] yo ku wa 25/07/2018
Amabwiriza rusange ya Banki Nkuru y'u Rwanda yerekeye ibisabwa mu gutanga raporo…..3
Nº 2100 /2018 - 008[614] of 25/07/2018
Regulation of the National Bank of Rwanda on reporting requirements……...3
Nº 2100 /2018 - 008[614] du 25/07/ 2018
Règlement de la Banque Nationale du Rwanda relatif aux exigences de rapport……3

Nº 2100 /2018 - 009[614] yo ku wa 25/07/2018
Amabwiriza rusange ya Banki Nkuru y'u Rwanda yerekeye imicungire y'ibyateza ingorane amabanki……..16
Nº 2100 /2018 - 008[614] of 25/07/2018
Regulation of the National Bank of Rwanda on risk management for banks……..16
Nº 2100 /2018 - 008[614] du 25/07/ 2018
Règlement de la Banque Nationale du Rwanda du sur la gestion des risques pour les banques.……....16

B. Guhindura amazina/ Change of names / Changement de noms

Icyemezo gitanga uburenganzira bwo guhindura izina:

- NGAYABO Evode ……..104
- UMUBERA Grace Sarah ……105
- KAZENEZA Gloria ……106
- UWIMANA Théophila.……107
- NKUSI Benjamin.…….....108
- NDABARAMIYE Heritier ……...109
- NYIRAMBEBA Philomène ……110
- January Narcisse ……...111
- MUNYANKUSI Lwanga Thierry ……112
- SEMASAKA Eriel.……113
- BUGINGO Keith ……..114
- DUSABE Marie Claire Aimée ……115
- KAYITESI GASANA Melysa ……116
- KARARA Paul Alice ……...117
- NARAME Gaudence ……....118
- BANDI Emmanuel ……...119
- MBARUSHUMURAGE Boanerge ……..120
- NYIRAGARUKA Aline ……...121
- KINANI Delphine ……122

Ingingo z'ingenzi z'urwandiko rusaba guhindura amazina:

- INGABIRE Jean Marie Pacifique ……...123
- NYIRANTAMBARA Dative ……..123
- UZAMUKUNDA Beatrice ……..124
- RWIYEREKA NYIRABURANGA BOKANGA Claire.…….124
- WIBABARA Diane ……125
- SIMBI Sandra …….....125
- UMULISA Soleil ……126
- BARAYAVUGA.……..126
- UWAMAHORO Deborah.……127
- MBISHIBISHI Adolphe ……..127
- KABASINGE Barnabe ……128
- BIGONZIKI Jeanne ……128

C. Amakoperative / Cooperatives / Coopératives

- GATSIBO AGROPROCESSING COOPERATIVE.…….129
- KORANUMURAVA BUTARE.……..130
- CODFM - KOREREJO.……131
- KOWIRU.……..132
- IMBONEZA - KAVUMU ……...133
- DUFATANYE RUSORORO ……..134
- KKAEP.…….135
- DUKOMEZANYE - NKANGA.……...136
- ABABUNGABUNGA INGAGI ……..137
- COOTRAMOKI.……138
- ABAHUJUMURIMO GASANZE.……139
- COSHIKIGI ……..140

AMABWIRIZA RUSANGE YA BANKI NKURU Y'U RWANDA Nº 2100 /2018 - 008[614] YO KU WA 25/07/2018 YEREKEYE IBISABWA MU GUTANGA RAPORO

REGULATION OF THE NATIONAL BANK OF RWANDA Nº 2100 /2018 - 008[614] OF 25/07/2018 ON REPORTING REQUIREMENTS

REGLEMENT DE LA BANQUE NATIONALE DU RWANDA Nº 2100 /2018 - 008[614] DU 25/07/ 2018 RELATIF AUX EXIGENCES DE RAPPORT

ISHAKIRO

TABLE OF CONTENTS

TABLE DES MATIERES

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza rusange agamije

Ingingo ya 2: Ibisobanuro

UMUTWE WA II: KUBONA AMAKURU

Ingingo ya 3: Uburyo bukurikizwa mu kugaragariza Banki Nkuru amakuru

Ingingo ya 4: Kugaragaza amakuru

Ingingo ya 5: Ubwoko bw'amakuru agaragazwa n'ibigo bigenzurwa

Ingingo ya 6: Kuva mu muyoboro njyanamakuru wikoresha (ADF) ujya mu muyoboro njyanamakuru utikoresha (NONADF)

Ingingo ya 7: Gusoza Umwaka w'Ibaruramari

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this regulation

Article 2: Definitions

CHAPTER II:DATA READINESS

Article 3: Process of availing data to the Central Bank

Article 4: Availability of data

Article 5: Types of data to be availed by supervised institutions

Article 6: Switching from ADF to NONADF

Article 7: Closure of Financial Year

CHAPITRE PREMIER: DISPOSITIONS GENERALES

Article premier: Objet du présent règlement

Article 2: Définitions

CHAPITRE II: MISE A DISPOSITION DE DONNEES

Article 3: Processus de mise à disposition de données à la Banque Centrale

Article 4: Disponibilité des données

Article 5: Types de données devant être utilisées par les institutions supervisées

Article 6: Passage de l'ADF au NONADF

Article 7: Clôture de l'Exercice Financier

Ingingo ya 8: Gusaba amakuru y'inyongera	**Article 8: Request for further information**	**Article 8: Demande d'informations complémentaires**
UMUTWE WA III: AMAKURU AFITE IREME KANDI ATANGANYWE UBUSHISHOZI	**CHAPTER III:DATA INTEGRITY AND QUALITY**	**CHAPITRE III : INTEGRITE ET QUALITE DES DONNEES**
Ingingo ya 9: Inkomoko y'amakuru	**Article 9:Data Source**	**Article 9: Source de données**
Ingingo ya 10: Kwemeza amakuru atanzwe	**Article 10: Data Validation**	**Article 10: Validation des données**
Ingingo ya 11: Kuba amakuru ari ukuri kandi yuzuye	**Article 11: Data Accuracy and Completeness**	**Article 11: Exactitude et exhaustivité des données**
Ingingo ya 12: Guhindura amakuru	**Article 12: Data modification**	**Article 12: Modification des données**
Ingingo ya 13: Ireme ry'uburyo bukoresha ikoranabuhanga	**Article 13: Soundness of ICT System**	**Article 13: Qualité du système des TIC**
UMUTWE WA IV: INGINGO ZISOZAIngingo	**CHAPTER IV: FINAL PROVISIONS**	**CHAPITRE IV: DISPOSITIONS FINALES**
ya 14: Ibihano by'amafaranga	**Article 14: Pecuniary sanctions**	**Article 14: Sanctions pécuniaires**
Ingingo ya 15: Igihe cy'inzibacyuho	**Article 15:Transition Period**	**Article 15: Période de transition**
Ingingo ya 16: Ivanwaho ry'ingingo inyuranyije n'aya mabwiriza rusange	**Article 16: Repealing provisions**	**Article 16: Dispositions abrogatoire**
Ingingo ya 17: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange	**Article 17: Drafting, consideration and approval of this regulation**	**Article 17: Initiation, examen et approbation du présent règlement**
Ingingo ya 18: Igihe aya mabwiriza atangira gukurikizwa	**Article 18: Commencement**	**Article 18: Entrée en vigueur**

AMABWIRIZA RUSANGE YA BANKI NKURU Y'U RWANDA Nº2100 /2018 - 008[614] YO KU WA 25/07/2018 YEREKEYE IBISABWA MU GUTANGA RAPORO	REGULATION OF THE NATIONAL BANK OF RWANDA Nº 2100/2018 - 008[614] OF 25/07/2018 ON REPORTING REQUIREMENTS	REGLEMENT DE LA BANQUE NATIONALE DU RWANDA Nº 2100 /2018 - 008[614] DU 25/07/ 2018 RELATIF AUX EXIGENCES DE RAPPORT
Ishingiye ku Itegeko n° 40/2008 ryo ku wa 26/08/2008 ryerekeye imitunganyirize y'imikorere y'ibigo by'imari icirirtse, nk'uko ryahinduwe kugeza ubu, cyane cyane mu ngingo zaryo iyi 40 n'iya 41;	Pursuant to the Law n° 40/2008 of 26/08/2008 establishing the organisation of micro finance activities, as amended to date, especially its articles 40 and 41;	Vu la loi n° 40/2008 du 26/08/2008 portant organisation des activités de microfinance, telle que modifiée à ce jour, spécialement en ses articles 40 et 41 ;
Ishingiye ku Itegeko n° 52/2008 ryo ku wa 10/09/2008 ryerekeye imitunganyirize y'umurimo w'ubwishingizi cyane cyana mu ngingo yaryo ya 52;	Pursuant to the Law nº 52/2008 of 10/09/2008 governing the organization of insurance business, especially its article 52;	Vu la loi n° 52/2008 du 10/09/2008 régissant l'organisation des activités d'assurances, spécialement en ses articles, spécialement en son article 52;
Ishingiye ku Itegeko n° 03/2010 ryo ku wa 26/02/2010 ryerekeye uburyo bw'imyishyuranire, cyane cyane mu ngingo zayo iya 8 n'iya 9 ;	Pursuant to the Law n° 03/2010 of 26/02/2010 concerning Payment System, especially its articles 8 and 9;	Vu la Loi n° 03/2010 du 26/02/2010 relative au Système de Paiement, spécialement en ses articles 8 et 9;
Ishingiye ku Itegeko n° 16/2010 ryo ku wa 7/05/2010 rigenga uburyo bwo guhanahana amakuru ku nguzanyo mu Rwanda, cyane cyane mu ngingo yayo ya 3;	Pursuant to Law nº 16/2010 of 7/05/2010 governing Credit Information System in Rwanda, especially its articles 3;	Vu la loi n° 16/2010 du 7/05/2010 régissant le système d'information sur les crédits au Rwanda, spécialement en son article 3;
Ishingiye ku Itegeko n° 05/2/2015 ryo ku wa 30/03/2015 ryerekeye imitunganyirize y'ubwiteganyirize bwa pansiyo, cyane cyane mu ngingo yaryo ya 79;	Pursuant to the Law nº 05/2/2015 of 30/03/2015 governing organization of pension schemes, especially its article 79;	Vu la loi n° 05/2/2015 du 30/03/2015 portant organisation des régimes de pension, spécialement en son article 79 ;
Inshingiye ku Itegeko n° 31/2015 ryo ku wa 05/06/2015 rigena imiterere n'imikorere by'ikigega cy'ubwishingizi bw'amafaranga	Pursuant to Law n°31/2015 of 05/06/2015 determining the organization and functioning of deposit guarantee fund for banks and microfinance institutions especially its article 13;	Vu la loi n°31/2015 du 05/06/2015 portant organisation et fonctionnement du fonds de garantie des dépôts pour les banques et les

yabikijwe mu mabanki no mu bigo by'imari icirirtse cyane cyane ingingo yayo ya 13;

Ishingiye ku Itegeko n° 48/2017 ryo ku wa 23/09/2017 rigenga Banki Nkuru y'u Rwanda, cyane cyane mu ngingo zaryo, iya 8 n'iya 10;

Ishingiye ku Itegeko n° 47/2017 ryo ku wa 23/09/2017 ryerekeye imitunganyirize y'imirimo y'amabanki, cyane cyane mu ngingo zaryo iya 61, iya 63 n'iya 117 ;

Isubiye ku ibwiriza n° 02/2009 ryerekeye imitunganyirize y'imikorere y'ibigo by'imari icirirtse cyane cyane mu ngingo yaryo ya 33;

Isubiye ku Mabwiriza nº 05/2009 yo kuwa 29/07/2009 yerekeye iyemererwa n'ibindi bisabwa mu murimo w'ubwishingizi cyane cyane ingingo yayo iya 24, iya 25 n'iya 26;

Isubiye ku Mabwiriza n°06/2009 yo kuwa 29/07/2009 ku iyemezwa n'ibindi bisabwa ku bahuza b'ubwishingizi cyane cyane mu ngingo yayo ya 24;

Isubiye ku Mabwiriza n°001/2016 yo kuwa 18/05/2016 ya Banki Nkuru y'u Rwanda yerekeye imikorere y'Ikigega cy'Ubwishingizi bw'amafaranga yabikijwe mu mabanki no mu bigo by'imari icirirtse cyane cyane ingingo yayo ya 19;

Isubiye ku Mabwiriza nº 05/2016 yo kuwa 26/09/2016 ya Banki Nkuru y'u Rwanda agena ibisabwa ku mikorere n'ibindi bisabwa mu

institutions de microfinance, spécialement son article 3;

Pursuant to the Law nº 48/2017 of 23/09/2017 governing the National Bank of Rwanda, especially its articles 8 and 10;

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

Pursuant to the Law nº 47/2017 of 23/09/2017 governing the Organisation of Banking, especially its articles 61, 63 and 117;

Vu la loi n° 47/2017 du 23/09/2017 portant organisation de l'activité bancaire, spécialement en ses articles 61, 63 et 117

Having reviewed the Regulation n° 02/2009 on the organisation of microfinance activity especially its article 33;

Revu le règlement n° 02/2009 relatif à l'organisation de l'activité de microfinance spécialement en son article 33 ;

Having reviewed the Regulation n°05/2009 of 29/07/2009 on licensing requirements and other requirements for carrying out insurance business especially its articles 24, 25 and 26;

Revu le règlement n° 05/2009 relatif aux conditions d'agrément et autres conditions requises pour l'exercice de l'activité assurance spécialement ses article 24,25 and 26 ;

Having reviewed the Regulation nº 06/2009 of 29/07/2009 on licensing requirements and other requirements for insurance intermediaries especially its article 24;

Revu le règlement nº6/2009 du 29/07/2009 relatif aux conditions d'agrément et autres conditions requises pour intermédiaires d'assurance spécialement en son article 24 ;

Having reviewed the Regulation n°001/2016 of 18/05/2016 concerning operations of the deposit guarantee fund for banks and microfinance institutions especially its article 19;

Revu le règlement nº 001/2016 of 18/05/2016 concernant le fonctionnement du fonds de garantie des dépôts pour les banques et les institutions de microfinance spécialement son article 19 ;

Having reviewed the Regulation of the National Bank of Rwanda nº 05/2016 of 26/09/2016

Revu le règlement de la Banque Nationale du Rwanda nº 05/2016 du 26/09/2016 sur les exigences opérationnelles et autres exigences pour

bwiteganyirize bwa pansiyo cyane cyane ingingo yayo ya 18;

Isubiye ku Mabwiriza rusange n° 01/2017 yo kuwa 22/02/2017 agenga ibiro by'ivunjisha cyane cyane ingingo yayo ya 25;

Isubiye ku Mabwiriza rusange n° 05/2018 yo ku wa 27/03/2018 agenga abatanga serivisi zo kwishyurana cyane cyane mu ngingo yayo ya 40;

Isubiye ku mabwiriza rusange nº 02/2012 yo kuwa 30/04/2012 agena raporo zisabwa amabanki;

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

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza rusange agamije

Aya mabwiriza rusange agamije gushyiraho uburyo bw'ikoranabuhanga ibigo bigenzurwa bikoresha mu guha Banki Nkuru amakuru bisabwa, agomba kuba ari ay'ukuri, yuzuye kandi bikayatangira igihe.

Ingingo ya 2: Ibisobanuro

Muri aya mabwiriza rusange, uretse aho biteganyijwe ukundi, amagambo n'imvugo bikoreshwa bifite ibisobanuro bikurikira:

establishing operational and other requirements for pension schemes especially its article 18;

Having reviewed the Regulation n° 01/2017 governing of 22/02/2017 foreign exchange bureaus especially its article 25;

Having reviewed the Regulation n° 05/2018 of 27/03/2018 governing payment services providers especially its 40;

Having reviewed the regulation nº 02/2012 of 30/04/2012 on reporting requirements from banks;

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

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this regulation

This regulation aims at creating an electronic platform from which supervised institutions shall provide to the Central Bank with accurate, complete and timely required data.

Article 2: Definitions

In this regulation, unless the context requires otherwise, the following words and expressions shall mean:

les régimes de pension spécialement son article 18 ;

Revu le règlement n° 01/2017 du 22/02/2017 régissant l'activité de bureaux de change, spécialement en son article 25 ;

Revu le règlement n° 05/2018 du 27/03/2018 régissant les prestataires de services de paiement spécialement son article 40 ;

Revu le règlement nº 02/2012 du 30/04/2012 portant sur des rapports exigés aux banques;

La Banque Nationale du Rwanda, ci-après dénommée la « Banque Centrale », édicte :

CHAPITRE PREMIER: DISPOSITIONS GENERALES

Article premier: Objet du présent règlement

Le présent règlement vise à créer une plate-forme électronique à partir de laquelle les institutions supervisées doivent fournir à la Banque Centrale des données requises exactes, complètes et en temps opportun.

Article 2 : Définitions

Dans le présent règlement, à moins que le contexte ne l'exige autrement, les mots et expressions suivants signifient :

1° **Ububiko bw'Amakuru (DWH)**: ubushyinguro bwa Banki Nkuru bukusanyirizwamo amakuru yerekeye ikigo, akubiyemo ibisabwa byose, agenda ahinduka akurikije igihe kandi afite ireme akanafasha ubuyobozi mu ifatwa ry'ibyemezo ; cyangwa ububiko bwagutse bw'amakuru yakusanyijwe aturutse ahantu hatandukanye mu bafatanyabikorwa ba Banki Nkuru kandi bwifashishwa mu guha Banki Nkuru umurongo igenderaho ifata ibyemezo birebana na politiki y'ifaranga no kudahungabana k'urwego rw'imari.

2° **Ikigo kigenzurwa**: ikigo cyose kigenzurwa kandi gikuriranwa na Banki Nkuru;

3° **Umuyoboro njyanamakuru wikoresha** (**ADF**): uburyo bwikoresha buhita bwohereza amakuru mu Bubiko bw'Amakuru asabwa na Banki Nkuru aturutse mu buryo bukoreshwa n'ikigo kigenzurwa na yo hatagombye gukoreshwa intoki cyangwa kugira ikindi kiyakosorwaho. Amakuru aboneka aho yoherejwe afite ikimenyetso ko ashobora guhita yifashishwa;

4° **Umuyoboro njyanamakuru utikoresha (NON ADF**): uburyo bwo kohereza amakuru mu bubiko bw'amakuru bwa Banki Nkuru aturutse mu bubiko bw'ikigo

1° **Data Warehouse (DWH):** a repository for the Central Bank that is subject-oriented, integrated, time-variant and non-volatile collection of data in support of management's decision-making process; or a large store of data accumulated from a wide range of sources within Central Bank stakeholders and used to guide Central Bank monetary policy and financial stability decisions.

2° **Supervised institution:** any institution regulated and supervised by the Central Bank;

3° **Automated Data Flow (ADF):** automatic and direct transmission to the Central Bank's Data Warehouse of required data from a supervised institution's source system without any manual intervention or adjustment. Data are availed with readiness flag;

4° **Non Automated Data Flow (NON ADF):**transmission to the Central Bank's Data Warehouse of data from a supervised

1° **Entrepôt de données (DWH)**: un référentiel de la Banque Centrale utilisé pour la collecte de données orientées, intégrée, variable dans le temps et non volatile pour appuyer le processus décisionnel de la direction; ou un grand stock de données accumulées auprès d'un large éventail de sources au sein des partenaires de la Banque Centrale et utilisé pour guider les décisions de la politique monétaires et de stabilité financière.

2° **Institution supervisée**: toute institution réglementée et supervisée par la Banque Centrale;

3° **Flux de Données Automatisé** (**ADF**) : transmission automatique et directe à l'entrepôt de données de la Banque Centrale des données requises provenant du système source d'une institution supervisée, sans aucune intervention manuelle ou ajustement. Les données sont disponibles avec un indicateur de disponibilité ;

4° **Flux de Données Non-Automatisé (NONADF**) : transmission à l'entrepôt de données de la Banque Centrale des données provenant de la base de données

kigenzurwa na yo cyangwa uburyo bukoreshwa hifashishijwe intoki;

5° **Banki Nkuru**: Banki Nkuru y'u Rwanda;

6° **Amakosora akorwa mu mpera z'igihe cy'ibaruramari:** inyandiko zishyirwa mu gitabo mu mpera z'umwaka w'ibaruramari hagamijwe gukosora amakuru kugira ngo agaragaze ukuri ku byerekeye uko ikigo cy'imari gihagaze mu gihe gikorwaho raporo;

7° **Inyandiko zahawe itariki ya mbere y'igihe zakorewe**: Inyandiko zishyirwa mu gitabo zifitanye isano n'ibihe byabanjirije ibaruramari;

8° **Amakuru**: Amakuru ari mu buryo bw'ikoranabuhanga ashobora guhererekanywa cyangwa gutunganywa ;

9° **Gusubiza kuri zeru**: kwimurira inyandiko y'ibaruranyungu cyangwa ibaruragihombo cy'umwaka mu nyungu zitagabanywe ;

10° **Uburyo koranabuhanga bw'ibanze** : uburyo koranabuhanga butunganye bw'ikigo kigenzurwa butanga amakuru.

institution's database or system with manual intervention;

5° **Central Bank:** the National Bank of Rwanda;

6° **End of period adjustments:** journal entries made at the end of an accounting period for the adjustment of data to accurately reflect the supervised institution's financial position for the reporting period;

7° **Back-dated entries:** journal entries related to some previous accounting periods;

8° **Data**: Information in digital form that can be transmitted or processed.

9° **Zerolisation**: Transfer of current year profit or loss to retained earnings;

10° **Core IT system:** an organisational IT data production system.

ou du système d'une institution supervisée avec intervention manuelle;

5° **Banque Centrale**: la Banque Nationale du Rwanda ;

6° **Ajustements de fin de période comptable**: les écritures du journal faites à la fin d'une période comptable pour l'ajustement des données afin de refléter avec précision la situation financière de l'institution supervisée pour la période de rapport;

7° **Entrées antidatées** : Entrées du journal liées à certaines périodes comptables antérieures;

8° **Données**: Informations sous format numérique pouvant être transmises ou traitées ;

9° **Remise à zéro**: Transfert du résultat de l'exercice en cours aux bénéfices non distribués ;

10° **System d'information de technologie de base** : a système de production de données organisationnelles.

UMUTWE WA II: KUBONA AMAKURU

Ingingo ya 3: Uburyo bukurikizwa mu kugaragariza Banki Nkuru amakuru

Ibigo bigenzurwa bigomba kugeza amakuru mu Bubiko bw'Amakuru bwa Banki Nkuru bikoresheje umuyoboro njyanamakuru wikoresha (ADF) cyangwa utikoresha(N0NADF).

Ingingo ya 4: Kugaragaza amakuru

Buri kigo cyose kigenzurwa kigomba kugaragaza amakuru gisabwa mu buryo bukurikira:

1° ku makuru atangwa buri munsi arebana n'igurisha n'igura ry'amadevise, uwo munsi mbere ya saa kumi n'ebyiri z'umugoraba ;

2° ku y 'andi makuru atangwa ku munsi : ku munsi w'akazi ukurikira, mbere ya saa ine z'amanywa ;

3° ku makuru atangwa buri kwezi: atangwa mu iminsi itanu (5) y'akazi mu kwezi gukurikira ;

4° ku makuru atangwa buri gihembwe : atangwa mu iminsi itanu (5) y'akazi mu igembwe gikurikira.

CHAPTER II: DATA READINESS

Article 3: Process of availing data to the Central Bank

Supervised institutions shall avail data to the Central Bank DWH by either ADF or NONADF.

Article 4: Availability of data

Any supervised institution shall avail required data as follows:

1° for daily data related to foreign exchange for cash purchase and sales, the same day before 6:00 pm;

2° for other daily data: the next working day, before 10:pm;

3° for monthly data: Within five (5) working days of the following month;

4° for quarterly data: Within five (5) working days of the following quarter.

CHAPITRE II: MISE A DISPOSITION DE DONNEES

Article 3: Processus de mise à disposition de données à la Banque Centrale

Les institutions supervisées doivent fournir des données à l'Entrepôt de données de la Banque Centrale par l'intermédiaire du flux de données automatisé (ADF) ou du flux de données non automatisé (NONADF).

Article 4: Disponibilité des données

Toute institution supervisée doit disposer des données requises comme suit:

1° pour les données quotidiennes relatives à l'achat et vente de devises, le même jour avant 6 :00 pm ;

2° pour d'autres données quotidiennes : le jour ouvrable suivant, avant 10 : 00pm après le jour où les données ont été enregistrées dans le système;

3° Pour les données mensuelles: dans les cinq (5) jours ouvrables du mois suivant ;

4° pour les données trimestrielles : dans les cinq (5) jours ouvrables du trimestre suivant.

Ingingo ya 5: Ubwoko bw'amakuru agaragazwa n'ibigo bigenzurwa

Banki Nkuru ishyiraho amabwiriza asobanura amakuru agomba kugaragazwa n'ibigo bigenzurwa mu byiciro bitandukanye.

Article 5: Types of data to be availed by supervised institutions

The Central Bank issues a directive specifying data to be availed by supervised institutions in different domains.

Article 5: Types de données devant être utilisées par les institutions supervisées

La Banque Centrale émet des directives spécifiant les données devant être utilisées par les institutions supervisées dans différents domaines.

Ingingo ya 6: Kuva mu muyoboro njyanamakuru wikoresha (ADF) ujya mu muyoboro njyanamakuru utikoresha (NonADF)

Ikigo kigenzurwa cyifashisha umuyoboro njyanamakuru wikoresha (ADF) gishobora guhindura kigakoresha umuyoboro njyanamakuru utikoresha (NONADF) mu gihe uwo muyoboro udakora neza. Icyakora, mbere yo guhindura umuyoboro njyanamakuru cyakoreshaga, ikigo kigomba kubanza kubyemererwa na Banki Nkuru.

Article 6: Switching from ADF to NON ADF

A supervised institution using ADF may switch to NON ADF in case of system failure. However, before switching, the institution shall seek prior approval from Central Bank.

Article 6: Passage de l'ADF au NONADF

Une institution supervisée utilisant le Flux de Données Automatisé (ADF) peut passer au Flux de Données Non automatisé (NONADF) en cas de défaillance du système. Toutefois, avant de changer, l'institution doit obtenir l'approbation préalable de la Banque Centrale.

Ingingo ya 7: Gusoza Umwaka w'Ibaruramari

Buri kigo kigenzurwa kigomba kagaragaza amakuru arangiza umwaka mu Bubiko bw'Amakuru bwa Banki Nkuru mbere yo gusubiza kuri Zeru. Uko kwimura inyandiko bikorwa mbere y'uko umwaka w'ibaruramari urangira.

Article 7: Closure of Financial Year

Each supervised institution shall avail closing data entries to the Central Bank Data Warehouse before zerolisation. The later takes place at the end of the year.

Article 7: Clôture de l'Exercice Financier

Chaque institution supervisée doit disposer des données de clôture à l'Entrepôt de Données de la Banque Centrale avant la remise à zéro. Cette dernière a lieu à la fin de l'année.

Ingingo ya 8: Gusaba amakuru y'inyongera

Banki Nkuru ishobora gusaba ibigo bigenzurwa andi makuru y'inyongera akenewe kugira ngo isohoze inshingano zayo.

Article 8: Request for further information

The Central Bank may request from supervised institutions such other information as may deem necessary to achieve its mandate.

Article 8: Demande d'informations complémentaires

La Banque Centrale peut demander aux institutions supervisées toute autre information jugée nécessaire à la réalisation de son mandat.

UMUTWE WA III: AMAKURU AFITE IREME KANDI ATANGANYWE UBUSHISHOZI

Ingingo ya 9: Inkomoko y'amakuru

Ibigo bigenzurwa bitanga amakuru bikoresheje umuyoboro njyanamakuru wikoresha (ADF) agomba kuva mu buryo karanabuhanga bw'ibanze. Naho ibikoresha umuyoboro nyanamakuru utikoresha(NonADF) amakuru agomba guturuka mu ikusanyirizo ry'amakuru ritunganyije, ryagenzuwe kandi ritanga amakuru yose.

Ingingo ya 10: Kwemeza amakuru atanzwe

Banki Nkuru igena amabwiriza yerekeye umurongo ukurikizwa mu kwemeza amakuru ibigo bigenzurwa bitanga.

Ingingo ya 11: Kuba amakuru ari ukuri kandi yuzuye

Buri kigo kigenzurwa kigomba kugenzura ko amakuru yavanywe mu buryo gikoresha cyangwa yakuruwe hakoreshejwe ikoranabuhanga ari ukuri kandi yuzuye hakurikijwe imirongo ngenderwaho y'Ububiko bw'Amakuru bwo muri Banki Nkuru.

Ingingo ya 12: Guhindura amakuru

Buri kigo kigenzurwa kigomba kureba ko amakosora yakozwe mu mpera z'igihe cy'ibaruramari yashyizwe mu buryo ikigo

CHAPTER III: DATA INTEGRITY AND QUALITY

Article 9: Data Source

Supervised institutions shall ensure that data availed through ADF are from their respective IT Core system. Data availed through NON ADF are from an organized, controlled, and integrated database.

Article 10: Data Validation

The Central Bank shall issue a directive on the guidance for the processes on data validation by supervised institutions.

Article 11: Data Accuracy and Completeness

Each supervised institution shall ensure that the data extracted or uploaded from its system are accurate and completed in accordance with the Central Bank Data Warehouse guidelines.

Article 12: Data modification

Any supervised institution shall ensure that end of period adjustments are posted into its system before

CHAPITRE III: INTEGRITE ET QUALITE DES DONNEES

Article 9: Source de données

Les institutions supervisées s'assurent que les données fournies à partir du Flux de Données Automatisé (ADF) proviennent dans le system de l'information de technologie de base. Les données fournies à partir du flux de données Non-Automatisé (NONDF) doivent provenir d'une base de données organisée, contrôlée et intégrée.

Article 10: Validation des données

La Banque Centrale émet une directive sur les orientations relatives aux processus de validation des données devant être fournies par les institutions supervisée.

Article 11: Exactitude et exhaustivité des données

Chaque institution supervisée doit s'assurer que les données extraites ou téléchargées depuis son système sont exactes et complètes conformément aux directives de l'Entrepôt de Données de la Banque Centrale.

Article 12: Modification des données

Toute institution supervisée doit s'assurer que les ajustements de fin de période sont enregistrés dans son système avant de pouvoir utiliser les données

gikoresha mbere yo kuyatanga anyujijwe mu muyoboro njyanamakuru wikoresha (ADF) cyangwa utikoresha (NONADF). Icyakora, ibikorwa byahawe itariki ibanziriza igihe byakorewe ntibyemewe.

availing data through ADF or NON ADF. However, back-dated transactions are not allowed.

par l'intermédiaire du Flux de Données Automatisé (ADF) ou non automatisé (NONADF). Cependant, les transactions antidatées ne sont pas autorisées.

Ihindura iryo ari ryo ryose ry'amakuru mu buryo bw'amakosora yakozwe mu mpera z'igihe cy'ibaruramari cyangwa gukosora amakosa ayo ari yo yose agaragara mu makuru yavanywe cyangwa yakuruwe hakoreshejwe ikoranabuhanga bigomba gukorwa nyuma.

Any data modification in form of adjustment of the end period or correction of any error in data already extracted or uploaded shall be done prospectively.

Les ajustements de fin de période, toute modification ou rectification de toute erreur dans les données déjà extraites ou téléchargées doit être faite prospectivement.

Banki Nkuru itangaza amabwiriza yerekeye inama zikurikizwa mu guhindura amakuru bikozwe n'ibigo bigenzurwa.

The Central Bank shall issue a directive on the guidance for data modifications by supervised institutions.

La Banque Centrale publie une directive sur les orientations à suivre pour modifier les données transmises par les institutions supervisées.

Ingingo ya 13: Ireme ry'uburyo bukoresha ikoranabuhanga

Article 13: Soundness of ICT System

Article 13: Qualité du système des TIC

Buri kigo kigenzurwa kigomba kuba gifite uburyo bw'ikoranabuhanga bukora neza kandi bukomeye, buhuje n'ibisabwa mu itangwa ry'amakuru afite ireme kandi yakusanyijwe mu bushishozi.

Each supervised institution is required to have a sound IT system that meets the requirements for data readiness, integrity and quality.

Chaque institution supervisée doit être doté d'un système informatique fiable répondant aux exigences de mise à disposition, d'intégrité et de qualité des données.

UMUTWE WA IV: INGINGO ZISOZA

CHAPTER IV: FINAL PROVISIONS

CHAPITRE IV: DISPOSITIONS FINALES

Ingingo ya 14: Ibihano by'amafaranga

Article 14: Pecuniary sanctions

Article 14: Sanctions pécuniaires

Iyo Banki Nkuru isanze ikigo kigenzurwa cyaratanze amakuru atuzuye, arimo amakosa, abeshya cyangwa ayobya cyangwa adakurikije ingingo iyo ari yo yose iteganyijwe muri aya mabwiriza rusange, icyo gihe Banki Nkuru

Where the Central Bank determines that a supervised institution has availed incomplete, erroneous, false or misleading data or does not comply with any of the provision of this regulation,

Lorsque la Banque Centrale trouve qu'une institution supervisée a fourni des données incomplètes, erronées, fausses ou trompeuses ou qui ne sont pas conformes à l'une des dispositions

ihanisha icyo kigo ibihano by'amafaranga biteganywa mu mabwiriza.

it shall apply pecuniary sanctions defined in the directive.

du présent règlement, elle applique des sanctions pécuniaires définies dans la directive.

Ingingo ya 15: Igihe cy'inzibacyuho

Buri kigo kigenzurwa kitubahirije uko bikwiye aya mabwiriza rusange kigomba gufata ingamba za ngombwa zo kwikosora kugira ngo kibonera umuti ibyuho byagaragaye mu gihe kitarenze amezi abiri (2) uhereye igihe aya mabwiriza rusange atangarijwe.

Ikigo kigenzurwa gishyikiriza Banki Nkuru gahunda y'ikosora mu gihe kitarenze iminsi mirongo itatu (30) nyuma y'itangazwa ry'aya mabwiriza rusange.

Article 15:Transition Period

Any supervised institution, which is not in full compliance with this regulation, shall take necessary remedial measures to address identified data gaps within a period not exceeding two (2) months from the publication of this regulation.

A supervised institution must submit to the Central Bank a detailed remedial plan within a period not exceeding thirty (30) days after the publication of this Regulation.

Article 15: Période de transition

Toute institution supervisée qui ne respecte pas le présent règlement dans son intégralité, doit prendre les mesures correctives nécessaires pour combler les lacunes déjà identifiées dans un délai ne dépassant pas deux (2) mois à compter de la publication du présent règlement.

Cette institution soumet également à la Banque Centrale un plan de redressement détaillé dans un délai ne dépassant pas trente (30) jours après la publication du présent règlement.

Ingingo ya 16: Ivanwaho ry'ingingo inyuranyije n'aya mabwiriza rusange

Ingingo zose z'amabwiriza rusange yabanjirije aya kandi zinyuranye na yo, by'umwihariko Amabwiriza rusange N°03/2011 yerekeye ibisabwa mu gutanga raporo, zivanyweho.

Article 16: Repealing provisions

All prior regulatory provisions contrary to this Regulation, notably the regulation n° 03/2011 on reporting requirements are hereby repealed.

Article 16: Dispositions abrogatoires

Toutes les dispositions réglementaires antérieures contraires au présent règlement, notamment le règlement n°03/2011 relatif aux exigences de rapport, sont abrogées.

Ingingo ya 17: Itegurwa, isuzumwa n'iyemezwa ry'aya mabwiriza rusange

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

Article 17: Drafting, consideration and approval of this regulation

This Regulation was drafted, considered and approved in English.

Article 17: Initiation, examen et approbation du présent règlement

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

Ingingo ya 18: Igihe aya mabwiriza atangira gukurikizwa

Aya mabwiriza rusange atangira gukurikizwa ku munsi atangarijweho mu Igazeti ya Leta ya Repubulika y'u Rwanda.

Bikorewe i Kigali, ku wa 25/07/ 2018

(sé)
RWANGOMBWA John
Guverineri

Article 18: Commencement

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

Done at Kigali, on 25/07/2018

(sé)
RWANGOMBWA John
Governor

Article 18: Entrée en vigueur

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

Fait à Kigali, le 25/07/ 2018

(sé)
RWANGOMBWA John
Gouverneur

AMABWIRIZA RUSANGE YA BANKI NKURU Y'U RWANDA Nº 2100 /2018 - 009[614] YO KUWA 25/07/2018 YEREKEYE IMICUNGIRE Y'IBYATEZA INGORANE AMABANKI

REGULATION OF THE NATIONAL BANK OF RWANDA Nº 2100 /2018 - 009[614] OF 25/07/2018 ON RISK MANAGEMENT FOR BANKS

REGLEMENT DE LA BANQUE NATIONALE DU RWANDA Nº 2100 /2018 – 009/20[614] DU 25/07/2018 DU SUR LA GESTION DES RISQUES POUR LES BANQUES

ISHAKIRO

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza rusange agamije

Ingingo ya 2: Ibisobanuro by'amagambo

UMUTWE WA 2: GAHUNDA Y'IMICUNGIRE Y'IBYATEZA INGORANE

Ingingo ya 3: Uburyo bwo gukora imicungire y'ibyateza ingorane

Ingingo ya 4: Gahunda y'imicungire y'ibyateza ingorane

Ingingo ya 5: Gahunda n'uburyo bw'imicungire y'ibyateza ingorane

Ingingo ya 6: Imicungire y'ibyateza ingorane, Ikurikirana n'Isesengura ryerekeye Imari

Ingingo ya 7: Imicungire y'ibyateza ingorane no kugira imari hagije

TABLE OF CONTENTS

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this regulation

Article 2: Definitions

CHAPTER 2: RISK MANAGEMENT PROGRAM

Article 3: Approach to risk management

Article 4: Risk management program

Article 5: Risk management program and process

Article 6: Risk Management, Oversight and Financial Analysis

Article 7: Risk Management and Capital Adequacy

TABLE DES MATIERES

CHAPITRE PREMIER: DISPOSITIONS GENERALES

Article premier: Objet du présent règlement

Article 2: Définitions

CHAPITRE 2: PROGRAMME DE GESTION DE RISQUE

Article 3: Approche pour la gestion du risque

Article 4: Programme de gestion du risque

Article 5: Programme de gestion du risque

Article 6: Gestion de Risque, supervision et analyse financière

Article 7: Gestion du risque et adéquation du capital

Ingingo ya 8: Uburyo bukurikizwa mu byerekeye imicungire y'ibyateza ingorane	**Article 8: Risk Management Methodology**	**Article 8: Méthodologie de Gestion du Risque**
Ingingo ya 9: Ibyateza ingorane n'igenzura ry'imbere mu ikurikizwa ry'imicungire y'ibyateza ingorane	**Article 9: Internal control in the application of Risk Management**	**Article 9: Contrôle interne dans l'application de la Gestion du Risque**
Ingingo ya 10: Imicungire y'ibyateza ingorane n'Imenyekanisha	**Article 10: Risk Management and disclosure**	**Article 10: Gestion du risque et divulgation**
Ingingo ya 11: Gutanga gahunda y'imicungire y'ibyateza ingorane n'ibigenderwaho bya za komite y'Inama y'Ubutegetsi yerekeye Imicungire y'ibyateza ingorane	**Article 11: Submission of the risk management program and Terms of Reference of Board risk management Committee**	**Article 11: Transmission du programme de gestion du risque et des termes de référence du comité du Conseil d'Administration responsable de la gestion du risque**
Ingingo ya 12: Isuzumwa n'isubiramo rya gahunda y'imicungire y'ibyateza ingorane	**Article 12: Review and subsequent revision of the risk management program**	**Article 12: Examen et révision ultérieure du programme de gestion du risque**
Ingingo ya 13: Ibihano byerekeye imyitwarire n'amafaranga	**Article 13: Disciplinary and pecuniary sanctions**	**Article 13: Sanctions disciplinaires et pécuniaires**
Ingingo ya 14: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza rusange	**Article 14: Repealing of inconsistent Provisions**	**Article 14: Dispositions abrogatoire**
Ingingo ya 15: Igihe aya mabwiriza rusange atangira gukurikizwa	**Article 15: Commencement**	**Article 15: Entrée en vigueur**

AMABWIRIZA RUSANGE YA BANKI NKURU Y'U RWANDA Nº 2100 /2018 - 009[614] YO KUWA 25/07/2018 YEREKEYE IMICUNGIRE Y'IBYATEZA INGORANE AMABANKI

Ishingiye ku Itegeko n° 48/2017 ryo ku wa 23/09/2017 rigenga Banki Nkuru y'u Rwanda, cyane cyane mu ngingo zaryo iya 8 n'iya 10;

Ishingiye ku Itegeko n° 47/2017 ryo ku wa 23 /09/2017 rigena imitunganyirize y'imirimo y'amabanki, cyane cyane mu ngingo zaryo iya 63; iya 66, iya 67 n'iya 68;

Isubiye ku mabwriza rusange n° 03/2012/ yo ku wa 30/04/2012 ku micungire y'ibyateza ingorane amabanki;

Banki Nkuru y'u Rwanda, mu ngingo zikurikira yitwa "Banki Nkuru", itanze amabwiriza akurikira:

REGULATION OF THE NATIONAL BANK OF RWANDA Nº 2100 /2018 - 009[614] OF 25/07/2018 ON RISK MANAGEMENT FOR BANKS

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

Pursuant to Law n° 47/2017 of 23 /09/2017 governing the organization of banking, especially in its articles 63; 66, 67 and 68;

Having reviewed the regulation n° 03/2012/ of 30/04/2012 on Risk Management Banks;

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

REGLEMENT DE LA BANQUE NATIONALE DU RWANDA Nº 2100 /2018 - 009[614] DU 25/07/2018 DU SUR LA GESTION DES RISQUES POUR LES BANQUES

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

Vu la Loi n° 47/2017 du 23 /09/2017 portant organisation de l'activité bancaire, spécialement en ses articles 63; 66, 67 et 68;

Revu le règlement n° 03/2012/ du 30/04/2012 sur la gestion des risques pour les Banques;

La Banque Nationale du Rwanda ci-après dénommée « Banque Centrale », édicte le règlement ci-après :

UMUTWE WA MBERE: INGINGO RUSANGE

Ingingo ya mbere: Icyo aya mabwiriza rusange agamije

Aya mabwiriza agamije guteza imbere ishyirwaho ry'amahame y'imicungire y'ibyateza ingorane n'ibikurikizwa mu gushyuraho uburyo cyangwa

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this regulation

This regulation aims to promote the adoption of risk management principles and procedures to provide for an effective risk management system/

CHAPITRE PREMIER : DISPOSITIONS GENERALES

Article premier : Objet du présent règlement

Le présent règlement vise à promouvoir l'adoption des principes et procédures pour prévoir le système ou programme efficace de gestion de risque ainsi

gahunda nyayo y'imicungire y'ibyateza ingorane n'uburyo bw'igenzura ry'imbere kugira ngo amabanki ashobore kugaragaza, gupima, gukurikirana no kugenzura mu buryo nyabwo ibyateza ingorane.

program and internal control systems to enable banks to properly identify, measure, monitor and control their risk exposures.

que les systèmes de contrôle interne en vue de permettre banques d'identifier, mesurer, suivre et contrôler efficacement leurs expositions au risque.

Ingingo ya 2: Ibisobanuro by'amagambo

Article 2: Definitions

Article 2 : Définitions

1° **Ingorane ziri mu nguzanyo**: ni ibyateza ingorane biriho cyangwa bishobora kubaho ku nyungu no ku mari shingiro kubera ko uwahawe umwenda ananiwe kubahiriza ibikubiye mu masezerano na banki cyangwa uwahawe umwenda ku bundi buryo ananiwe kurangiza ibyo agomba nk'uko byumvikanweho;

1° **Credit risk**: is the current or prospective risk to earnings and capital arising from an obligor's failure to meet the terms of any contract with the bank or if an obligor otherwise fails to perform as agreed;

1° **Risque de crédit:** c'est un risque actuel ou éventuel aux profits et au capital résultant de défaut du débiteur d'honorer les termes de tout contrat conclu avec une banque ou lorsque le débiteur faillit autrement de respecter son engagement tel que convenu ;

2° **Ibyateza ingorane ku mafaranga abitse:** ni ibyateza ingorane biriho cyangwa bishobora kubaho ku nyungu no ku mari shingiro biturutse ku kuba banki nta bushobozi ifite bwo kwishyura imyenda yayo iyo igeze igihe cyo kwishyurwa itagize ibihombo bitemewe. Izo ngorane zivuka iyo igabanuka rituruka ku mitungo y'amafaranga idahagije mu kuzuza inshingano zayo.

2° **Liquidity risk:** is the current or prospective risk to earnings and capital arising from a bank's inability to meet its liabilities when they fall due without incurring unacceptable losses. It arises when the cushion provided by the liquid assets are not sufficient to meet its obligations.

2° **Risque de liquidité:** c'est un risque actuel ou éventuel aux profits et au capital résultant du défaut de la banque d'honorer ses engagements lorsque ces engagements arrivent à échéance sans encourir des pertes inacceptables. Cela arrive lorsque la diminution découle de l'insuffisance des avoirs réalisables pour remplir ses obligations.

3° **Ingorane zerekeye imiterere y'isoko**: ni ibyateza ingorane byerekeye agaciro k'imitungo ya banki iri mu ifoto y'umutungo cyangwa itari mu ifoto y'umutungo byagira

3° **Market Risk**: is the risk that the value of on and off-balance sheet positions of a bank will be adversely affected by movements in market

3° **Risque du marché:** c'est un risque dont la valeur des actifs et du passif et du hors bilan de la banque sera négativement affectée par la

ingaruka mbi bitewe n'imigendekere y'ibiciro cyangwa ibipimo ku isoko nk'ibipimo by'inyungu, ibiciro by'ivunjisha, ibiciro by'imigabane ku isoko ry'imari, imitangire y'inguzanyo n'ibiciro by'ibicuruzwa byateza igihombo ku nyungu n'imari;

4° **Ingorane ziri mu bikorwa**: ni igihombo kiziguye cyangwa kitaziguye kiba giturutse ku kuba nta mikorere y'imbere ihari cyangwa ihari ikaba idahwitse, ku bantu cyangwa iturutse ku bintu byo hanze cyangwa ku bindi biza. Gishobora guturuka ku kudakurikiza imigenzurire y'imbere mu kigo;

5° **Ingorane zijyanye n'ikoranabuhanga**: ni ibyateza igihombo byaterwa n'uko uburyo bw'amakuru budahwitse cyangwa ikoranabuhanga ridakora;

6° **Ingorane zijyanye no kudakurikiza amategeko:** ni ibyateza ingorane biriho cyangwa byabaho ku nyungu n'imari shingiro biturutse ku kutubahiriza cyangwa kudakurikiza amategeko, amabwiriza, imikorere yagenwe cyangwa ibipimo ngenderwaho by'imyitwarire byashyizweho n'utanga amabwiriza rimwe na rimwe. Ibyateza zijyanye no kutubahiriza amategeko zibaho iyo

rates or prices such as interest rates, foreign exchange rates, equity prices, credit spreads and/or commodity prices resulting in a loss to earnings and capital;

4° **Operational risk**: it is the risk of direct or indirect loss resulting from the absence or inadequacy of the internal control process, persons and systems or due to an external event or other disasters. It may result from breach of internal controls;

5° **Technology risk**: it is the risk of loss arising from the potential inadequate information system or technology failures;

6° **Legal and compliance risk**: is the current and prospective risk to earnings or capital arising from violations of, or non-conformance with laws, rules, regulations, prescribed practice, or ethical standards issued by the regulator from time to time. Regulatory risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested;

fluctuation des taux du marché ou les prix tels que le taux d'intérêt, le taux de change, les prix des capitaux propres, la répartition du crédit et ou les prix des produits résultant de la perte aux profits et au capital;

4° **Risque opérationnel** : c'est le risque de perte directe ou indirecte découlant de l'absence ou l'insuffisance des procédures de contrôle interne, des personnes et des systèmes ou qui est causé par un événement externe ou d'autres catastrophes. Il peut découler de la violation des contrôles internes;

5° **Risque de Technologie** : c'est le risque de perte découlant du système d'information potentiel insuffisant ou des défauts de technologie ;

6° **Risque juridique et de conformité :** c'est un risque actuel ou éventuel aux profits et au capital résultant des violations ou de non conformités aux lois, règles, règlements, pratique prescrite ou des normes de conduite édictées de temps en temps par le régulateur. Le risque réglementaire découle également des situations où les lois et les règles régissant certains produits de la banque ou les activités des clients de la banque peuvent être ambigües ou incertaines ;

amategeko cyangwa amabwiriza agenga ibicuruzwa bimwe cyangwa ibikorwa by'abakiliya b'ikigo bishobora kuba bidasobanutse cyangwa bitarageragejwe;

7° **"Ingorane zerekeye ingamba"**: ni ingaruka ziriho cyangwa zabaho ku nyungu cyangwa ku mari shingiro biturutse ku byemezo bibi mu mirimo, kudashyira mu bikorwa ibyemezo mu buryo nyabwo cyangwa ibura ry'ibisubizo ku mpinduka zerekeye urwego;

8° **Ingorane zerekeye igihugu**: ni ingaruka ko ibisabwa mu bukungu, imibereho myiza na politiki n'ibindi bintu bibera mu bihugu by'amahanga bizagira ingaruka mbi ku miterere y'imari y'ikigo;

9° **Ingorane zerekeye ihererekanya**: ni ingorane z'uko usaba inguzanyo ashobora kuba atabasha kubona amadevize kugira ngo yishyure imyemda yafashe mu gihugu cy'amahanga.

7° **"Strategic risk"**: is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes;

8° **Country risk**: is the risk that economic, social, and political conditions and events in a foreign country will adversely affect an institution's financial condition;

9° **Transfer risk**: is the risk that a borrower may not be able to secure foreign exchange to service its external obligations.

7° **Risque stratégique :** c'est un impact actuel ou éventuel sur les profits ou sur le capital découlant des mauvaises décisions dans les activités, de l'exécution inappropriée des décisions ou de l'absence de réactions des changements dans le secteur ;

8° **Risque de Pays**: c'est le risque que les conditions économiques, sociales et politiques et les événements présents dans un pays étranger pourront exercer un effet négatif sur la situation financière d'une institution ;

9° **Risque de transfert** : c'est le risque qu'un emprunteur pourrait ne pas être capable d'obtenir de devises pour s'acquitter de ses obligations externes.

UMUTWE WA 2: GAHUNDA Y'IMICUNGIRE Y'IBYATEZA INGORANE

Ingingo ya 3: Uburyo bwo gukora imicungire y'ibyateza ingorane

Banki igomba gushyiraho uburyo cyangwa gahunda ifatika kandi ihuriweho mu kugaragaza, gupima, gukurikirana, kugenzura no gutanga raporo ku byateza ingorane byose hakurikijwe imirongo ngenderwaho yometse kuri aya mabwiriza rusange.

Imirongo ngenderwaho yometse kuri aya mabwiriza rusange na yo ni kimwe mu bigize aya mabwiriza rusange.

Ingingo ya 4: Gahunda y'imicungire y'ibyateza ingorane

Gahunda y'imicungire y'ibyateza ingorane igomba kugira imiterere yerekeye imiyoborere irimo Komite y'Inama y'Ubutegetsi ishinzwe imicungire y'ibyateza ingorane n'umurimo w'imicungire y'ibyateza ingorane.

Komite ahanini ifite inshingano zo kwemeza ingorane za banki n'uko izazihanganira kandi ko ifite inshingano zo kugaragaza, gupima, gukurikirana, kugenzura no gutanga raporo ku gihe kandi mu buryo bukwiye ku byateza ingorane byose.

CHAPTER 2: RISK MANAGEMENT PROGRAM

Article 3: Approach to Risk Management

A Bank shall adopt a holistic and integrated approach/program for identification, measurement, monitoring, control, and reporting of all risk in accordance with the guidelines attached to this regulation.

The attached guidelines are part and parcel of this regulation.

Article 4: Risk management program

The risk management program shall have a governance structure that includes a Board risk management committee and a Risk Management function.

The committee shall be mainly responsible for approving the bank's risk appetite and risk tolerance and have responsibility for timely and adequate identification, measurement, monitoring, control and reporting of all risks.

CHAPITRE 2: PROGRAMME DE GESTION DE RISQUE

Article 3: Approche pour la gestion du risque

Une institution financière adopte une approche ou programme holistique et intégrée pour identifier, mesurer, suivre, contrôler et rapporter tous les risques conformément aux lignes directrices attachées au présent règlement.

Les lignes directrices en annexe font partie intégrante du présent règlement.

Article 4: Programme de gestion du risque

Le programme de gestion du risque doit avoir une structure de gouvernance qui comprend un Comité du Conseil d'Administration de Gestion des Risques et une fonction de gestion de risque.

Le comité est principalement chargé d'approuver l'appétit de la banque pour le risque et sa tolérance du risque et avoir la responsabilité, de façon adéquate et dans le respect du temps, d'identifier,

mesurer, faire le suivi, contrôler et rapporter tous les risques.

Kugira ngo hakurikizwe ku buryo buhamye imicungire y'ibyateza ingorane, buri banki igomba gutegura imiterere y'inzego ihuje n'intego na politiki zerekeye gukora ubucuruzi, ingano, urusobekerane n'ubushobozi bya banki.

For the purpose of effective application of risk management, each bank shall prepare an organizational structure appropriate to the objectives and business policies, size, complexity, and capability of the bank.

Aux fins de l'application efficace de la gestion du risque, chaque Banque doit préparer une structure organisationnelle appropriée aux objectifs, à la taille, à la complexité et à la capacité de la banque.

Imiterere y'inzego z'umurimo rw'imicungire y'ibyateza ingorane igomba kuba ihuje n'ingano n'urusobekerane rw'ibikorwa bya banki n'ibijyana n'ibyo bikorwa byateza ingorane banki.

The organizational structure of the Risk Management function shall be appropriate to the size and complexity of Bank operations and the inherent risks of the bank.

La structure organisationnelle de la fonction de Gestion du Risque doit être appropriée à la taille et à la complexité des opérations de la banque et des risques inhérents de la banque.

Gahunda y'imicungire y'ibyateza ingorane igomba kwerekana uburyo bwerekeye ukuntu ukuriye umurimo w'imicungire y'ibyateza ingorane agomba kuzakorana inama zitandukanye n'Inama y'Ubutegetsi cyangwa Komite y'Inama y'Ubutegetsi ishinzwe Imicungire y'Ibyateza Ingorane kugira ngo baganire ku bibazo bifitanye isano n'ibyateza banki ingorane.

The risk management program shall indicate the procedures on how the head of risk management function shall have separate meetings with the Board or the Risk Management Board Committee to discuss issues related to risks of the bank.

Le programme de gestion du risque doit indiquer la procédure à suivre quant à la façon dont le chef chargé de la fonction de la gestion du risqué tiendra des réunions séparées avec le Conseil d'Administration ou avec le Comite du Conseil d'Administration chargé de la Gestion du Risque pour débattre des questions en rapport avec les risques de la banque.

Ingingo ya 5: Gahunda n'uburyo bw'imicungire y'ibyateza ingorane

Article 5: Risk Management Program and process

Article 5: Programme et processus de gestion du risque

Gahunda ya buri kigo y'imicungire y'ibyateza ingorane igomba kuba nibura igizwe n'ibi bikurikira bigize uburyo buhamye bw'imicungire y'ibyateza ingorane:

The risk management program of each institution shall contain at least the following elements of a sound risk management system:

Le programme de gestion du risque de chaque institution contient au moins les éléments suivants qui composent un système solide de gestion du risque :

1° inama y'Ubutegetsi ry'Abayobozi Bakuru bashoboye kandi bakurikirana;

2° politiki , imirongongenderwaho n'ibipimo ntarengwa bisonutse;

3° igenzura ry'imbere rikwiye;

4° Gukurikirana bihagije ibyateza ingorane n'uburyo bukora neza bwerekeye Imicungire y'Amakuru.

Banki igomba kugira uburyo buhujwe bw'imicungire y'ibyateza ingorane mu kugaragaza, gusuzuma, gukurikirana no kugenzura cyangwa kugabanya ibyateza ingorane bifatika byose no gusuzuma ko banki ifite imari ihagije muri rusange ku birebana n'isura y'icyateza ingorane. Iyi mikorere igomba kuba iri ku kigero gihuje n'ingano n'urusobekerane by'ikigo.

Ingingo ya 6: Imicungire y'ibyateza ingorane, Ikurikirana n'Isesengura ryerekeye Imari

Gahunda y'imicungire y'ibyateza ingorane igomba kubamo uburyo bw'ikurikirana n'isensenguramari bya buri banki bigomba kugaragazwa mu rwego rw'imicungire y'ibyateza ingorane rwa banki.

1° active Board and Senior Management Oversight;

2° adequate policies procedures and limits;

3° adequate internal controls;

4° adequate risk monitoring and Management Information Systems.

A bank shall have a comprehensive risk management processes to identify, evaluate, monitor and control or mitigate all material risks and to assess its overall capital adequacy in relation to its risk profile. These processes must be commensurate with the size and complexity of the institution.

Article 6: Risk Management, Oversight and Financial Analysis

A risk management program shall include a process for each bank's oversight and financial analysis that shall be reflected within the risk management function of a bank.

1° supervision active du Conseil d'Administration et de la Direction ;

2° processus et limites des politiques adéquates ;

3° contrôles internes adéquats;

4° suivi adéquat du risque et Systèmes de Gestion des Informations.

Une banque doit disposer de processus de gestion globale du risque pour identifier, évaluer, surveiller et contrôler ou atténuer tous les risques substantiels et évaluer et son adéquation totale du capital par rapport à son profil de risque. Ces processus doivent être proportionnels à la taille et à la complexité de l'institution.

Article 6: Gestion de Risque, supervision et analyse financière

Un programme de gestion du risque inclut un processus de surveillance de chaque institution financière et l'analyse financière qui doit être reflété dans la fonction de gestion de risque d'une banque.

Ingingo ya 7: Imicungire y'ibyateza ingorane no kugira imari hagije

Banki isabwa kugira ibipimo by'imari shingiro bisabwa mu kwemererwa gukora nka banki no kugira imari iri hejuru y'ikigereranyo gito kitagibwa munsi gishyirwaho n'amategeko mu rwego rwo kubahiriza ibisabwa amabanki ku byerekeye imari shingiro.

Article 7: Risk management and capital adequacy

A bank is required to hold total capital levels in compliance with licensing requirements and hold capital above the minimum regulatory capital ratio in compliance with the Regulation on capital requirements of banks.

Article 7: Gestion du risque et adéquation du capital

Une banque est tenue d'avoir des niveaux du capital total dans le cadre de respecter les exigences d'agrément et d'avoir un capital qui est au-dessus du ratio du capital minimum réglementaire conforme aux règlements sur les exigences relatives au capital pour les banques.

Ingingo ya 8: Uburyo bukurikizwa mu byerekeye imicungire y'ibyateza ingorane

Banki ishobora gukoresha ubururyo bwihariye mu gusesengura ingorane ziri mu nguzanyo, ingorane zerekeye imiterere y'isoko, isuzuma ry'ingorane zerekeye imikorere n'uburyo bw'imari ikoreshwa.

Ibi bishobora kuba uburyo bw'icyemezo cyahawe umurongo mu igenamigambi ryerekeye imari cyangwa ikitegererezo cy'imari mu byerekeye ubukungu. Uburyo bwemejwe buterwa n'ingano, urusobekerane n'ingamba z'imirimo bya banki.

Article 8: Risk management methodology

A bank can use a specific credit risk, market risk, operational risk assessment and capital allocation methodology.

This may be judgment-oriented approach to capital planning or economic capital models. The approach taken will depend on the size, complexity, and business strategy of a bank.

Article 8: Méthodologie de Gestion du Risque

Une banque peut utiliser un risque de crédit spécifique, un risque de marché, une évaluation du risque opérationnel et une méthodologie d'allocation du capital.

Ceci peut-être une approche du jugement orienté vers la planification du capital ou des modèles de capital économique. L'approche adoptée dépendra de la taille, de la complexité et de la stratégie d'affaires d'une institution financière.

Ingingo ya 9: Igenzura ry'imbere mu kubahiriza imicungire y'ibyateza ingorane

Igenzura ry'imbere mu ikurikizwa ry'imicungire y'ibyateza ingorane igomba kwita nibura kuri ibi bikurikira:

1° kuba uburyo bw'igenzura ry'imbere bukwiriye ubwoko n'igipimo by'ingorane

Article 9: Internal control in the application of risk management

The scope of the internal control system in the application of risk management shall cover at least the following:

1° appropriateness of the internal control system to the type and level of inherent risk in the business operations of a bank;

Article 9: Contrôle interne dans l'application de la Gestion du Risque

Le champ d'application du système de contrôle interne dans l'application de la gestion des risques couvre au moins les éléments suivants:

1° l'adéquation du système de contrôle interne au type et au niveau du risque

zijyana na byo mu bikorwa by'ubucuruzi banki ikora;		inhérent aux opérations commerciales d'une banque ;
2° ishyirwaho ry'ububasha n'inshingano bigamije gukurikirana iyubahirizwa rya politiki, uburyo bukurikizwa n'ibipimo ntarengwa;	2° establishment of powers and responsibilities for monitoring of compliance with policy, procedures, and limits;	2° la mise en place des pouvoirs et des responsabilités pour le contrôle du respect de la politique, des procédures et des limites;
3° ishyirwaho ry'imirongo yo gukora raporo no gutandukanya ku buryo bugaragara inshingano hagati y'amashami ashinzwe ibikorwa n'amashami akora imirimo y'igenzura;	3° establishment of reporting lines and clear segregation of functions between operating units and units performing control functions;	3° la mise en place de lignes hiérarchiques et la séparation claire des fonctions entre les unités opérationnelles et les unités exerçant des fonctions de contrôle;
4° imiterere y'inzego isobanura ku buryo bugaragara ibikorwa by'ubucuruzi bya Banki;	4° organizational structure that clearly depicts the business activities of a Bank;	4° une structure organisationnelle qui décrit clairement les activités commerciales d'une Banque;
5° kuba hari uburyo bukurikizwa buhagije bwo kugenzura ko Banki yubahiriza amategeko n'amabwiriza rusange biriho;	5° adequacy of procedures to ensure the compliance of the Bank with prevailing laws and regulations;	5° L'adéquation des procédures pour assurer la conformité de la Banque avec les lois et règlements en vigueur;
6° isuzuma rihamye, ryigenga kandi rikozwe nta marangamutima ry'uburyo bukurikizwa mu isesengura ry'ibikorwa bya banki;	6° effective, independent, and objective review of the procedures for assessment of bank operations;	6° Un examen efficace, indépendant et objectif des procédures d'évaluation des opérations de la banque;
Nubwo umurongo w'imicungire y'imirimo uzakomeza kugira inshingano z'igenzura ry'imbere, Inama y'Ubutegetsi igomba kureba ko inzego zifite uburyo bw'igenzura bukora bushobora guha agaciro ingufu z'igenzura ry'imbere kandi iri genzura rikaba rikwiye ku mimerere n'ingano y'imirimo y'amabanki.	Although business line management remain responsible for internal controls, the Board of Directors has to ensure that their organization has an effective audit process that can validate the strength of internal controls and that these controls are adequate for the nature and scope of a bank business.	Bien que la ligne de gestion d'activité reste responsable des contrôles internes, le Conseil d'Administration doit s'assurer que leur organisation dispose d'un processus d'audit efficace qui peut valider la solidité des contrôles internes et que ces contrôles sont adéquats pour la nature et la portée d'activité de la banque.

Ubwiza bw'uburyo bw'igenzura ku nzego zose za banki bugomba kugaragaza ibipimo ngenderwaho byashyizweho n'imiterere n'umurimo w'igenzura ry'imbere bikora koko.

Urwego rw'igenzura ry'imbere rusuzuma imirongo n'ibikurikizwa byemejwe n'Inama y'Ubutegetsi bishyirwa mu bikorwa mu buryo bukwiye kandi nyabwo, ko hagaragazwa ibyateza ingorane mu mikorere y'imbere, ko hakomezwa gutandukanya inshingano, ko hirindwa ingongana ry'inyungu, ko harebwa ikurikizwa ry'inzitizi rusange n'izihariye ku byateza ingorane, ko hakurikiranwa ibyerekeye inzitizi zitubahirizwa, ko hashimangirwa uburyo bwizewe bw'amakuru mu mabanki no guteza imbere ikurikirana, igenzura n'umuco wo gutanga raporo ku gihe muri banki.

<u>Ingingo ya 10</u>: **Imicungire y'ibyateza ingorane n'Imenyekanisha**

Ibyateza ingorane byose bikomeye (ku ifoto y'umutungo no hanze y'ifoto y'umutungo) bigomba kumenyekanishwa hagaragazwa ingaruka zabyo ku miterere y'imari no ku musaruro, ku mutungo w'amafaranga, n'inyungu zishoboka. Iri menyekanisha rigomba gukorwa mu buryo bugaragaza ubwiza n'ingano no kwerekana uburyo ibyateza ingorane bigiye gucungwa nk'uko bikubiye mu mirongo ngenderwaho yometse kuri aya mabwiriza rusange.

The quality of the control processes at all bank levels shall reflect standards set by an effective internal audit function and system.

The internal control function ensures proper and adequate implementation of the Board approved policies and procedures, identification of risks in the internal processes, maintaining segregation of duties, avoiding conflicts of interests, ensuring compliance with general and specific risk limits, follow-up non-compliance with limits, emphasize reliable information systems in banks and to promote monitoring, control and timely reporting culture in a bank.

<u>Article 10</u>: **Risk Management and disclosure**

All significant risk exposures (on balance sheet and off balance sheet) shall be disclosed, reflecting their impact on the financial condition and performance, cash flows, and earnings potential. These disclosures shall be qualitative and quantitative and show how risks are being managed as detailed in the guidelines attached to this regulation.

La qualité des processus de contrôle à tous les niveaux de la banque doit refléter les normes établies par la fonction et le système d'audit interne efficace.

Il garantit l'exécution correcte et adéquate des politiques et procédures approuvées par le Conseil d'Administration, identifier les risques dans les processus internes, maintenir la séparation des fonctions, éviter les conflits d'intérêts, assurer la conformité avec les limites générales et spécifiques de risques , suivre le non-respect des limites, focaliser sur les systèmes d'informations fiables au sein des banques et promouvoir la surveillance, contrôler et avoir une culture de faire des rapports à temps au sein d'une banque.

<u>Article 10</u>: **Gestion du risque et divulgation**

Tous les risques importants (sur le bilan et hors bilan) doivent être communiqués en reflétant leur impact sur la situation financière et la performance, la trésorerie et les revenus potentiels. Ces divulgations doivent être qualitatives et quantitatives et doivent montrer comment les risques sont gérés comme prévu dans les lignes directives annexes au présent règlement.

Ingingo ya 11: Gutanga gahunda y'imicungire y'ibyateza ingorane n'ibigenderwaho bya za komite y'Inama y'Ubutegetsi yerekeye Imicungire y'ibyateza ingorane

Banki isabwa kohererereza Banki Nkuru mbere y'ukwezi kwa Werurwe k'umwaka ukurikiyeho, kopi ya gahunda yayo y'imicungire y'ibyateza ingorane yuzuye, harimo ibyagenderaho by'abagize komite y'imicungire y'ibyateza ingorane n'abashinzwe imicungire y'ibyateza ingorane.

Article 11: Submission of the risk management program and Terms of Reference of Board risk management Committee

The bank is required to submit a copy of its complete risk management program, including the terms of reference of the members of the risk management committee and the risk managers, to the Central Bank before March of the following calendar year.

Article 11: Transmission du programme de gestion du risque et des termes de référence du comité du Conseil d'Administration responsable de la gestion du risque

La banque est tenue de présenter une copie complète de son programme de gestion du risque, y compris les termes de référence des membres du comité de gestion du risque ainsi que des gestionnaires du risque, à la Banque Centrale avant le mois de Mars de l'année civile suivante.

Ingingo ya 12: Isuzumwa n'isubiramo rya gahunda y'imicungire y'ibyateza ingorane

Banki Nkuru ikora isuzuma rya gahunda y'imicungire y'ibyateza ingorane ya buri kigo cy'imari kandi n'ihindurwa ryose rya gahunda rikozwe na buri kigo cy'imari rizongera ritangwe muri Banki Nkuru mu minsi cumi nitanu (15) nyuma yo kwemezwa.

Article 12: Review and subsequent revision of the risk management program

The Central Bank performs a review of the risk management program of each bank and any revision of the program by each bank shall be resubmitted to the National Bank of Rwanda within fifteen (15) days after its approval.

Article 12: Examen et révision ultérieure du programme de gestion du risque

La Banque Centrale effectue un examen du programme de gestion du risque de chaque banque et tout examen du programme de chaque banque sera de nouveau soumis à la Banque Centrale endéans quinze (15) jours après son approbation.

Ingingo ya 13: Ibihano byerekeye imyitwarire n'amafaranga

Iyo Banki Nkuru isanze Banki itubahiriza aya mabwiriza rusange, ishobora gufata ibihano byo mu rwego rw'ubutegetsi n'amafaranga biteganywa

Article 13: Disciplinary and pecuniary

Where the Central Bank determines that a bank does not comply with this regulation, it may invoke any or all Admistrative and pecuniary

Article 13: Sanctions disciplinaires et pécuniaires

Lorsque la Banque Centrale constate qu'une Banque ne respecte pas ces règlements, elle peut imposer tout ou partie des sanctions administrative

mu mabwiriza yerekeye ibihano byo mu rwego rw'ubutegetsi n'amafaranga.

Ishobora kandi gushyira mu bikorwa ibihano by'amafaranga n'ibyo mu rwego rw'ubutegetsi nk'uko bisobanuwe mu mabwiriza rusange yerekeye ibihano by'amafaranga bihabwa Amabanki.

Ingingo ya 14: Ivanwaho ry'ingingo zinyuranyije n'aya mabwiriza rusange

Amabwiriza rusange Nº 03/2012 yo kuwa 30/04/2012 ku micungire y'ibyateza ingorane n'izindi ngingo zose z'amabwiriza abanziriza aya kandi zinyuranye na yo, zivanyweho.

Ingingo ya 15: Igihe aya mabwiriza rusange atangira gukurikizwa

Aya mabwiriza rusange atangira gukurikizwa ku munsi atangarijweho mu Igazeti ya Leta ya Repubulika y'u Rwanda.

Bikorewe i Kigali, ku wa 25/07/2018

(sé)
RWANGOMBWA John
Guverineri

sanctions specified in the regulation on administrative and pecuniary sanctions.

It may also apply administrative and pecuniary sanctions as specified in the regulation on administrative and pecuniary sanctions applicable to Banks.

Article 14: Repealing of inconsistent Provisions

The Regulation Nº 03/2012/ of 30/04/2012 on risk management and all prior provisions contrary to this regulation are hereby repealed.

Article 15: Commencement

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

Done at Kigali, on 25/07/2018

(sé)
RWANGOMBWA John
Governor

prévues dans le règlement relatif aux sanctions administrative et pécuniaire.

Elle peut également appliquer des sanctions pécuniaires telle que prévues dans le règlement sur les sanctions pécuniaires applicables aux Banques.

Article 14: Dispositions abrogatoire

Le règlement Nº 03/2012 du 30/04/2012 sur la gestion du risque et toutes les dispositions antérieures contraires au présent règlement sont abrogées.

Article 15: Entrée en vigueur

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

Fait à Kigali, le 25/07/2018

(sé)
RWANGOMBWA John
Gouverneur

APPENDIX- RISK MANAGEMENT GUIDELINES

1. INTRODUCTION

Banks deal with various risks in managing their business. In general, a bank's profits are a function of the risks it accepts.

Risk is the probability of an expected or unexpected event having an impact on the financial situation of the institution (in terms of its capital or profits).

Since decisions are made on a continuous basis, executives of banks must make sure that the risks engaged are covered.

Risks are well managed when they are defined, quantified and controlled by an appropriate management system.

The management of banks shall therefore attach great importance to strengthening their capacity to identify, assess, monitor and control all levels of risk.

These guidelines proposed by the National Bank of Rwanda offer guidance to all banks on the risk management system they shall implement.

The guidelines point to the minimum features of a risk management program. They are mainly based on internationally accepted risk management principles and best practices and cover the main risks faced by banks: credit risk, interest rate risk, foreign exchange risk, operational risk, liquidity risk, strategic risk, reputational risk and legal and compliance risk.

The National Bank of Rwanda (BNR) has the statutory obligation to supervise banks under its jurisdiction in order to preserve public confidence in the Rwandan financial system by enabling banks to avoid excessive risks.

To perform this mission, the National Bank of Rwanda uses two supervisory methods: continuous or off-site supervision and on-site supervision.

Off-site supervision is intended to identify financial problems before they are detected by on-site supervision. It is done on the basis of various and periodic reports that the BNR receives from Banks. Quicker identification of problems makes it possible to take actions to slow the deterioration of the financial situation of banks and limit losses that depositors might potentially incur.

On-site supervision is conducted at the bank and makes it possible to review certain aspects of the bank that can be evaluated from a distance.
Preparation of these risk management guidelines also reflects the decision by the National Bank of Rwanda to move from the traditional supervisory approach to a risk-based approach.

Such an approach involves making sure that all banks have a comprehensive risk management process (including monitoring approved by the Board of Directors and general management) to identify, measure, monitor and control all essential risks and where appropriate, to create equity coverage to cover these risks.

Where the risks taken by the bank are not properly managed, the National Bank of Rwanda will be required to take the appropriate corrective measures, including reducing risk exposure, increasing capital, strengthening the risk management process and any other appropriate measures.

2. RISK MANAGEMENT PROGRAM

No single risk management system can cover all banks. For that reason, the National Bank of Rwanda asks each bank to develop its own risk management program, focused on its own needs and its risk profile.

The choice of the objectives and strategies of banks is closely linked to the specific risk decisions that banks are ready to make and the methods that will be used to manage and mitigate these risks.

The types of risk assumed and the relative size of each type of risk in the risk management program of a given bank vary according to the make-up of its activities and its risk tolerance. Risk management is based, at least in part, on an understanding of the quality of the asset and the nature of the liability associated with it.

Risk management systems and practices vary according to the scope and size of the institution and the nature of its risk exposure. But whatever approach is adopted, each institution shall have integrated policies that, when viewed as a whole, cover all its significant activities and a corporate philosophy on risk management that details the institution's risk tolerance, risk management objectives, delegation of powers and responsibilities and the process for identifying, assessing, monitoring and controlling risk.

This process must be adapted to the specific nature of the institution. It may, for example, present different degrees of centralization or decentralization and be organized in various ways while allowing the Board and senior management to perform their responsibilities throughout the organization. Completeness is a key attribute of effective risk management.

Risks can result from a commitment made directly or through subsidiaries or affiliates. In both cases, the bank must be able to detect all the material risks to which it is exposed, evaluate their potential repercussions and introduce policies and procedures to manage them effectively.

They shall periodically review these policies and procedures to maintain their relevance in the light of their actual effectiveness and any changes in the situation. Like senior management, the Board of Directors must make sure that such reviews are made.

3. COMPONENTS OF A SOLID RISK MANAGEMENT SYSTEM

A risk management program in each bank shall contain the following components:

- **Active Board of Directors and senior management:**

The Board of Directors has the ultimate responsibility for the risk assumed by the institutions. As a result, it shall approve all of the bank's business strategies and major policies, including those regarding risk management and risk assumption.

It shall also make sure that senior management has the skills to manage all the bank's activities. All directors are responsible for understanding the nature of the institution's main risks. They must make sure that the management team takes steps to identify measure, control and monitor its risks.

The level of professional knowledge of the directors will vary from bank to bank but it is nevertheless important for the directors to have a good understanding of various types of risks to which the bank is exposed and receive regular reports on how risks are managed.

Senior management is responsible for instituting strategies that reflect the associated limits.
Each bank shall produce a series of management reports and reports to the Board of Directors to reinforce the risk control activities. These reports can include a daily or weekly balance and income statements, a watch list for overdue loans, reports on overdrafts, and rates or other reports.

Banks are thus asked to have risk control and information management systems that can inform senior management and the Board of Directors of the overall risk exposure.

- **Adequate internal control:**

Internal control includes the policies, processes, culture, tasks and other aspects of an institution that support the achievement of its objectives.

These elements add to the effectiveness of activities, allow effective risk management, help ensure respect for applicable laws and regulations and enhance the ability to react appropriately to business opportunities.

- **Adequate policies, procedures and limits:**

The Board of Directors and senior management shall match risk management policies procedures to the types of risk detected by the institution's activities, once the risks have been clearly identified.

The bank's policies and procedures shall describe in detail the established path to follow in order to build on the institution's business plan and indicate the limits necessary to avoid any excessive or imprudent risks.

Once banks have policies and procedures that reflect their activities and risks, the coverage and level of detail proposed in these guidelines will necessarily vary from bank to bank. Management must make sure that its policies and procedures respond to the bank's concerns regarding risk management and are reviewed when necessary to respond to major changes in bank activities.

- **Adequate risk identification, assessment, control and monitoring and information system management:**

Risk control requires each institution to identify and assess any risk exposure. Accordingly, risk control activities must be supported by information systems that provide senior management and the Board of Directors with regular reports on the financial situation, performance of operations and risk exposure.

4. RISK MANAGEMENT PROCESSES FOR INDIVIDUAL RISKS

4.1 CREDIT RISK MANAGEMENT

4.1.1 Purpose

These guidelines state the policies and basic procedures that each bank must include in its credit risk management program, as well as the basic criteria it must adopt to manage prudently
and to monitor its portfolio and credit risk.

Experience shows that the adoption of sound lending policies and procedures is associated with financial solidity. That is why violations of these policies or procedures by banks so often result in weakening them. The main risk associated with weakening the loan portfolio is inadequacy of capital or liquidity.

For most banks, providing credit through lending operations or investment constitutes a major element of their business. The quality of the credit portfolio of a bank is thus a risk element assumed by its underwriters and shareholders. Credit risk management is necessarily part of an overall business plan.

Although these guidelines involve mainly the responsibility of each bank regarding the management and control of its investment and loan portfolio and the associated credit risk, it is impossible to disassociate the management of credit risk from other aspects, such as asset-liability management and the necessity for preserving sufficient liquidity and capital.

The effective management of credit risk is a critical component of a comprehensive approach to risk management and essential to the long- term success of any banking organization.
Banks need to manage the credit risk inherent in the entire portfolio as well as the risk in individual credits or transactions.

For most banks, loans are the largest and most obvious source of credit risk; however, other sources of credit risk exist throughout the activities of a bank, including in the banking book and in the trading book, and both on and off the balance sheet. Banks are increasingly facing credit risk in various financial instruments other than loans, including acceptances, interbank transactions, trade financing, foreign exchange transactions, financial futures, swaps, bonds, equities, options, and in the extension of commitments and guarantees, and the settlement of transactions.

Banks should also consider the relationships between credit risk and other risks.

4.1.2 Definitions

Within the framework of lending and investment operations of a bank, credit is defined as any asset or off balance sheet item which contains credit risk, such as loans, overdrafts, advances, finance leases, acceptances, bills discounted, guarantees and other assets or contingencies connected with credit risk.

The credit can be granted, with or without collateral, in the form of mortgage loans, bonds, private placements, derivatives and leasing contracts.

The credit risk is the risk of financial loss, despite realization of the main or secondary collateral, because of a debtor's inability to satisfy his obligations to a bank.

Credit risk management is the way to contain the repercussions for the bank of events associated with this risk. It consists of identifying, understanding and assessing the risk of losses and taking the appropriate steps for mitigation.

4.1.3 Credit risk management program

For a bank, credit risk management is a fundamental element of sound and prudent management. It requires the preparation of guidelines and relevant policies and procedures in order to prudently management the risk-return ratio from various aspects, such as quality, concentration, currencies, maturities, primary or secondary collateral and the type of credit facilities.

In developing its credit risk management program, it is vital that a bank take into account the extent to which the credit risk in any part of its operations could affect the whole enterprise.
Credit risk management will vary from bank to bank
However, a full credit risk management program
must provide:

- identification of the credit risks to which the bank is or could be exposed, (on or off the balance sheet) as part of its lending and investment operations, as well as the development and implementation of sound and prudent policies intended to efficiently manage and control these risks;

- the development and implementation of effective loan granting, document preparation and collection procedures;

- the development and implementation of complete procedures for monitoring and controlling the nature, characteristics and quality of the loan portfolio;

- the development of methods for managing problem accounts.

It is important to always respect the standards for credit risk management, despite pressures to increase profitability, marketing requirements and the existence of a much more complex financial community.

4.1.4. Policies, Procedures, and Establishment of Limits

In addition to requirements set by the National Bank of Rwanda, a Bank shall observe internal policy, procedures and set limits.

Establishment of sound and well-defined policies, procedures and limits is vital in the management of credit risk. These must be well documented, duly approved by the board and strictly implemented by management. Credit policies establish the framework for lending and guide the credit-granting activities of the institution.

1. Policies relating to limits

Credit concentration can exist when the portfolio of a bank is exposed, among others, to a risk from:

- an independent party or a group of related parties;
- groups linked to the bank (staff, shareholders, directors);
- a sector of economic activity;
- a category of primary or secondary collateral;
- a given region.

Apart from the regulatory limits, to ensure that its credit portfolio is not excessively exposed to credit concentration, banks must set its credit risk limits as a function of its exposure to such concentration. An effective credit policy should outline the following:

- Defines the credit concentrations, limits and exposures the organization is willing to assume. These limits will ensure that credit activities are adequately diversified. The policy on large exposures should be well documented to enable banks to take adequate measures to ensure concentration risk is mitigated. The policy will stipulate clearly the percentage of the bank's capital and reserves that the institution can grant as loans or extend as other credit facilities to any individual entity or related group of entities.

- In the exposure limit, contingent liabilities should be included – for example guarantees, acceptances and letters of credit. In the case of large exposures, banks must pay attention to the completeness and adequacy of information about the debtor. Credit staff should ensure they monitor events affecting large debtors and their performance on an on-going basis. Where external events present a cause for concern, credit officers should request for additional information from the debtor. If there are signs that the debtor might have difficulties in meeting its obligations to the bank, the

concerns should be raised with the credit management and a contingency plan developed to address the issues.

- The policy should require that the board approve all loans to related or connected parties. These credits should be based on market terms and should not be more favourable with regard to amount, maturity, rate and collateral than those provided to other customers.

- On exposure limits the policies should include the following:
  - Acceptable exposure to individual borrowers.
  - Maximum exposure to related parties and insider dealings.
  - The total overall limit on the credit portfolio in relation to capital, assets or liabilities.
  - Limits in relation to geographical location.
  - Maximum exposure to individual economic sectors (for example commercial, consumer, real estate, agricultural).
  - Acceptable limits on specific products.

Banks should ensure that their own internal exposure limits comply with any requirement made by the National Bank of Rwanda under the Banking Law. In order to be effective, credit policies must be communicated throughout the organization, implemented through appropriate procedures, and periodically revised to take into account changing internal and external circumstances.

2. Policies relating to segregation of Duties

Credit policy formulation, credit limit setting, monitoring of credit exposures and review and monitoring of documentation are functions that should be performed independent of the loan origination function. For small banks, where it might not be feasible to establish such structural hierarchy, there should be adequate compensating measures to maintain credit discipline, introduce adequate checks and balances and standards to address potential conflicts of interest.

3. Policies relating to credit products

The various types of loan products and credit instruments the institution intends to offer should be documented. Management must have a good understanding of all the products on offer and a careful review of the existing and potential risks must be undertaken. The products should also have a maturity profile and the pricing of these products should be included and periodically reviewed. Any new products should be fully researched and prior board approval obtained before introduction to the customers.

Credit exposure for all off balance sheet commitments should be well documented. These main off balance sheet items include letters of credit, guarantees, futures, options, swaps etc.

The policy will stipulate the credit risk analysis procedures and the administration of these credit instruments. The key objective of the review is to assess the ability of the client to meet particular financial commitments in a timely manner.

4. Policies relating to credit assessment and granting process

Banks must operate under sound, well-defined credit-granting criteria. These criteria should include a thorough understanding of the borrower or counterparty, as well as the purpose and structure of the credit, and its source of repayment.

Banks must receive sufficient information to enable a comprehensive assessment of the true risk profile of the borrower or counterparty. At a minimum, the factors to be considered and documented in approving credits must include:

- the purpose of the credit and source of repayment;
- the integrity and reputation of the borrower or counterparty;
- the current risk profile (including the nature and aggregate amounts of risks) of the borrower or counterparty and its sensitivity to economic and market developments;
- the borrower's repayment history and current capacity to repay, based on historical financial trends and cash flow projections;
- The borrower credit rating/report from licensed Credit Reference Bureau;
- a forward-looking analysis of the capacity to repay based on various scenarios;
- the legal capacity of the borrower or counterparty to assume the liability;
- for commercial credits, the borrower's business expertise and the status of the borrower's economic sector and its position within that sector;
- the proposed terms and conditions of the credit, including covenants designed to limit changes in the future risk profile of the borrower; and
- where applicable, the adequacy and enforceability of collateral or guarantees, including under various scenarios.

Also lending authority delegated to staff with clearly established limits should be documented. It is important to include the functions and reporting procedures of the various committees and individual lending officers.

In addition, it is important to have checks and balances in places that ensure credit is granted on arms-length basis. Extensions of credit to directors, senior management and other influential parties, for example shareholders, should not override the established credit granting and monitoring processes of the bank.

5. Credit risk mitigation techniques

Institutions use various techniques of mitigating credit risk. The most common are collateral, guarantees and netting off of loans against deposits of the same counter-party. While the use of these techniques will reduce or transfer credit risk, other risks may arise which include legal, operational, liquidity and market risks. Therefore there is a need for a bank to have stringent procedures and processes to control these risks and have them well documented in the policies. At present, in this jurisdiction, the common credit risk mitigation technique used is collateral.

A collateralized transaction is one in which institutions have a credit exposure or potential credit exposure and the exposure is reduced in whole or in part by collateral. The following is essential:

- There must be legal certainty. All documentation used for collateralized transactions must be binding to all parties and also be legally enforceable;
- The legal environment must provide for right of liquidation or right of possession in a timely manner in the event of default;
- Necessary steps must be taken for obtaining and maintaining an enforceable security, for example registration, right of set-off or transfer of title must meet all the legal requirements;
- Procedures for timely liquidation of collateral should be in place;
- Ongoing valuations of the collateral should be undertaken to confirm that it remains realizable;
- Guidance on the various acceptable forms of collateral should be documented.

The institution should primarily assess the borrower's capacity to repay and should not use collateral to compensate for insufficient information.

6. Internal Risk Rating Systems

An important tool in monitoring the quality of individual credits, as well as the total portfolio, is the use of an internal risk rating system. A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a banking institution. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits and the adequacy of loan loss reserves. In determining loan loss reserves, banks should ensure that the National Bank of Rwanda classification criteria are the minimum.

Typically, an internal risk rating system categorizes credits into various classes designed to take into account the gradations in risk. Simpler systems might be based on several categories ranging from satisfactory to unsatisfactory; however, more meaningful systems will have numerous ratings for credits considered satisfactory in order to truly differentiate the relative credit risk they pose.

While developing their systems, banks must decide whether to rate the riskiness of the borrower or counterparty, the risks associated with a specific transaction, or both. Internal risk ratings are an important tool in monitoring and controlling credit risk. In order to facilitate early identification, institution's internal risk rating system should be responsive to indicators of potential or actual deterioration in credit risk e.g. financial position and business condition of the borrower, conduct of the borrower's accounts, adherence to loan covenants and value of collateral.

Credits with deteriorating ratings should be subject to additional oversight and monitoring, for example, through more frequent visits from credit officers and inclusion on a watch list that is regularly reviewed by senior management. The internal risk ratings can be used by line management in different departments to track the current characteristics of the credit portfolio and help determine necessary changes to the credit strategy. Consequently, it is important that the board of directors and senior management also receive periodic reports on the condition of the credit portfolios based on such ratings.

The ratings assigned to individual borrowers or counterparties at the time the credit is granted must be reviewed on a periodic basis and individual credits should be assigned a new rating when conditions either improve or deteriorate. Because of the importance of ensuring that internal ratings are consistent and accurately reflect the quality of individual credits, responsibility for setting or confirming such ratings should rest with a credit review function independent of that which originated the credit concerned. It is also important that the consistency and accuracy of ratings is examined periodically by a function such as an independent credit review group.

7. Policies on Management of problem credits

The credit policy should establish the procedures for dealing with deteriorating and managing problem credits. Early recognition of weaknesses in the credit portfolio is important and allows alternative action and for an effective determination of loan loss potential.

An institution must have clearly articulated and documented policies in respect of the counting of days past due. In particular, policies should cover granting extensions, deferrals, renewals and additional credits to existing accounts. At a minimum, it must have approval levels and reporting requirements in respect of the above.
The policy should define a follow-up procedure for all loans and the various reports to be submitted both to management and board of directors. It should also include the internal rating for loan classification and provisioning.

8. Policies on Inter-bank transactions

Inter-bank transactions also portend significant credit risk. These transactions are essentially for facilitation of fund transfers, settlement of securities transactions or because certain services are more economically

performed by other banks due to their size or geographical location. An institution's lending policy should typically focus on the following:

- The establishment and observation of counter party credit limits;
- Any inter-bank transaction for which specific provisions should be made;
- The method and accuracy of reconciliation of the nostro and vostro accounts;
- Any inter-bank credit with terms of pricing that is not a market norm;
- The concentration of inter–bank exposure with a detailed listing of banks and amounts outstanding as well as lending limits.

9. Provisioning policy

The credit policy must clearly outline the provisioning procedures for all credits and the capital charge to be held. This should comply at a minimum to the International Accounting Standards, regulatory requirements and provisioning guidelines already issued by the National Bank of Rwanda.

4.1.5 Measuring and Monitoring Credit Risk

1. Measuring Credit risk

An institution should have procedures for measuring its overall exposure to credit risk as well as exposure to connected groups, products, customers, market segments and industries for appropriate risk management decisions to be made.

Internationally, the direction has been for institutions to put in place stringent internal systems and models, which allow them to effectively measure credit risk. This risk measurement system assists institutions to make provisions for credit risk and assign adequate capital. The effectiveness of the institution's credit risk measurement process is dependent on the quality of management information systems and the underlying assumptions supporting the models. The quality, detail and timeliness of the information is of paramount importance in determining the effectiveness of the credit risk management.

The measurement of the risk should take into account the nature of the credit, maturity, exposure, profile, existence of collateral or guarantees and potential for default. The institution should also undertake an analysis of the whole economy or in particular sectors to ensure contingency plans are developed for higher than expected levels of delinquencies and defaults.

An important tool in monitoring the quality of individual credits, as well as the total portfolio, is the use of an internal risk rating system. A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a bank. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits, and the adequacy of loan loss reserves. More detailed and sophisticated internal risk rating systems, used primarily at larger banks, can also be used to determine internal capital allocation, pricing of credits, and profitability of transactions and relationships.

Typically, an internal risk rating system categorizes credits into various classes designed to take into account the graduations in risk. Simpler systems might be based on five categories which include Normal, Watch, Substandard, Doubtful and Loss; however, more detailed systems with numerous ratings for credits may be considered.

2. Monitoring Credit Risk

An institution should have in place a system for monitoring the condition of individual credits. Key indicators of credit condition should be specified and monitored to identify and report potential problem credits. These would include indicators from the following areas:

Financial Position and Business Conditions

Key financial performance indicators on profitability, equity, leverage and liquidity should be analyzed as well as the operating environment of the obligor. When monitoring companies dependent on key management personnel or shareholders, such as small and medium enterprises, an institution should pay particular attention to assessing the status of these parties.

Conduct of Accounts

An institution should monitor the borrower's principal and interest repayments, account activity, as well as instances of excesses over credit limits.

Loan Covenants

The borrower's ability to adhere to pledges and financial covenants stated in the loan agreement should be assessed and breaches detected should trigger prompt action.

Status and Valuation of Collateral

The value of collateral should be updated periodically to account for changes in market conditions. For example, where the collateral is property or shares, an institution should undertake more frequent valuations in adverse market conditions. If the facility is backed by an inventory or goods purportedly on the obligor's premises, appropriate inspections should be conducted to verify the existence and valuation of the collateral.

External Rating and Market Price

Changes in an obligor's external credit rating and market prices of its debt or equity issues could indicate potential credit concerns.

Force Majeure Situation

The institution should consider any unforeseen circumstances that have come into play which might affect the borrower's ability to repay a facility.

In addition to monitoring the above risk indicators, an institution should also monitor the use of funds to determine whether credit facilities are drawn down for their intended purposes. Where a borrower has utilised funds for purposes not shown in the original proposal, the institution should determine the implications on the creditworthiness of the obligor. Exceptions noted during the monitoring process should be promptly acted upon and reported to management.

3. Credit administration

Credit administration is critical in ensuring the soundness of the credit portfolio. It is the responsibility of management to set up a credit administration team to ensure that once a credit is granted it is properly maintained and administered. This will include record keeping, preparation of the terms and conditions as well as perfection and safe custody of the securities. Credit files of banks should contain the following information:

- Credit application;
- Evidence of approval;
- Latest financial information;
- Record and date of all credit reviews;

- Record of all guarantees and securities;
- Record of terms and conditions of facility;
- Evidence of securities validation function that should include legal validity, existence, valuation, registration of charge and safekeeping;
- Internal rating.

While developing the credit administration process, banks should develop controls to ensure compliance with the applicable laws and regulations and internal policy. Adequate segregation of duties between approval and administration process should be maintained.

Ongoing administration of the credit portfolio is an essential part of the credit process. The credit administration function is basically a back office activity that supports and control extension and maintenance of credit. A typical credit administration unit performs the following functions:

a) Documentation - It is the responsibility of credit administration to ensure completeness of documentation (loan agreements, guarantees, transfer of title of collaterals etc) in accordance with approved terms and conditions. Outstanding documents should be tracked and followed up to ensure execution and receipt;

b) Credit Disbursement - The credit administration function should ensure that the loan application has proper approval before entering facility limits into computer systems. Disbursement should be effected only after completion of covenants, and receipt of collateral holdings. In case of exceptions necessary approval should be obtained from competent authorities;

c) Credit monitoring - After the loan is approved and draw down allowed, the loan should be continuously monitored. These include keeping track of borrowers' compliance with credit terms, identifying early signs of irregularity, conducting periodic valuation of collateral and monitoring timely repayments;

d) Loan Repayment - The obligors should be communicated to ahead of time as and when the principal/markup installment becomes due. Any exceptions such as non-payment or late payment should be tagged and communicated to the management. Proper records and updates should also be made after receipt;

e) Maintenance of Credit Files - banks should devise procedural guidelines and standards for maintenance of credit files. The credit files should not only include all correspondence with the borrower but should also contain sufficient information necessary to assess the financial health of the borrower and its repayment performance;

f) Collateral and Security Documents - banks should ensure that all security documents are kept in a fireproof safe under dual control. Registers for documents should be maintained to keep track of their movement.

Procedures should also be established to track and review relevant insurance coverage for certain facilities/collateral. Physical checks on security documents should be conducted on a regular basis.

While in small banks, it may not be cost effective to institute a separate credit administrative set-up, it is important that in such institutions individuals performing sensitive functions such as custody of key documents, wiring out funds, entering limits into system, should report to managers who are independent of business origination and credit approval process.

4. Credit exposure and risk reporting

Credit risk information should be provided to the board and management with sufficient frequency, timelines and should be reliable. Reports should be generated on the credit activities both on and off balance sheet for example:

- Credit exposures by business line such as commercial, industrial sector, real estate, construction, credit cards, mortgage and leasing;

- Credit exposures relating to the composition of on and off balance sheet credits by major types of counterparties, including government, foreign corporate, domestic corporate, consumer and other financial institutions;

- Significant credit exposure in relation to individual borrowers or counterparties, related borrowers or groups of borrowers;

- Credit exposures by major asset category showing impaired and past due amounts relating to each category;

- Credit exposures restructured during a certain period and credits for which special conditions have been granted;

4.1.6 Stress testing

There is a distinct difference in the nature and magnitude of credit risks faced by an institution under normal business conditions and under stress conditions, such as financial crises. Under stress conditions, asset values and credit quality may deteriorate by a magnitude not predicted by analysis of normal business conditions.

Stress testing is a tool that can be used to assess the impact of market dislocations on an institution's credit portfolio. It can aid the institution in estimating the range of losses that it could incur in stress conditions, and in planning appropriate remedial actions.

An important component of stress testing is the identification and simulation of stress conditions or scenarios an institution could encounter. The stress events and scenarios postulated should be plausible and relevant to the institution's portfolio. These scenarios could include economic or industry changes, market – risk events and liquidity conditions.

Institutions must be in a position of analyzing the various situations in the economy or certain sectors to determine the event that could lead to substantial losses or liquidity problem. Whatever methods are used for stress testing, the output of these should be reviewed periodically and appropriate action taken by senior management in cases where results exceed agreed tolerance.

4.1.7 Internal controls and audit

Institutions should have in place an independent internal system for assessment of the credit risk management process. This function is necessary in order to independently enable the board determine whether the risk management process is working effectively. The results of these audits should be communicated promptly to the directors and senior management. The review should provide sufficient information to the board and management to enable them evaluate accurately performance and condition of the portfolio. The credit review function should report directly to the board of directors or a board audit committee.

A review of the lending process should include analysis of the credit manuals and other written guidelines applied by various departments of a bank, and the capacity and actual performance of all departments involved in the credit function. It should also cover origination, appraisal, approval, disbursement, monitoring, collection and handling procedures for the various credit functions provided by the institution. The internal audit review team should ensure the following:

- The credit granting function is carried out effectively;
- The credit exposures are within the prudential and internal limits set by the board;
- Validation of significant change in the risk management process;
- Verification of the consistency, timeliness and reliability of data used for internal risk rating system;
- Compliance with the institution's credit policies and procedures;
- Adherence to internal risk rating system;
- Identification of areas of weaknesses in the credit risk management process;
- Exceptions to the policies, procedures and limits.

The internal audit should be conducted on a periodic basis and ideally not less than once a year. The audits should also identify weaknesses in the credit risk management process and any deficiencies in the policies and procedures.

4.1.8 Board and Senior Management Oversight

1. The Board of Directors

The board of directors carries the ultimate responsibility of approving and reviewing the credit risk strategy and credit risk policies of the bank. This role is part of the board's ultimate responsibility of offering overall strategic direction to the bank. The credit risk strategy should clearly set the acceptable risk appetite and tolerance the institution is willing to engage, and the level of profitability the bank expects to achieve for incurring the various credit risks. The credit policies should be adequate and must cover all the activities in which credit exposure is a significant risk. The board should ensure that:

- The credit strategy has a statement on acceptable levels of exposure to the various economic sectors, currencies and maturities. It should also include the target markets, diversification and concentration of the credit portfolio;
- The credit risk strategy and policies are effectively communicated throughout the institution.
- The financial results of the institution are periodically reviewed to determine if changes need to be made to the credit risk strategy.
- The recruitment procedure ensures that the senior management team is fully capable of managing the credit risk.
- There is an internal audit function capable of assessing compliance with the credit policies and management of the entire credit portfolio.
- The delegation authority and approval levels are clearly defined.
- The management provides periodic reports on the insiders, provisioning and write-off on credit loan losses and audit findings on the credit granting and monitoring processes.

2. Senior Management

The senior management has the responsibility of implementing the credit strategy approved by the board of directors and developing policies and procedures for effective management of the credit risk. The senior management should ensure the following:

- The credit granting activities conform to the laid down strategy.

- Written procedures have been developed, implemented and responsibilities of the various functions are clearly defined.
- Compliance with internal exposure limits, prudential limits and regulatory requirements.
- The credit policies must be communicated throughout the institution, implemented, monitored and revised periodically to address any changes.
- Internal audit reviews of the credit risk management system and credit portfolio are undertaken regularly.
- Adequate research is undertaken for any new products or activities to ensure the risks are appropriately identified and managed. These products must receive prior board approval.

4.2. LIQUIDITY RISK MANAGEMENT

4.2.1 Purpose

These guidelines state the issues of prudence associated with the liquidity risk to which deposit institutions are exposed. Liquidity management ensures that the bank has the funds or the assurance of the availability of the funds needed to meet all its commitments. Effective liquidity management is essential for maintaining market confidence and protecting the bank's capital. It is at the heart of asset and liability management. Bank must ensure daily tracking of liquidities and implement a careful liquidity management policy to be sure of meeting its commitments.

It must pay special attention to the maturity of deposits and loans and to the availability and accessibility of funds while respecting the statutory requirements applicable to it and its offices.

4.2.2 Definitions

Liquidity means ability of a bank to obtain sufficient cash or its equivalent at the right time to pay its liabilities as they become due.

Liquidity risk management systems involves not only analyzing banks on and off balance sheet positions to forecast future cash flows but also how the funding requirements could be met. The latter involves identifying the funding market to which the bank has access, understanding the nature of those markets, evaluating the bank's current and future use of the market and monitoring signs of erosion of confidence

These guidelines indicate some of the elements that are taken into account in an evaluation of a bank's liquidity management, as well as certain quantitative factors that serve to evaluate liquidity levels.

Banks must:

- have robust financing and liquidity policies and controls approved by their Board of Directors;
- continuously track their financing and liquidity requirements;
- acquire integrated management systems that enable them to obtain timely information and satisfy the procedures, frequency and format needed to efficiently manage liquidities;
- analyze, where appropriate, changes made to financing requirements under other scenarios;
- analyze, where appropriate, changes made to financing scenarios;
- establish policies on the diversification of financing sources; and
- establish emergency plans.

Sound liquidity management can reduce the probability of serious problems. Indeed, the importance of liquidity transcends the individual bank, since a liquidity shortfall at a single institution can have system- wide repercussions. For this reason, the analysis of liquidity requires the management of the bank on an ongoing basis, but also to examine how funding requirements are likely to evolve under

various scenarios, including adverse conditions. National Bank of Rwanda requires all banks to have a formal strategy setting out the institution's management of liquidity.

This strategy shall be communicated throughout the organization. This step would involve setting a strategy for the bank, ensuring effective board and management oversight, as well as operating under a sound process for measurement, monitoring and controlling liquidity risk.

The formality and sophistication of the liquidity management process shall be appropriate for the overall level of risk incurred by the bank.

The liquidity strategy shall set out the general approach the bank will have to liquidity, including various quantitative and qualitative targets.

This goal shall address the bank' goal of protecting financial strength and the ability to withstand events in the market place.

All business units within the bank that conduct activities having an impact on liquidity shall be fully aware of the liquidity strategy and operate under the approved policies, procedures and limits.

Senior management and appropriate personnel shall have a thorough understanding of how other risks impact on the bank's overall liquidity strategy.

4.2.3 Liquidity Risk Tolerance

1. Liquidity risk tolerance is the level and types of liquidity risk that it is willing to assume. A bank must set a liquidity risk tolerance in light of its business objectives, strategic direction and overall risk appetite, and ensure that it is clearly articulated and communicated to all levels of management.

2. The bank should design the liquidity risk tolerance in a way that:

- it should be clearly defined the level of unmitigated funding liquidity risk the bank is willing to assume under normal and stressed conditions in accordance with its business strategy, financial condition, funding capacity and its role in the financial system,

- bank should ensure that funding is available to meet all obligations in times of stress, whether caused by market events or issues specific to a bank,

- all levels of management clearly understand the trade-off between risks and profits.

3. Banks should document its liquidity risk tolerance level which should be articulated preferably with a combination of qualitative and quantitative expressions.

4. The risk tolerance is required to be subject to the specification of a minimum survival period (at least one month) without the need for seeking emergency liquidity assistance from the BNR under a range of severe but plausible stress scenarios and other limits on liquidity metrics used for controlling different aspects of liquidity risk. The stress scenarios should consider any significant changes in the market circumstances or the validity of assumptions used. The quantitative measures relate to controls over such areas as liquid asset holdings, maturity or currency mismatches, concentration of funding and contingent liquidity obligations, depending on where the bank's risks and vulnerabilities lie.

5. The board should regularly monitor liquidity risk to ensure that executive officer operates within the Board's liquidity risk tolerance and limits.

6. The BNR will assess the appropriateness of a bank's liquidity risk tolerance (and any subsequent changes to such risk tolerance).

4.2.4 Board and Senior Management Oversight

The prerequisites of an effective liquidity risk management include an informed board, capable management, staff with relevant expertise and efficient systems and procedures. It is the responsibility of an institution's board and management to ensure that the institution has sufficient liquidity to meet its obligations as they fall due. It is primarily the duty of the board of directors to understand the liquidity risk profile of the institution and the tools used to manage liquidity risk. The board has to ensure that the institution has necessary liquidity risk management framework and that the institution is capable of confronting uneven liquidity scenarios. Generally the board should:

- Approve the institution's strategic direction and tolerance level for liquidity risk;
- Appoint senior managers who have the ability to manage liquidity risk and delegate to them the required authority to accomplish the job;
- Continuously monitor the institution's performance and overall liquidity risk profile; and
- Ensure that liquidity risk is identified, measured, monitored and controlled.

Each bank shall have a management structure in place to effectively execute the liquidity strategy. The responsibility for managing the liquidities of a bank shall be entrusted to a group in the form of an ALCO (assets and liabilities committee), consisting of senior management and the treasury function. The National Bank of Rwanda asks the Board of Directors of each bank to establish an ALCO that will introduce a guide to the institution's risk tolerance.

Senior management is responsible for the implementation of sound policies and procedures keeping in mind the strategic direction and risk appetite specified by the board. To effectively oversee the daily and long term management of liquidity risk, senior managers should:

- Develop and implement procedures and practices that translate the board's goals, objectives and risk tolerance into operating standards that are well understood by the bank staff;

- Adhere to the lines of authority and responsibility that the board has established for managing liquidity risk;

- Oversee the implementation and maintenance of management information and other systems that identify, measure, monitor, and control the bank's liquidity risk;

- Establish effective internal controls over the liquidity risk management process; and

- Ensure and review the contingency plans of the institution for handling disruptions to its ability to fund some or all of its activities in a timely manner and at a reasonable cost.

A sound framework for managing liquidity risk has three dimensions:

- maintaining a stock of liquid assets that is appropriate to the institution's cash flow profile and that can be readily converted into cash without incurring undue capital losses;

- measuring, controlling and scenario testing of funding requirements; and

- Managing access to funding sources.

4.2.5 Policies, Procedures and Limits

1. Policies

Banks must develop and implement the detailed, sound and prudent policies on financing and liquidities that are recommended by their senior management and approved by their Board of Directors, and then reviewed at least once each year by their Board of Directors or one of its committees. While specific details vary across institutions according to the nature of their business, the key elements of any liquidity policy should include:

- General liquidity strategy (short- and long term), specific goals and objectives in relation to liquidity risk management, process for strategy formulation and the level of approval within the institution;

- Roles and responsibilities of individuals performing liquidity risk management functions, including structural balance sheet management, pricing, marketing, contingency planning, management reporting, lines of authority and responsibility for liquidity decisions;

- Liquidity risk management structure for monitoring, reporting and reviewing liquidity;

- Liquidity risk management tools for identifying, measuring, monitoring and controlling liquidity risk (including the types of liquidity limits and ratios in place and rationale for establishing limits and ratios);

- Where an institution is actively involved in multiple currencies and/or where positions in specific foreign currencies are significant to its business, its liquidity policy should address the measurement and management of liquidity in these individual currencies which should include a back-up liquidity strategy for circumstances in which its normal access to funding in individual foreign currencies is disrupted; and

- Contingency plan for handling liquidity crisis.

To be effective the liquidity policy must be communicated down the line throughout the organization.

Procedures

Institutions should establish appropriate procedures and processes to implement their liquidity policies and include the following features:

- A procedures manual which should explicitly narrate the necessary operational steps and processes to execute the relevant liquidity risk controls;

- Periodic review and updating of the manual to take into account new activities, changes in risk management approaches and systems;

- Management should be able to accurately identify and quantify the primary sources of an institution’s liquidity risk in a timely manner;

- To properly identify the sources, management should understand both existing as well as future risk that the institution can be exposed to; and

- Management should always be alert for new sources of liquidity risk at both the transaction and portfolio levels.

2. Limits

Limits should be set and be appropriate to the size, complexity and financial condition of the financial institution. The limits should be periodically reviewed and adjusted when conditions or risk tolerances change. When limiting risk exposure, senior management should consider the nature of the institution's strategies and activities, its past performance, the level of earnings, capital available to absorb potential losses, and the board's tolerance for risk. Institutions may use a variety of ratios to quantify liquidity and create limits for liquidity management.

In addition, balance sheet complexity will determine how much and what types of limits a bank should establish over daily and long-term horizons. While limits will not prevent liquidity crisis, limit exceptions can be early indicators of excessive risk or inadequate liquidity risk management.

4.2.6 Measuring and Monitoring Liquidity Risk

Liquidity measurement involves assessing an institution's cash inflows against its outflows and the liquidity value of its assets to identify the potential for future net funding shortfalls. An institution should be able to measure and forecast its prospective cash flows for assets, liabilities, off-balance sheet commitments and derivatives over a variety of time horizons, under normal conditions and a range of stress scenarios, including scenarios of severe stress.

An effective measurement and monitoring system is essential for adequate management of liquidity risk. Consequently, institutions should institute systems that enable them to capture liquidity risk ahead of time, so that appropriate remedial measures could be prompted to avoid any significant losses. An effective liquidity risk measurement and monitoring system not only helps in managing liquidity in times of crisis but also optimize return through efficient utilization of available funds. Key elements of an effective risk management process include an efficient Management Information System (MIS), systems to measure, monitor and control risks.

The information system must verify whether the bank respects the regulations and enable management to evaluate trends affecting its global liquidity exposure.

1. Measurement of liquidity position

A number of techniques can be used to measure the liquidity risk, from simple calculation to statistical simulations based on sophisticated models.

Since Banks are affected by the changes in the political climate and market conditions, tracking of market trends and the economy is a key element of liquidity risk management.

Another important aspect of liquidity risk management consists of preparing scenarios of future needs for funds.

The following are the indicators that a bank should utilize at a minimum, to measure its liquidity position. A bank must establish appropriate internal guidelines on the level of the ratio and ensure prompt corrective actions are undertaken to address any liquidity shortfall.

a) Liquidity Coverage ratio

In compliance with the regulation nº 07/2017 of 19/05/2016 on Liquidity requirements for banks, a bank must compute and maintain on regular basis its Liquidity Coverage Ratio (LCR). The LCR is intended to promote resilience to potential liquidity disruptions over a thirty day horizon. The ratio

ensures that banks have sufficient unencumbered, high- quality liquid assets to offset the net cash outflows it could encounter under an acute short-term stress scenario. This ratio shall be computed

b) Net Stable Funding Ratio

Also, in compliance with the regulation Nº 07/2017 of 19/05/2016 on Liquidity requirements for banks, a bank must compute and maintain on regular basis its Net Stable Funding Ratio (NSFR). Stable Funding is funding which is not susceptible to fluctuations and is readily available at affordable cost and for a longer period of time (at least one year). The NSFR aims to limit over- reliance on short-term wholesale funding during times of buoyant market liquidity and encourage better assessment of liquidity risk across all on- and off-balance sheet items.

c) Loan to Deposit Ratio

Banks must compute at month end, a loan to deposit ratio. Such ratio provides a simplified indication of the extent to which a bank is funding illiquid assets by stable liabilities. Institutions should set a trigger loan-deposit ratio above which liquidity risk management should be enhanced.

d) Maturity Profile

Analyzing funding requirements involves the construction of a maturity profile. A cash flow projection estimates a bank's inflows and outflows and thus establishes net deficit or surplus (GAP) over time horizon. It takes into account the institution's funding requirement arising out of distinct sources on different time frames.

Maturity profiles will depend heavily on assumptions regarding future cash flows associated with assets, liabilities and off-balance sheet items.

Institutions should review the assumptions utilized in managing liquidity frequently to determine that they continue to be valid, since an institution's future liquidity position will be affected by factors that cannot always be forecast with precision given the rapidity of change in financial markets.

To evaluate its financing surplus or deficit, a bank must take into account, the following factors:

- the amount of assets easily cashable in relation to the amount of the surplus or deficit;
- the size of the surplus or deficit in relation to the total financing amount;
- the diversity of its financing sources; and
- Asset quality.

A bank must establish its internal limits for its short-term financing needs by taking into account its proven ability to finance itself on the market at a reasonable price.

These limits must be applied for each currency or group of currencies and, depending on the structure of the bank, they can also be set by entity or geographic location.

4.2.7 Monitoring Liquidity

1. Management Information

An institution must have a reliable management information system designed to provide the board of directors, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the bank. The management information system should have the ability to calculate liquidity positions in all of the currencies in which the bank conducts business. To effectively manage and monitor its net funding requirements, an institution should have the ability to calculate liquidity positions on an intraday basis, on a day-to-day basis for the shorter time horizons, and over a series of more distant time periods thereafter. The management information system should

be used in day-to-day liquidity risk management to monitor compliance with the bank's established policies, procedures and limits.

2. Key Liquidity Factors

The following key liquidity factors should be monitored closely:

- The maturity profile of cash flows under varying scenarios;
- The stock of liquid assets available to the institution and their market values;
- The ability of an institution to execute assets sales in various markets (notably under adverse conditions) and to borrow in markets;
- Potential sources of volatility in assets and liabilities (and claims and obligations arising from off-balance sheet business);
- The impact of adverse trends in asset quality on future cash flows and market confidence in the bank;
- Credit standing and capacity of providers of standby facilities to meet their obligations;
- The impact of market disruptions on cash flows and on customers;
- Intra-group cash flows and the accessibility of intra-group funding; and
- The type of new deposits being obtained, as well as its source, maturity, and price.

3. Asset Liability Committee (ALCO)

In order to effectively monitor its liquidity risk, an institution is supposed to establish an Asset Liability Committee (ALCO) with the following roles:

a) Management of the overall liquidity of the institution;
b) ALCO must report directly to the Board or in the case of a foreign incorporated bank, to senior management of the institution in the country;
c) ALCO must facilitate, coordinate, communicate and control balance sheet planning with regards to risks inherent in managing liquidity and convergences in interest rates; and
d) ALCO is responsible for ensuring that a bank's operations lies within the parameters set by its Board of Directors. However, the ALCO is not responsible for formulating the in-house liquidity risk management policy.

In determining the composition, size and various roles of the ALCO, the Board is required to consider the size of the institution, the risks inherent in the institution's operations and the organizational complexity.

All institutions are required to maintain written report of the deliberations, decisions and roles of the ALCO with regards to liquidity risk management.

4.2.8 Contingency Planning

In order to develop a comprehensive liquidity risk management framework, instutitions should have way out plans for stress scenarios.

1. Contingency Funding Plan

A Contingency Funding Plan (CFP) is a set of policies and procedures that serves as a blue print for a bank to meet its funding needs in a timely manner and a reasonable cost. It is a projection of future cash flows sources of a bank under market scenarios including aggressive asset growth or rapid liability

erosion. To be effective it is important that a CFP represent management's best estimate of balance sheet changes that may result from liquidity or credit events.

- Provide specific procedures to ensure timely and uninterrupted information flows to senior management.
- Clear division of responsibility within management in a crisis.
- Action plans for altering asset and liability behaviors (i.e., market assets more aggressively, sell assets intended to hold, raise interest rates on deposits).
- An indication of the priority of alternative sources of funds (i.e., designating primary and secondary sources of liquidity).
- A classification of borrowers and trading customers according to their importance to the institution in order to maintain customer relationships; and
- Plans and procedures for communicating with the media. Astute public relations management can help a bank to avoid the spread of rumors that could result in a significant run-off of funds.

2 Contingency Funding Sources

Banks should determine estimated amount of funds that will be used in liquidity crisis and expected degree of reliability, under what conditions these sources should be used, and the lead time needed to tap additional funds from each of the sources in the CFP.

In case a bank is part of a banking group (local or foreign), CFP should contain the operational procedures needed to transfer liquidity and collateral across group entities and borders by taking into account legal, regulatory, operational and time zone restrictions and controls governing such transfers.

4.2.9 Funding Diversification

Banks must develop and document an annual funding strategy that provide a bank to maintain access to sufficient funding at all times. They must periodically review their efforts to maintain diversification of its liabilities by establishing relations with the holders of its liability.

The funding strategy should include, but not limited to, following issues when banks develop annual funding strategy:

- funding limits by counterparty, instrument type, currency and geographic market,
- a diversification of wholesale funding sources, whether secured or unsecured, to ensure timely access to funds at reasonable costs and appropriate maturities,
- a higher reserve of unencumbered liquid assets if they depend more on volatile wholesale funding sources than on retail funding,
- access to diverse sources of liquidity for each of the major currencies in which a bank is active.

Banks should diversify funding across short-, medium- and long-term sources and establish targets that provide for effective funding diversification as part of their medium- and long-term funding plans. These funding targets should also be integrated into the banks' budget and business planning processes.

To verify if the liabilities are sufficiently diversified, a bank must examine the level of recourse to each source of financing by type of instrument, funder and geographic location, and set internal limits regarding the ceiling of the amounts it can accept from counterparty or a capital market (e.g. Commercial paper) in the normal course of business.

The frequency of reports and the frequency of recourse to a source of financing are two possible indicators of the vigor of the links for financing and, as a result, of their reliability.

Banks should analyze the characteristics of their available funding sources and the potential impact these may have on their liquidity position.

Banks should evaluate their exposure to large depositors on an ongoing basis and review regularly reports on largest twenty depositors. The historical performance of these fund providers, e.g. in terms of the maximum, minimum and average balances over the previous 12 months, should also be monitored.

The establishment of solid links with funders outside bank members of a group can constitute a good defense method in liquidity management.

Banks shall establish themselves permanently on different financial markets, where possible, and track developments in order to apply anticipatory measures, such as extending maturities or identifying alternative sources of funding (e.g. intragroup fund transfers, new debt issues, asset sales, etc.) to be used to generate liquidity in case of stress time.

4.2.10 Intraday Liquidity Risk Management

Banks should actively manage their intraday liquidity risk positions and risks to meeting payment and settlement obligations on a timely basis under both normal and stressed conditions.

Banks must develop effective procedures, systems and controls for managing their intraday liquidity risks in all of the financial markets and currencies in which they have significant payment and settlement activities.

Intraday liquidity procedures, systems and controls should, among other things, allow a bank to;

- measure all expected cash flows, anticipate their intraday timing and forecast the range of net funding shortfalls that might arise during the day. To implement these issues, bank's management should;
- understand the rules of all payment and settlement systems in which the bank participates, and understand the level and timing of liquidity needs of a bank that may arise as a result of the failure-to-settle procedures of these systems;
- identify key counterparties, correspondents or custodians that act as the source of incoming or outgoing gross liquidity flows;
- identify key times, days and circumstances where liquidity flows and possible intraday credit needs may be particularly high;
- understand the business needs underlying the timing of liquidity flows and intraday credit needs of internal business lines and key customers;
- monitor intraday liquidity positions against expected activities and available resources and prioritize payments if necessary. This requires a bank to monitor key function frequently during the day;
- to assess for additional intraday liquidity or restricting liquidity outflows to meet critical payments;
- allocate intraday liquidity efficiently among its own needs and those of its customers;
- react quickly to unexpected payment flows and adjust overnight funding positions;
- maintain sufficient assets that can be mobilized as collateral to obtain intraday or overnight funding from various sources, including the BNR, correspondent banks, and other counterparties in the markets mobilize collateral as necessary to obtain intraday funds with operational arrangements to pledge or deliver the collateral being already in place;

- manage the timing of outflows and be prepared to deal with unexpected disruptions to intraday flows. This requires a bank to conduct robust stress-testing and prepare contingency funding planning that reflect intraday considerations.

In meeting the operational needs for intraday liquidity management, a bank should apply appropriate tools and resources that are tailored to the bank's business model and its role in the financial system. This relates, for example, to whether the bank participates in a payment or settlement system directly or through correspondent or custodian banks, and whether it provides correspondent or custodian services and intraday credit facilities to other banks, firms or systems.

4.2.11 Foreign Currency Liquidity Management

Banks must have adequate systems in place for measuring, monitoring and controlling their liquidity positions in each major currency in which they undertake business activity. They must assess their aggregate foreign currency liquidity needs under both normal and stressed conditions, and control currency mismatches within acceptable levels.

Banks must assess the size and sustainability for each foreign currency mismatches using the same analysis that it applies to its domestic currency mismatches. Banks should also regularly review internal limits to control the size of cumulative net mismatches over particular time bands for each major foreign currency in which they operate. The size of foreign currency mismatches should take into account, inter alia, the following factors:

- the convertibility and price volatility of individual foreign currencies, the timing of access to funds in those currencies, as well as the potential for impairment;
- the conditions of foreign exchange markets, including the depth and liquidity of the markets and the level of interest rates;
- the stickiness of deposits in foreign currencies under stressed conditions.

4.2.12 Intragroup Liquidity Risk Management

In case a bank is part of a banking group (local or foreign), the bank should also be able to monitor and control liquidity risks arising from intragroup transactions (including cross-border transactions where applicable) with other legal entities in the group, taking into account any legal, regulatory, operational or other constraints on the transferability of liquidity and collateral to and from those entities.

While banks prepare their cash-flow projections, they should take into account the treatment of intragroup liquidity and assumptions on intragroup dependencies. Banks should treat intragroup transactions in the same way as other third party transactions for the purpose of cash-flow projections under normal business conditions.

Banks must specify their assumptions regarding intragroup liquidity movements (e.g. transferability of funds and collateral) in their liquidity risk management policies. The National Bank of Rwanda will review these assumptions by considering regulatory, legal, accounting, credit, tax and internal constraints on the effective movement of liquidity and collateral.

Banks should not take into account their back-to-back transactions with their group entities for the purpose of cash-flow projections or their statutory and risk control limits calculations.

Banks should establish internal limits on intragroup liquidity transactions to mitigate the risk of contagion from other group entities when those entities are under liquidity stress. In case the financial and liquidity position of the group is in doubt, the BNR monitors the level and trend of bank's intragroup transactions, and may constrain intragroup transactions by establishing supervisory limits.

Banks which are subsidiaries of foreign banks must submit information regarding group's liquidity risk profile and management to the BNR quarterly.

4.2.13 Stress Testing

In addition to conducting cash-flow projections to monitor net funding requirements under normal business conditions, banks must perform stress tests regularly for a variety of short-term and protracted institution-specific and market-wide stress scenarios (individually and in combination), by conducting projections based on "what if" scenarios on their liquidity positions to;

- detect vulnerabilities in a bank's liquidity profile that may not appear under normal market conditions,
- build up a liquidity cushion that can allow a firm to 'buy time' to reduce its liquidity risk levels,
- form the basis of a bank's liquidity management under adverse circumstances and help to shape its contingency funding plan.

The stress test outcomes must be used to adjust banks' liquidity risk management strategies, policies, and positions and to develop effective contingency plans.

Stress testing involves subjecting institution's liquidity position to several scenarios and assessing whether the institution can withstand liquidity shocks. The scenario entails a significant stress, albeit not a worst-case scenario, and assumes the following:

- a significant downgrade of the institution's public credit rating;
- loss of major deposits;
- a significant change in market interest rates;
- a significant increase in demand for loans and other funding;
- increases off-balance sheet exposures, including committed credit and liquidity facilities.

4.2.14 Internal Controls and Audit

In order to have effective implementation of policies and procedures, banks should institute review processes that should ensure the compliance of various procedures and limits prescribed by senior management. Banks shall have an adequate internal control system for the liquidity risk management process. This can be done through independent reviews and assessments. The results of such reviews are sent to the National Bank of Rwanda.

An effective internal control system for the liquidity risk includes:

- sufficient monitoring of the environment;
- an adequate liquidity risk evaluation and management process;
- the introduction of control instruments;
- an appropriate information system;
- regular reviews of policies; and
- procedures with regard to limits.

Periodic reviews and evaluations shall be conducted regularly to verify the level of liquidity risk and management's compliance with limits and operating procedures. Any exceptions should be reported immediately to board of directors and senior management for necessary action to be taken.

Management shall ensure that all such reviews and evaluations are conducted by individuals who are independent of the function being reviewed.

4.3 MARKET RISK MANAGEMENT

Banks may be exposed to Market Risk in variety of ways. Market risk exposure may be explicit in portfolios of securities / equities and instruments that are actively traded. Conversely it may be implicit such as interest rate risk due to mismatch of loans and deposits.

Besides, market risk may also arise from activities categorized as off-balance sheet item.

Therefore market risk is potential for loss resulting from adverse movement in market risk factors such as interest rates, forex rates, equity and commodity prices. The risks arising from these factors are discussed in the following paragraphs.

The risk arising from market risk factors can be categorized into the following categories:

- Interest rate risk;
- Foreign Exchange risk;
- Price Risk.

4.3.1 INTEREST RATE RISK MANAGEMENT

1. Purpose

These guidelines set out the policies and basic procedures that each bank must integrate in its interest rate risk management program, as well as the basic criteria that it must adopt to manage and control prudently its interest rate risk.

These guidelines apply to all bank operations (on or off the balance sheet) that are substantially exposed to interest rate risk.

Interest rate risk management is necessarily part of an overall business plan. Although these guidelines deal essentially with the responsibility of each bank with respect to interest rate risk.

management, it does not mean that such management can be dissociated from other aspects of asset-liability management, such as liquidity needs, credit risk and other types of risk.

2. Definitions

Interest rate risk corresponds to the risk of financial loss resulting from interest rate fluctuations.

This risk appears when monetary flows of assets, with respect to capital and interest, do not correspond to the monetary flows of liabilities, with respect to capital, interest and services.

The monetary flows of a bank can be uncertain. This uncertainty results, among other factors, from the existence of inherent variations in the asset and liability elements, as well as inherent options.

The sources of the interest rate risk are thus mainly three fundamental factors:

- basis risk: the imperfect correlation in the adjustment of borrowing and lending rates on various instruments;
- the yield curve risk for rates resulting from different instrument pricing;
- the rate repricing risk;

Changes in interest rates can have effects on future profits and on the discounted economic value of the bank or bank.

4.3.2 FOREIGN EXCHANGE RISK MANAGEMENT

1. Purpose

These guidelines set out the basic policies and procedures each bank must include in its foreign exchange risk management program, as well as the basic criteria it must adopt to prudently manage and monitor its foreign exchange risk.

Foreign exchange risk management is necessarily a part of a comprehensive company plan.

Although these guidelines essentially cover the responsibility of the individual bank for foreign exchange risk management, that does not mean that such management can be dissociated from other types of risks or other aspects of asset- liability management (such as the absolute necessity to preserve sufficient liquidity).

2. Definitions

Exchange rate risk is defined as the risk that a bank incurs with respect to its financial stability because of fluctuations in exchange rates. It is any unfavorable fluctuation in exchange rates risks affecting its financial stability.

Two factors are the source of the foreign exchange risk: (i) a mismatch of currencies between a bank's asset and liability elements (on or off the balance sheet), including capital, and (ii) mismatch of inflows and outflows of funds in foreign currencies. The bank is exposed to this risk as long as it has not hedged its foreign exchange position. The source of exchange rate risk can be specifically in services and operations in foreign currency, foreign exchange operations, and investments denominated in foreign currencies and investments in foreign subsidiaries.

The amount of the risk depends on the scale of the possible fluctuations of rates and the degree and duration of the exposure to the currency risk.

The gain or loss of the bank must be recognized in accordance with the chart of accounts. Accordingly, the limit of the currency exposure must be perceived as a necessary and important component of the foreign exchange risk management program of each bank.

The National Bank of Rwanda urges all banks to establish a solid risk management framework for exchange rate risk in order to be able to deal with risks of this type.

As with the other categories of risk, management of exchange rate risk includes the role of the Board of Directors and the exchange rate risk management program, which in turn includes the policies, limits and delegations of powers.

4.3.3 PRICE RISK

1. Equity Risk

Equity risk is the potential for reduced income or losses in on- and off-balance sheet positions arising from adverse changes in equity prices. The measurement of equity risk should capture the risk exposure to price movements in the overall equity market (e.g. a market index), specific sectors of the equity market (e.g. industry sectors or cyclical and non-cyclical sectors), and individual equity issues where appropriate.

2. Commodity Risk

Commodity risk is the risk that on- or off-balance sheet positions will be adversely affected by movements in commodity prices. Commodities include agricultural products, minerals and precious

metals. In addition to directional risk arising from changes in their spot prices, banks should also take into account basis risk while they measure their commodity risk (basis risk is the risk that the relationship between prices of similar commodities alters through time).

Likewise other risks, the concern for management of the equity and commodity risks must start from the top management. Effective board and senior management oversight of the bank's overall equity and commodity risk exposure is cornerstone of risk management process.

4.3.4 Market risk management program

Market risk management is a fundamental component of a sound and prudent management of bank operations. It requires prudent management of the bank's assets and liabilities, in order to monitor the repercussions of market fluctuations on the bank's financial results.

The specific procedures of the market risk management program vary from bank to bank, according to the size, nature and complexity of the asset-liability position, risk tolerance and risk profile.

However, a complete market risk management procedure must include the best interest rate management practices:

- Board and Senior Management Oversight;
- senior management supervision;
- the role of internal audit;
- the development and implementation of sound and prudent policies governing interest rate risk;
- the definition and application on a timely basis of appropriate interest rate risk evaluation techniques;
- The development and implementation of effective procedures for interest rate risk management and control.

4.3.5 Board and Senior Management Oversight

1. Role of the Board of Directors

The board of directors has the ultimate responsibility for understanding the nature and the level of market risk taken by the institution. The board therefore has the following principal responsibilities:

- To formulate and approve broad business strategies and policies that govern or influence the market risk of the institution. Accordingly, the board of directors is responsible for approving the overall policies with respect to interest rate risk, price risk and foreign exchange and ensuring that management takes the steps necessary to identify, measure, monitor and control these risks.

- It should also review the overall objectives of the institution with respect to market risk and ensure the provision of clear guidance regarding the level of market risk acceptable to the institution.

- To approve policies that identify lines of authority and responsibility for managing market risk exposures. As such it is responsible for ensuring that the institution has adequate policies and procedures for managing market risk on both a long-term and day-to-day basis and that it maintains clear lines of authority and responsibility for managing and controlling this risk.

- The board of directors should also review and approve the procedures to measure, manage and control price risk within which foreign exchange transactions shall be conducted.

- The board and senior management should therefore identify and have a clear understanding and working knowledge of the price risks inherent in the institution's investment portfolio and make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the institution's activities evolve.

- The board of directors should also review and approve the procedures to measure, manage and control foreign exchange risk within which foreign exchange transactions shall be conducted.

- To periodically review information that is sufficient in detail and timeliness to allow it to understand and assess the performance of senior management in monitoring and controlling these risks in compliance with the institution's board- approved policies.

2. Senior Management

The senior management has the responsibility of implementing all approved policies that govern Market Risk and developing procedures for effective management of the risks.

a) Management should be mandated by the board to be responsible for maintaining:
   - Appropriate limits on risk taking;
   - Adequate systems and standards for measuring market risk;
   - Standards for valuing positions and measuring performance;
   - A comprehensive market risk reporting and review process.
   - Effective internal controls.

b) Management should be sufficiently competent and able to respond to price risks, interest risks and foreign exchange risks that may arise from changes in the competitive environment or from innovations in markets in which the institution is active.

4.3.6 Evaluation of the market risk

To manage the market risk, there must be an accurate idea of the amounts at risk and the impacts of market fluctuations on the risk position.

To do this, the bank must have access to data that will allow it to take the appropriate measures on a timely basis, even when the deadlines are very short. The more time the bank takes to compile, eliminate or neutralize an undesired risk, the greater the possibility of loss.

Each bank must have risk evaluation techniques that precisely measure the impact of future market fluctuations on its financial situation.

In its choice of relevant scenarios, the bank must take into account the volatility of rates and price, and the reasonable time it will need to be able to react to unfavorable market fluctuations.

There are many techniques that a bank can use to evaluate the market risk. Each bank will use at least one and preferably several of these techniques to manage the rate risk to which it is exposed.

Each technique serves to view the risk involved from a different angle, offers various advantages and disadvantages and turns out to be more effective when combined with other techniques.

Among the evaluation techniques used, there are the matching of monetary flows by calendar year, matching the duration, matching convexity and analysis of the partial duration (key rate). The evaluation techniques chosen must comply with the guidelines on market risk and the limits applied to the asset portfolio.

The National Bank of Rwanda subscribes to the principle that the degree of sophistication of market risk assessment techniques shall reflect the level of risk inherent in the bank.

When the bank uses a model to measure and mitigate its exposure to market risk, the National Bank of Rwanda expects that this model has been tested and thoroughly examined by use of an independent function.

These models must be revised as a function of the scale of exposure to market risk, the nature of market variations and the complexity of innovations associated with interest rate and price measurement.

4.3.7 Policies, Procedures and Limits

1. Policies and Procedures

Institutions must have clearly defined policies and procedures for limiting and controlling market risk on both on- and off- balance sheet positions. These policies should be applied on a consolidated basis and as appropriate, at specific affiliates or other units of the institution

Such policies and procedures must be designed to reflect the importance and complexity of the market risk to which the bank is exposed. For this purpose, it is important to submit frequent and timely reports on the bank's position regarding risk.

In particular, it is important to report promptly any violation of market risk limits and to take steps to correct the situation.

Audits are a basic element for managing and monitoring a bank's market risk management program. Each bank will make use of this to approach to see that its policies and management procedures are respected and ensure their integrity.

These audits must be applied to all aspects of the bank's market risk management in order to:

- ensure respect for policies and procedures established to manage interest rate risks;
- ensure that effective management controls are exercised regarding the market risk positions;
- verify the relevance and accuracy of the data in the management information reports;
- See that the managers of the market risk have a thorough knowledge of the bank's risk management policies and limits and have the desired skills to make wise decisions that are compatible with these policies.

The results of these evaluations must be submitted on a timely basis to the Board of Directors of the bank for examination.

Policies and procedures related to market risk should:

- Delineate lines of responsibility and accountability over market risk management decisions and should clearly define authorized instruments, hedging strategies and position-taking opportunities;

- Identify the types of instruments and activities that the institution may employ or conduct, thus acting as a means through which the board can communicate their tolerance of risk on a consolidated basis and at different legal entities;

- Identify quantitative parameters that define the levels of interest rate risk, price risk and foreign exchange risk acceptable for the institution and where appropriate, such limits should be further specified for certain types of instruments, portfolios and activities;

- Review and revise periodically the procedures so as to define the specific procedures and approvals necessary for exceptions to policies, limits and authorizations;

- Delineate a clear set of institutional procedures for acquiring specific instruments, managing portfolios and controlling the institution's aggregate market risk exposure.

Prior to introducing a new product, hedging, or position-taking strategy, management should ensure that adequate operational procedures and risk control systems are in place. The board or its appropriate delegated committee should also approve major hedging or risk management initiatives in advance of their implementation.

2. Limits

Each bank must establish prudent and precise limits for market risk and make sure that its level of exposure to this risk does not exceed these limits, which must comply with the guidelines of the bank on market risk.

To determine these limits, the bank must consider the other risks to which it is exposed.

These limits can reflect the capacity of the bank to compensate internally its positions regarding market risk, for example, by combining the monetary flows of liabilities of various complementary products.

Moreover, these limits must be reassessed regularly to reflect the modifications of the bank's risk profile and the general guidelines it has adopted for market risk.

An appropriate limit system should:

- Enable management to control market risk exposures, initiate discussion about opportunities and risks and monitor actual risk taking against predetermined risk tolerances;
- Ensure that positions that exceed certain predetermined levels receive prompt management attention;
- Be consistent with overall approach to measuring market risk;
- Should be approved by the board of directors and re-evaluated periodically;
- Be appropriate to the size, complexity and capital adequacy of the institution as well as its ability to measure and manage its risk; and
- Be identifiable with individual business unit, portfolios, instrument types or specific instruments.

Institutions must have adequate information systems for measuring, monitoring, controlling and reporting market risk exposures. Reports must be provided on a timely basis to the board of directors, senior management and, where appropriate, individual business line managers.

The following are some of the board reports that should be provided:

- Violation of approved responsibilities by managers when taking interest rate risk exposures. Or investing in un- approved instruments;
- Excesses over approved interest rate limits;
- Any exceptions highlighted by the internal auditor.

4.3.8 Measurement, Monitoring and Control

1. Risk monitoring and control

Banks should establish a sound and comprehensive risk management process to monitor and control its market risk. This process should include, among other things,

- an appropriately detailed structure of risk limits, guidelines and other parameters used to govern market risk taking;
- an appropriate management information system (MIS) for controlling, monitoring and reporting market risk,
- accounting policies on the treatment of market risk.

Banks should have the system that should be able to measure current exposures, through marked-to-market or marked-to-model pricing, as well as potential market risks. The bank's risk management system should, at least, provide the following information on a daily basis:

- the outstanding positions,
- unrealized profit or loss,
- the accrued profit or loss.

Banks should ensure the integrity of data used by their risk management systems. Data used should be:

- appropriate (e.g. marked-to-market data for trading activities),
- accurate,
- complete (e.g. both on- and off-balance sheet positions),
- timely,
- frequently updated, and
- sourced independently of the position-taking units.

A bank whose risk levels fluctuate significantly within a trading day should monitor its risk profile on an intra-day basis. The risk management system should, wherever feasible, be able to assess the probability of future losses. It should also enable an institution to identify risks promptly and take quick remedial action in response to adverse changes in market factors.

Bank's treasury and financial derivative valuation processes should be independent of its trading function. Banks should regularly evaluate market risk measurement models and assumptions to ensure that they provide reasonable estimates of market risk. These should be validated before deployment. Staff involved in the validation process should be adequately qualified and independent of the trading and model development functions. A back-testing program should also be conducted regularly to verify that the models are reliable in measuring potential losses over time.

Even if a bank could eliminate foreign currency risk by avoiding exposure to it or by hedging its position, a solution of this order cannot be desirable for other valid financial reasons.

As a consequence, foreign exchange risk management must not necessarily seek to eliminate the risks attributable to rate fluctuations. It must instead enable the bank to contain the effects of

fluctuations of exchange rates within the limits it has established after a careful review of various possible rate circumstances.

2. Approaches to measuring and limiting Market Risk

Measuring risk is very critical to understanding the potential loss an institution may be exposed to in event of any loss. The principal goal should be to provide strong assurance that losses resulting from market risk will not substantially diminish the capital and earnings of an institution. Common approaches to measuring and limiting market risk are:

- Limit the size of the open positions in each currency as of the close of business each day. Limits are established for either the nominal size of the position or the size of the percentage;
- Limit the size and concentration of investment that is price sensitive, based on percentage of either total investment or total assets of the institution;
- Adherence to the regulatory requirements that pertain to the net open positions;
- Determine, on a continuous basis, the size of the loss that would be incurred should the exchange rate move against the institution's open position.
- Determine the size of the loss that would be incurred should the prices of shares and other investments move against the position the institution has taken; and
- Ensure adequate training of personnel and segregation of duties between the front and the back office.

a. Stress Test

Stress tests to measure vulnerability to loss arising from market risk operations should be undertaken regularly. Stress tests shall cover major interest rate, foreign exchange, commodities and equities exposures. Stress situations include but are not limited to market movements or bank specific situations in terms of profitability, liquidity and capital adequacy.

The risk measurement system should support a meaningful evaluation of the effect of stressful market conditions on the financial institution. Stress testing should be designed to provide information on the kinds of conditions under which the institution's strategies or positions would be most vulnerable and thus may be tailored to the risk characteristics of the institution.

b. Assets and Liability Committee

ALCO committee is crucial in sound management of market risk. The committee is responsible for supervision and management of Market Risk and liquidity risk. The committee generally comprises of senior managers from treasury, Chief Financial Officer, business heads generating and using the funds of the bank, credit, and individuals from the departments having direct link with interest rate and liquidity risks.

The size as well as composition of ALCO depends on the size of each bank, business mix and organizational complexity. To be effective ALCO should have members from each area of the bank that significantly influences market and liquidity risk.

The Asset and Liability Management Committee (ALCO) should review the management of foreign currency denominated assets and liabilities within the risk parameters approved by the Board of Directors.

c. Management Information System

An accurate, informative, and timely management information system is essential for managing market risk exposure, both to inform management and to support compliance with board policy. Reporting of risk measures should be regular and should clearly compare current exposure to policy limits. In addition, past forecasts or risk estimates should be compared with actual results to identify any modeling shortcomings.

The board on a regular basis should review reports detailing the market risk exposure of the institution. While the types of reports prepared for the board and for various levels of management will vary based on the institution's market rate risk profile, they should, at a minimum include the following:

- Summaries of the institution's aggregate exposures;
- Reports demonstrating the institution's compliance with policies and limits;
- Results of stress tests including those assessing breakdown in key assumptions and parameters;
- Summaries of the findings of reviews of interest rate risk, price risk, and foreign exchange risk;
- Policies, procedures, and the adequacy of the market risk measurement systems, including any findings of internal and external auditors/consultants;
- Maturity distribution by currency of the assets and liabilities for both on and off balance sheet items;
- Outstanding contracts by settlement date and currency;
- Total value of outstanding contracts, spot and forward;
- Gains and losses, totals and comparison to previous day's;
- Market value of off-balance sheet products and aggregate dealing limits;
- Exceptional reports e.g. Limit or line excesses;
- Total value of outstanding investments, and current market values;
- Profit and loss, totals and comparison to previous mark to market and aggregate investment limits;
- Limit or sectoral excesses and valuation of option contracts, if any.

4.3.9 Internal controls and independent audits

As an integral part of the overall internal control system, banks should have adequate internal controls over their market risk. The effectiveness of such controls should be evaluated regularly by independent parties, e.g. internal or external auditors. An effective system of internal controls for market risk should ensure that:

- the policies and procedures established for market risk management are respected;
- banks have organizational controls to ensure that there exists a clear and effective segregation of duties between those persons who initiate transactions and those who are responsible for operational functions,
- any hedging measures adopted respond to the bank's policies, strategies and procedures for foreign exchange risk management;
- The market risk managers are perfectly informed of the market risk management policies and the limits for risk and have the desired competence to make wise decisions that are compatible with these policies;
- procedural controls to ensure that
  - transactions are fully recorded in the records and accounts of the institution,
  - transactions are correctly settled,
  - unauthorized dealing is promptly identified and reported to management.

- controls to ensure that market activities are monitored frequently against the institution's market risk limits that excesses are reported,
- there is an effective management information system and reports are complete and exact with respect to the market risk management practiced by the bank.

Banks should also ensure that market risk exposures are reported in a timely manner to the Board and Senior Management. The bank should establish the market risk management function which may be standalone, centralized or integrated with other risk management or supporting functions based on the bank's the nature and complexity of its operations. If small banks with simple operations find it difficult to establish such function as standalone, centralized, integrated, or supporting functions, then such function can be executed by dedicated staff provided that they have the capability to perform the function and do not assume any front-line risk-taking activities.

4.4. OPERATIONAL RISK MANAGEMENT

4.4.1. Object and Definitions

Operational risk is the risk of direct or indirect loss resulting from the absence or inadequacy of the internal control process, people and systems or due to an external event or other disasters.

It also includes exposure to loss resulting from the faulty operation of a manual or automatic system to process, produce or analyze operations and transactions within the time periods allowed and with the intended security.

Operational risk management is an important element of a solid risk management practice in every institution.

The main types of operational risk result from deficiencies in internal controls and corporate governance. These deficiencies can often be the source of financial losses as the result of error, fraud or failures to perform on time or compromise the financial interests of an institution.

The other aspects of operational risk concern specifically the failure of information technology systems or events like fire or other disasters.

At this time, operational risk represents a threat for banks in Rwanda because of technological innovation and developments in communications and information systems.

Institutions should develop, implement and maintain an enterprise-wide Operational Risk Management Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual institution will depend on a range of factors, including its nature, size, complexity and risk profile.

The policies defining the Framework should clearly

- Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

- Describe the risk assessment tools and how they are used;

- Describe the bank's accepted operational risk profile, permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments;

- Describe the bank's approach to establishing and monitoring thresholds or tolerances for inherent and residual risk exposure;

- Establish risk reporting and Management Information System (MIS);
- Provide for appropriate independent review and assessment of operational risk; and
- Require the policies to be revised whenever a material change in the operational risk profile of the bank occurs.

A real operational risk management program shall include: Board of Directors and senior management oversight, policies and procedures, risk measurement, information management systems, and internal controls and audit.

4.4.2 Board and Senior Management Oversight

The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior.

1. Role of Board of Directors

The board of directors should take the lead in establishing the "tone at the top" which promotes a strong risk management culture.

It is the responsibility of the board of directors to:-

- Establish a strong operational risk management culture throughout the institution;
- Ensure that the institution has developed, implemented and maintained a Framework that is fully integrated into the institution's overall risk management processes;
- Oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels;
- Review the framework regularly to ensure that the institution is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems;
- Approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

2. Role of Senior Management.

Senior management is responsible for consistently implementing and maintaining throughout the institution policies, processes and systems for managing operational risk in all of the institution's material products, services and activities, consistent with the institution's risk appetite and tolerance.

Senior Management responsibilities includes:

- Implementing the operational risk management framework approved by the Board of Directors by consistently implementing and maintaining throughout the institution policies, processes and systems for managing operational risk in all of the institution's material products, services and activities, consistent with the risk appetite and tolerance;

- Ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks and incentives are well understood;

- Ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk;

- To ensure that the institution's operational risk management policy has been clearly communicated to staff at all levels in the units that face material operational risk;

- Implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

4.4.3 Policies and procedures

Institutions should have policies, processes and procedures adopted by the Board of Directors reflecting management strategy to control or mitigate material operational risks. Operational risk policies and procedures that clearly define the way in which all aspects of operational risk are managed should be documented and communicated. These operational risk management policies and procedures should be aligned to the overall business strategy and should support the continuous improvement of risk management.

While each level of management is responsible for the existence of appropriate policies and procedures, senior management must clearly have authority and responsibility and require reporting that will encourage this action. Such responsibility includes making sure that the necessary resources are available to effectively manage the operational risk.

Moreover, senior management shall evaluate the monitoring system in the light of the risk inherent in each strategy and business line.

The primary responsibility for operational risk management lies in the business unit. The manager of the unit shall be expected to make sure that operational risk control systems are in place. All banks shall make reviews of the internal controls in each business line.

An institution's operational risk exposure is increased when it engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. An institution should therefore develop and implement policies and procedures that address the process for review and approval of new products, activities, processes and systems.

The review and approval process should consider:-

- Inherent risks in the new product, service, or activity;
- Resulting changes to the institution's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
- The necessary controls, risk management processes, and risk mitigation strategies;
- The residual risk;
- Changes to relevant risk limits; and
- The procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced.

Policies on Outsourcing

Outsourcing is the use of a third party either an affiliate within a corporate group or an unaffiliated external entity to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities.

Outsourcing policies and risk management activities should encompass:

- Procedures for determining whether and how activities can be outsourced;
- Processes for conducting due diligence in the selection of potential service providers;
- Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
- Program for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
- Establishment of an effective control environment at the bank and the service provider;
- Development of viable contingency plans; and
- Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

4.4.4 Measurement, Identification, Monitoring and control of the operational risk

1. **Measurement and identification of operation risk**

Risk identification is a prerequisite for risk assessment, control and monitoring. Effective risk identification considers both internal factors (such as the complexity of the institution's structure, the nature of its activities, the quality of its personnel, organizational changes and staff turnover) and external factors (such as fluctuations in economic conditions, change and technological advances) that can prevent institutional objectives from being achieved.

The risk identification process shall also determine which risks will be controlled by the bank institution and which not. There are several processes commonly used by banks to help them in identifying operational risk:

- **Self or risk assessment**: a bank evaluates its operations and activities with respect to operational risk events and internal processes and often incorporates checklists to identify the strengths and weaknesses of the operational risk environment.

- **Risk mapping**: in this process, the type of risk is associated with the different units and organizational functions; this exercise can reveal zones of weakness and help in prioritizing risk management actions.

- **Key Risk Indicators**: risk indicators that are statistical and/or metric and often financial shall be reviewed periodically. These indicators can include the number of failed trades, staff turnover rates and the frequency and/or severity of errors or omissions.

- **Threshold/ limits**: typically tied to risk indicators threshold levels (or change) in key risk indicators, when exceeded alert management to areas of potential problems.

- **Score cards**: these provide a means of translating qualitative assessments quantitative metrics that can be used to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

The operational risk measurement consists of estimating the probability and size of an operational loss. Such information fundamental for assessing, monitoring and controlling the operational risk exposure.

In any risk assessment system, statistics shall be collected to develop a general picture of the operational risk.

To measure operational risk, banks need to identify the operational risk factors.

The identification approach usually accepted is to break down the operational risk into risks linked to internal operations, persons and systems and those linked to the bank's external environment.

Operational risk can be linked to the events below (this list is not exhaustive):

Trades

- Execution error;
- Accounting error;
- Settlement error;
- Documentation error;
- Product complexity.

Operations control

- Limit overruns
- Internal fraud
- Money laundering
- Security risk

Systems

- Programming error
- Management information error
- Information system failure
- Telecommunications failure

The sources of operational risk are numerous and variable. Some are:

- employees(e.g. human error, internal fraud, inadequate knowledge, inadequate training, lack of understanding of performance, inadequate human
- technology (technological shortcomings, system degradation);
- customer relations (disputes);
- capital and assets (destruction by fire, other disasters);
- information risk;
- legal issues and litigation;

The impact of the technology can have a negative influence on bank services with respect to:

- control of customer accounts;
- electronic funds transfer;
- automatic cash dispensers;

- point of sale/purchase of payment card;
- home banking;
- e-mail billing (where available);
- on-line banking.

A good human resources management program makes it easier to:

- identify human resource needs (by calling attention to incompatible tasks);
- have competent personnel with the knowledge and expertise to develop the required positions;
- retain competent personnel with continuous training and other ways of developing the professional and intellectual capacities of the personnel;
- conduct performance reviews; and
- Engage in successor planning.

The clear definition of the limits of authority helps in making sure that:

- the level of effective and approach management is extended without the institution;
- the delegation of authority is adequate and appropriate;
- there is no ambiguity in responsibilities;
- the decisions are made by the persons who are able to assess their implications;
- persons are not assigned to conflicting responsibilities;
- and employees report to an appropriate level of authority.

Effective communication of responsibilities is an important element of human risk management. It makes to possible to make sure that personnel have a clear understanding of how the authorities perform their responsibilities. The prudent management of the assignment of responsibility, effective risk management and control of the environment are, to differing degrees, the responsibility of all personnel of the bank institution.

All individuals need to execute their responsibilities in the best conditions and need to feel comfortable in conveying to senior management every significant aspect of their work.

An effective separation of incompatible tasks between the persons who authorize, supervise and initiate or execute transactions and those who record or account for operations.

The separation of tasks between individuals and departments reduces the intentional or willful risk of manipulation or error by strengthening controls.

Process risk: no process can completely prevent the possibility of the wrong recording of operations. Properly documented activities, the risk management process, the policies, procedures and controls can contribute to reducing the occurrence of undetected errors. They also contribute to identifying the significant factors in the activities of a business and risk management, the assessment of the probability that these risks occur and the assurance of preventive controls, assets and other financial information of the establishment.

Information reliability risk: the risk for all institutions consists of decision-makers making decisions and measures that are incorrect or inappropriate as the result of accounting or other information that does not reflect the true situation of the activity.

Good accounting facilitates offers the assurance that:

- the accounting policies and practices of the establishment are appropriate
- the appropriate recording and other information are guaranteed

- there are effective accounting controls;
- the quality and value of the amounts of the assets and liabilities are regularly tracked and reviewed and;
- The assets and liabilities are valued and correctly recognized.

Decision-makers must regularly have reliable information to make various decisions. Information management systems offer an instrument for conveying information to decision-makers while allowing this information to be reviewed. The frequency with which the information is prepared, the level of detail, the analyses and explanations and the information media will depend on the nature of the operations or managed risk and the level of the responsible authority. The institution shall regularly review its systems to evaluate the information produced and the adequacy and quality of system performance.

Technological risk: Banks are dependent on communications and information technologies including the platforms, computers (hardware and software), data files and other technological systems that support their operations.

The possibility of dislocation of activities as the result of an obsolete or inadequate technology or technological interruption caused by external or internal events represents a significant risk.

The technological development and maintenance process offer assurance that there is a planned technological strategy and the investment to improve or keep up with technological innovation.

2. Monitoring of operational risk

All banks must introduce a system that monitors, on a continuous basis, their exposure to operational risk and the events that generate risks in the each of the main business lines.

An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss.

An institution should maintain a log of major operational risks events such as:-

- frauds and attempted frauds;
- robberies;
- breaches of the bank's risk appetite and tolerance level;
- details of recent significant internal and external operational risk events and losses;
- Any operational risk events witnessed in the financial industry and the how well the institution is prepared to mitigate such events;
- System downtime.

Data capture and risk reporting processes should be analyzed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk. Management should ensure that information is received by the appropriate people, on a timely basis, in a form and format that will aid

in the monitoring and control of the business. The reporting process should include information such as:

- The critical operational risks facing the institution;
- Risk events and issues together with intended remedial actions;
- The effectiveness of actions taken;
- Details of plans formulated to address any exposures where appropriate;
- Areas of stress where crystallization of operational risks is imminent;
- Exception reporting (covering among others authorized and unauthorized deviations from the bank's operational risk policy and likely or actual breaches in predefined thresholds for operational exposures and losses).

3. Control of operational risk

Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control program consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

a) Control and information system management

All banks must introduce a system that monitors, on a continuous basis, their exposure to operational risk and the events that generate risks in the each of the main business lines.

Banks shall directly track operational losses through an analysis of each occurrence and description of the nature and cause of the loss reported to senior management and the Board of Directors.

An effective control system is essential for adequate management of operational risk. Permanent controls can help quickly detect and correct the deficiencies in the policies, processes and procedures of operational risk management.

The frequency of the controls shall reflect the identified risks and the frequency and nature of changes in the operational environment. Control is more effective when the internal control system is integrated with the bank's operations and generates regular reports. The results of these control activities shall be included in the reports to management and the Board of Directors.

A good information system shall be capable of producing a report on operational risk management.

Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management program.

The use of technology related products, services, delivery channels and processes exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.

An institution should have a detailed Business Continuity Plan. Recovery plans and business resumption priorities must be defined and contingency procedures tested and practiced so that business and operating disruption arising from a serious operational risk incident is minimized. The recovery plan and incident response procedures should be evaluated periodically and updated as and when changes to business operations, systems and networks occur.

b) Control and Mitigation

All banks shall also have policies and procedures to control and/or mitigate operational risk. They shall evaluate the relative costs and benefits related to the limitation and control of the operational risk and adjust their exposure to operational risk with appropriate strategies in the light of the risk general profile.

The control activities shall make it possible to reduce or eliminate the risks identified by the bank institution. The control process and procedures shall be established and the banks should have a system in place to ensure the compliance of the documentation with the internal policies on risk management.

The elements in this process include:

- high level of reviews of progress of the institution with respect to assigned objectives;
- verifying the compliance with management controls;
- policies and procedures concerning the review, processing and adjustment of on-compliant aspects; and
- A documented system of authorizations and delegations to ensure the good governance of an appropriate management.

To be effective, control activities shall be an integral part of the regular activities of the bank and involve all levels of staff, including senior management and business units.

An effective control environment requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other counter-measures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and be subject to careful independent monitoring and review.

In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk.

Examples of these controls include:

- Clearly established authorities and/or processes for approval;
- Close monitoring of adherence to assigned risk limits or thresholds;
- Safeguards for access to, and use of, bank assets and records;
- Appropriate staffing level and training to maintain expertise;
- Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
- Regular verification and reconciliation of transactions and accounts; and
- Vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

In case where operational risks cannot be controlled or mitigated by the bank, Board of Directors should decide whether to reduce the level of business activity involved, or completely withdraw from the activity.

4. Internal control and audit

In order to mitigate or reduce operational risk, internal controls are very necessary and critical. The internal controls shall be considered a main instrument of operational risk management.

An effective internal control system assumes differentiation in tasks in and personnel with responsibilities that do not create conflicts of interest.

Assigning tasks subject to such conflicts to an individual or group of individuals can make it possible to cancel or reduce such losses, errors or inappropriate actions. As a consequence, conflicts of interest shall be identified, minimized and subjected to independent controls and reviews.

The activities of internal auditors constitute also an important element of the operational risk management. To be sure of the existence of good internal controls, the internal auditors must be proactive in treating an institution's problems.

In particular, the identification of potential problems, the independent validation of self-evaluations of the management of business and the adjustment of problem situations shall be a major function of internal audit.

An important role is also assigned to the external auditors, whose tasks consist of reviewing the internal controls, systems procedures and the information system management of the institution as well as the preparation of the management letter that discloses, among others any shortcomings in the internal control systems. The external auditors can also be asked to make an evaluation of the operational risk of a bank in order to see whether the risk is properly managed.

4.4.5 Stress Testing

An institution should conduct stress tests on a regular basis for a variety of short-term and protracted institution-specific and operational risks stress scenarios to identify sources of potential operational risks and to ensure that institution is prepared to continue in business after minor and major operational risk events. An institution should use stress test outcomes to adjust its operational risk management strategies, policies, and positions and to develop effective contingency plans.

4.5 TECHNOLOGY RISK MANAGEMENT

4.5.1 Introduction

Technology risk has been defined as the risk of loss arising from the potential inadequate information system or technology failures.

The purpose of Technology (Information and Communication Technology) risk management is to assist institutions to establish an effective mechanism that can identify, measure, monitor, and control the risks inherent in institutions' ICT systems, ensure data integrity, availability, confidentiality and consistency and provide the relevant early warning mechanism.

4.5.2 Board and Senior Management Oversight

1. Role and Responsibilities of Board of Directors

The board of directors of institutions has the following responsibilities with respect to the management of technology risk:

- Ensure that the institution has in place an appropriate IT governance structure and risk management framework which suits its own circumstances, business needs and risk tolerance.

- Ultimately responsible for understanding IT risks and overseeing the design and implementation of an appropriate internal controls and risk management practices on information systems. They should be familiar with IT and data center concepts and activities to carry out their responsibilities.

- Endorse the IT strategy that should be formally documented. The board of directors should also approve IT plans, policies and major expenditures.

- Periodically review the alignment of IT strategy with the overall business strategies and significant policies of the institution.

- Approve IT risk management strategies and policies.

- Set high ethical and integrity standards, and establish a culture within the institution that emphasizes and demonstrates to all levels of personnel the importance of IT risk management.

- Establish an IT steering committee which consists of representatives from senior management, the IT function, and major business units, to oversee these responsibilities and report the effectiveness of strategic IT planning, the IT budget and actual expenditure, and the overall IT performance to the board of directors and senior management periodically.

- Ensure that an effective internal audit of the IT risk management is carried out by operationally independent, well-trained and qualified staff, which report should be submitted to the audit committee;

- Ensure the appropriation of funding necessary for IT risk management function.

- Understand the major IT risks inherent in the institution's business, setting acceptable levels for these risks, and ensuring the implementation of the measures necessary to identify, measure, monitor and control these risks.

2. Responsibilities of Senior Management

The following are key responsibilities of senior management with regards to Technology risk management:

- Ensuring that all employees of the institution fully understand and adhere to the Technology risk management policies and procedures approved by the board of directors and the senior management, and are provided with pertinent training.

- Ensuring customer information, financial information, product information and core banking system of the legal entity are held in a secure environment.

- Reporting in a timely manner to the National Bank of Rwanda any significant adverse incidents of information and communication systems or unexpected events, and how they have been handled;

- Cooperating with the National Bank of Rwanda in the surveillance of the risk management of information systems, and ensure that supervisory opinions are followed up; and

- Performing other related Technology risk management tasks.

3. Head of Information and Communication Technology Unit

The following are the responsibilities of the Head of IT:

- Play a direct role in key decisions for the business development involving the use of ICT in the institution;

- Ensure that information systems meet the needs of the institution, and the IT strategies, in particular information system development strategies, comply with the overall business strategies and IT risk management policies of the institution;

- Be responsible for the establishment of an effective and efficient IT organization to carry out the IT functions of the institution. These include the IT budget and expenditure, IT risk management, IT policies, standards and procedures, IT internal controls, professional development, IT project initiatives, IT project management, information system maintenance and upgrade, IT operations, IT infrastructure, Information security, disaster recovery plan (DRP), IT outsourcing, and information system retirement;

- Ensure the effectiveness of IT risk management throughout the organization including all branches.

- Organize professional trainings to improve technical proficiency of staff.

4. Staffing of the Information and Communication Technology Unit:

Institutions should designate qualified officer(s) in the Management function for IT management. Staff in each position should meet acceptable minimum requirements on professional skills and knowledge. The following risk mitigation measures should be incorporated in the selection and management of IT staff:

- Verification of personal information including confirmation of personal identification issued by government, academic credentials, prior work experience, professional qualifications, certificates of good conduct by the Police;

- Ensuring that ICT staff meet professional ethics and integrity by obtaining character reference from independent referees, former employers, relevant sector regulators;

- Signing of agreements with employees about understanding of ICT policies and guidelines, non-disclosure of confidential information, authorized use of information systems, and adherence to ICT policies and procedures; and

- Evaluation of the risk of losing key ICT personnel, especially during major ICT development stage or in a period of unstable ICT operations, and the relevant risk mitigation measures such as staff backup arrangement and staff succession plan.

4.5.3 Intellectual Proprietary Rights

Insitutions should put in place policies and procedures to:

- ensure the utilization of only genuine and licensed software in order to avoid the violation of the law regarding intellectual properties,
- ensure purchase of legitimate software and hardware,
- prevention of the use of pirated software, and
- the protection of the proprietary rights of ICT products developed by the institution, and ensure that these are fully understood and complied with by all employees.

4.5.4 Technology Risk Management Framework

1. Information and Communication Technology Strategy

Institutions should formulate an ICT strategy that aligns with the overall business plan of the institution, ICT risk assessment plan and an ICT operational plan. The ICT strategy should ensure that adequate financial resources and human resources are allocated to maintain a stable and secure ICT environment.

2. Technology Risk Management Policy

Institutions should put in place a comprehensive set of Technology risk management policies that include the following areas:

- Information security classification,
- System development, testing and maintenance,
- IT operation and maintenance,
- Access control,
- Physical security,
- Change controls,
- Personnel security,
- Business Continuity Planning and Crisis and Emergency Management procedure, and
- Management of technology service providers

A bank should review IT control policies regularly, and where necessary updated to accommodate changing operating environments and technologies.

Internal controls related to IT should be structured to ensure that:

- appropriate segregation of duties is monitored,
- records are properly created, transmitted, and stored,
- data are reliable and reporting to management and the board of directors is adequate,
- high-risk conditions, functions and activities are identified and monitored.

3. Technology Risk Identification

Risk identification entails the determination of threats and vulnerabilities to the bank's IT environment which comprises the internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

Humans are significant sources of threats through deliberate acts or omissions which could inflict extensive harm to the organization and its information systems. The bank should be vigilant in monitoring security threats such as those manifested in denial of service attacks, internal sabotage and

malware infestation could cause severe harm and disruption to the operations of a bank with consequential losses for all parties affected.

Vigilant monitoring of these mutating, growing risks is a crucial step in the risk containment exercise.

Both threat-sources and threats must be identified. Threats should include the threat- source to ensure accurate assessment. Some common threat-sources include:

- Natural Threats—floods, earthquakes, hurricanes.
- Human Threats—threats caused by human beings, including both deliberate actions (network based attacks, virus infection, unauthorized access), and unintentional (Inadvertent data entry errors).
- Environmental Threats—power failure, pollution, chemicals, water damage

The risk management function in the institution should compile a list of threats that are present across the institution and use this list as the basis for all risk management activities.

4. Identifying Vulnerabilities

Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, insitutions should start with commonly available vulnerability lists or control areas.

The following tools and techniques are typically used to evaluate the effectiveness of controls, and can also be used to identify vulnerabilities:

- Vulnerability Scanners – software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.

- Penetration Testing – an attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.

- Operational and Management Controls – A review of operational and management controls by comparing the current documentation to best practices and by comparing actual practices against current documented processes.

4.5.5 Risk Assessment, Measurement and Monitoring

1. Risk Assessment

The risk assessment process incorporates specific assessments conducted for functional responsibilities such as security, business continuity, and vendor management.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

A typical risk assessment methodology encompasses the following nine primary steps;

- System Characterization;
- Threat Identification;
- Vulnerability Identification;

- Control Analysis;
- Likelihood Determination;
- Impact Analysis;
- Risk Determination;
- Control Recommendations;
- Results Documentation.

A bank should monitor the risks of the highest severity closely with regular reporting on the actions that have been taken to mitigate them.

To facilitate risk reporting to management, bank should:

- develop IT risk metrics to highlight systems by considering risk events, regulatory requirements and audit observations,
- processes or infrastructure that have the highest risk exposure.

2. Risk Measurement

Institutions should put in place a set of ongoing risk measurement and monitoring mechanisms, which should include:

- Pre and post-implementation review of IT projects;
- Benchmarks for periodic review of system performance;
- Reports of incidents and complaints about IT services;
- Reports of internal audit, external audit, and issues identified by National Bank of Rwanda;
- Arrangement with vendors and business units for periodic review of service level agreements (SLAs);
- The possible impact of new development of technology and new threats to software deployed;
- Timely review of operational risk and management controls in operation area;
- Assessment of the risk profile on IT outsourcing projects periodically.

3. Technology Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk- reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the institution's resources and mission.

Generally, risk mitigation can be achieved through any of the following risk mitigation options:

- Risk assumption - accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk avoidance - avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk limitation – limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
- Risk planning - manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.

- Research and acknowledgment - lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk transference - transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Institutions should therefore implement a comprehensive set of risk mitigation measures complying with the technology risk management policies and commensurate with the risk assessment of the institution. At a minimum the mitigation measures should include:

- A set of clearly documented technology risk policies, technical standards, and operational procedures, which should be communicated to the staff frequently and kept up to date in a timely manner;
- Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring. Also it requires that an appropriate control structure is set up to facilitate checks and balances, with control activities defined at every business level, which should include:
  i. Top level reviews;
  ii. Controls over physical and logical access to data and system;
  iii. Access granted on "need to know" and "minimum authorization" basis;
  iv. A system of approvals and authorizations; and
  v. A system of verification and reconciliation.

4.5.6 Information Security

Institutions should put in place an information and communication security management function to develop and maintain an ongoing information security management program including;

- Promoting information security awareness,
- advising other IT functions on security issues,
- serve as the leader of IT incident response team, and
- report the evaluation of the information security of the institution to the board periodically.

The Information and communication security management program should be documented in an information and communication security policy which should also document the information security standards, strategy, implementation plan, and an ongoing maintenance plan.

The Information security policy should include the following areas:

- ICT security policy management,
- Organization information security,
- Asset management,
- Personnel security,
- Physical and environment security,
- Communication and operation security,
- Access control and authentication,
- Acquirement, development and maintenance of information system,
- Information security event management,
- Business continuity management, and
- Compliance.

4.5.7 Information Classification and Protection

The IT function of nstitutions should oversee the establishment of an information classification and protection scheme. All employees of the institution should be made aware of the importance of ensuring information confidentiality and provided with the necessary training to fully understand the information protection procedures within their responsibilities.

Banks should classify information into different categories according to the degree of sensitivity. Categories might include:

- highly sensitive;
- sensitive;
- internal;
- public.

Banks should develop policies and definitions for each classification and define an appropriate set of procedures for information protection to detect and prevent unauthorized access, copying or transmission of confidential information. The information classification must be consistent across different media, such as paper and electronic media, including back-ups.

Banks should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.

4.5.8 Security Management

1. Authentication and Access Control

In order to restrict access to information and application systems, banks must use an authentication mechanism with access control rules and ensure the following:

a) All users are identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to provide accountability for their activities.
b) Implementation of the effective password rules and enforcement of strong password controls over users' access to applications and systems. Password controls should include a change of password upon first logon, minimum password length and history, password complexity as well as maximum validity period;
c) A system access log which records all attempts to use the system and shows the date and time, codes used, mode of access, data involved and operator interventions. These information should be logged for audit and review purposes;
d) Adoption of a stronger authentication methods for high-risk transactions and activities. These might include smart card or hardware security token and password;
e) that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities;
f) That responsibilities and duties for operating systems function, systems design and development, application maintenance programming, access control administration, data security, librarian and backup data file custody are separated and performed by different groups of employees;
g) Also that any person who needs to access backup files or system recovery resources is duly authorized for a specific reason and a specified time only. The bank should only grant access for a specific purpose and for a defined period and establish audit trials to document its use;
h) Closely supervise the use of and access to privileged accounts. The necessary control procedures include:

- implementing two-factor authentication for privileged users,
- proper safeguard of privileged accounts' passwords (e.g. kept in a sealed envelope and locked up inside the data center),
- change of privileged accounts' passwords immediately upon return by the requesters,
- instituting strong controls over remote access by privileged users,
- maintain audit logging of system activities performed by privileged users,
- disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring.

Banks must timely review and removal of user identity from the system should be implemented when a user transfers to a new job or leaves the institution.

The following controls should be put in place:

i. Physical Security Zones

Banks should ensure all physical security zones, such as computer centres or data centres, network closets, areas containing confidential information or critical IT equipment, and respective accountabilities are clearly defined, and appropriate preventive, detective, and curative control measures are put in place.

ii. Logical Security Domains

Banks should divide their networks into logical security domains (hereinafter referred to as the "domain") with different levels of security. The following security factors have to be assessed in order to define and implement effective security controls, such as physical or logical segregation of network, network filtering, logical access control, traffic encryption, network monitoring, activity log, for each domain and the whole network:

- Criticality of the applications and user groups within the domain;
- Access points to the domain through various communication channels;
- Network protocols and ports used by the applications and network equipment deployed within the domain;
- Performance requirement or benchmark;
- Nature of the domain, i.e. production or testing, internal or external;
- Connectivity between various domains; and
- Trustworthiness of the domain.

2. Operating System and System Software

Banks should secure the operating system and system software of all computer systems by:

- Developing baseline security requirement for each operating system and ensuring all systems meet the baseline security requirement;
- Clearly defining a set of access privileges for different groups of users, namely, end- users, system development staff, computer operators, and system administrators and user administrators;
- Setting up a system of approval, verification, and monitoring procedures for using the highest privileged system accounts;

- Requiring technical staff to review available security patches, and report exceptions in the patch status to Head of IT periodically; and
- Requiring technical staff to include important items such as unsuccessful logins, access to critical system files, and changes made to user accounts in system logs monitor the systems for any abnormal event manually or automatically, and report the monitoring periodically;
- Putting in place adequate controls such as:
  - prohibiting the download and use of unauthorized files and software, and the access to doubtful web sites;
  - installation and timely update of anti-virus software provided by reputable vendors;
  - disallowing the download of executable files, and small programs automatically downloaded from web sites by browsers for execution, especially those with known vulnerabilities (e.g. through the use of corporate firewalls and proper configuration of the browser software);
  - prompt and regular virus scanning of all computing devices and procedures for recovering from virus infections.

3. Application Software

Banks should ensure the security of all the application software by:

- Clearly defining the roles and responsibilities of end-users and IT staff regarding the application security;
- Implementing a robust authentication method commensurate with the criticality and sensitivity of the application system;
- Enforcing segregation of duties and dual control over critical or sensitive functions;
- Requiring verification of input or reconciliation of output at critical junctures;
- Requiring that the input and output of confidential information are handled in a secure manner to prevent theft, tampering, intentional leakage, or inadvertent leakage;
- Ensuring the system can handle exceptions in a predefined way and provide meaningful messages to users when the system is forced to terminate;
- Maintaining audit trail in either paper or electronic format.
- Requiring the user administrator to monitor and review unsuccessful logins and changes to user accounts.

4.5.9 Audit Trail

Institutions should have a set of policies and procedures controlling the logging of activities in all production systems to support effective auditing, security forensic analysis, and fraud prevention. Logging can be implemented in different layers of software and on different computer and networking equipment, which falls into two broad categories:

- Transaction journals are generated by application software and database management system, and contain authentication attempts, modification to data and error messages. Transaction journals should be kept according to the information retention policy legally stipulated in the country.
- System logs are generated by operating systems, database management system, firewalls, intrusion detection systems, and routers, etc. and contain authentication attempts, system events, network events and error messages. System logs should be kept for a period proportionate to the risk classification, but not less than one year.

- Banks should ensure that sufficient items are captured in the logs to facilitate effective internal controls, system trouble shooting, and auditing while taking appropriate measures to ensure time synchronization on all logs. Sufficient disk space should be allocated to prevent logs from being overwritten. System logs should be reviewed for any exception. The review frequency and retention period for transaction logs or database logs should be determined jointly by ICT function and pertinent business lines, and approved by the IT Steering Committee.

4.5.10 Encryption Technologies

Institutions should have the capacity to employ encryption technologies to mitigate the risk of losing confidential information in the information and communication systems or during its transmission. Appropriate management processes of the encryption facilities should be put in place to ensure that:

- Encryption facilities in use should meet international security standards or requirements;
- Staff in-charge of encryption facilities are well trained and vetted. This is verified through professional and academic testimonials, character reference from independent referees, certificates of good conduct;
- Encryption strength is adequate to protect the confidentiality of the information;
- Effective and efficient key management procedures, especially key lifecycle management and certificate lifecycle management, are in place.

4.5.11 Computing Equipment

Banks must put in place an effective and efficient system of securing all end-user computing equipment which include desktop personal computers (PCs), portable PCs, teller terminals, automatic teller machines (ATMs), passbook printers, debit or credit card readers, point of sale (POS) terminals, personal digital assistant (PDAs), tablet devices and smartphones, and conduct periodic security checks on all IT equipment.

With regard to end-user computing, banks should putting in place adequate controls such as:

- prohibiting the download and use of unauthorized files and software, and the access to doubtful web sites;
- installation and timely update of anti-virus software provided by reputable vendors;
- disallowing the download of executable files, and small programs automatically downloaded from web sites by browsers for execution, especially those with known vulnerabilities (e.g. through the use of corporate firewalls and proper configuration of the browser software);
- prompt and regular virus scanning of all computing devices and procedures for recovering from virus infections.

4.5.12 Handling Consumer Information

Institutions should put in place a set of policies and procedures to govern the collection, processing, storage, transmission, dissemination, and disposal of customer information.

4.5.13 Training

All employees, including contract staff, should be provided with the necessary training to fully understand the bank ICT policies, procedures and the consequences of their violation. Banks should adopt a zero tolerance policy against ICT security violation.

4.5.14 System Acquisition, Development, Testing and Maintenance

1. System Development

- Banks should have the capability to identify, plan, acquire, develop, test, deploy, maintain, upgrade, and retire information systems.
- Policies and procedures should be in place to govern the initiation, prioritization, approval, and control of ICT projects.
- Progress reports of major ICT projects should be submitted to and reviewed by the ICT Steering Committee periodically.
- Decisions involving significant change of schedule, change of key personnel, change of vendors, and major expenditures should be included in the progress report.

2. Project Risks

Institutions should recognize the risks associated with ICT projects, which include the possibilities of incurring various kinds of operational risk, financial losses, and opportunity costs stemming from ineffective project planning or inadequate project management controls of the bank. Therefore, appropriate project management methodologies should be adopted and implemented to control the risks associated with IT projects.

3. System Development Methodology

Institutions should adopt and implement a system implementation methodology to control the life cycle of Information systems. The typical phases of system life cycle include system analysis, design, development or acquisition, testing, trial run, deployment, maintenance, and retirement. The system implementation methodology to be used should be commensurate with the size, nature, and complexity of the ICT project.

4. Reliability, Integrity, and Relevance

Institutions should ensure system reliability, integrity, and relevance by controlling system changes with a set of policies and procedures, which should include the following elements:

- Ensure that production systems are separated from development or testing systems;
- Separating the duties of managing production systems and managing development or testing systems;
- Prohibiting application development and maintenance staff from accessing production systems under normal circumstances unless management approval is granted to perform emergency repair, and all emergency repair activities should be recorded and reviewed promptly;
- Progressing changes of ICT system configuration from development and testing systems to production systems should be jointly approved by the ICT function and business lines, properly documented, and reviewed periodically.

5. Data Integrity, Confidentiality, and Availability

Institutions should have in place a set of policies, standards, and procedures to ensure data integrity, confidentiality, and availability. These policies should be in accordance with relevant laws and regulations and latest international data integrity and information security standards.

6. System upgrade

Institutions should have a set of policies and procedures controlling the process of system upgrade. The underpinning software, namely, operating system, database management system, middleware, has to be upgraded, or the application software has to be upgraded. The system upgrade should be treated as a project and managed by all pertinent project management controls including user acceptance testing.

4.5.15 IT Operations

1. Physical and Environmental Controls

Banks must consider fully the environmental threats (e.g. fire, proximity to natural disaster zones, dangerous or hazardous facilities or busy/major roads, extreme temperature, water and dust) when selecting the locations of their data centres. Physical and environmental controls must be implemented to monitor environmental conditions that could affect adversely the operation of information processing facilities. Equipment facilities must be protected from power failures and electrical supply interference by installing backup power consisting uninterruptible power supplies, battery arrays, and/or standby diesel generators.

The bank should employ physical, human and procedural controls such as the use of security guards, card access systems, mantraps and bollards for accessing the data center, where appropriate.

2. Access by Third-party Personnel

In controlling access by third-party personnel (e.g. service providers) to secured areas, proper approval of access should be enforced and their activities should be closely monitored. It is important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for permanent and temporary technical staff and contractors.

3. Segregation of Duties

Institutions should separate ICT operations or computer center operations from system development and maintenance to ensure segregation of duties within the ICT function. The Institutions should document the roles and responsibilities of data center functions.

4. Documentation of operational instructions

Institutions should detail operational instructions such as computer operator tasks, job scheduling and execution in the IT operations manual. The IT operations manual should also cover the procedures and requirements for on-site and off-site backup of data and software in both the production and development environments (i.e. frequency, scope and retention periods of back-up).

5. Problem management

Institutions should have in place a problem management and processing system to respond promptly to IT operations incidents, to escalate reported incidents to relevant ICT management staff and to record, analyze and keep track of all these incidents until rectification of the incidents and the causes analysed. A helpdesk function should be set up to provide front-line support to users on all technology-related problems and to direct the problems to relevant IT functions for investigation and resolution.

6. System monitoring

Institutions should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The

performance monitoring process should include forecasting capability to enable exceptions to be identified and corrected before they affect system performance.

7. Capacity plan

Institutions should develop a capacity plan to cater for business growth and transaction increases due to changes of economic conditions. The capacity plan should be extended to cover back-up systems and related facilities in addition to the production environment.

8. Record keeping

Institutions should ensure the continued availability of technology related services with timely maintenance and appropriate system upgrades. Proper record keeping (including suspected and actual faults and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance.

9. Change management

Institutions should have an effective change management process in place to ensure integrity and reliability of the production environment. Institutions should develop a formal change management process.

4.5.16 Business Continuity Management

1. BCP plans

Institutions should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption in IT. These arrangements should be regularly updated and tested to ensure their effectiveness.

2. Documentation

Institutions should document their strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy.

4.5.17 Outsourcing

1. Supervisory Duties

Institutions should not contract out their obligations to regulatory authorities and should take reasonable care to supervise the discharge of outsourced IT functions.

2. Critical IT Functions

Institutions should take particular care to manage material outsourcing arrangement (such as outsourcing of data center, IT infrastructure, etc.), and should seek approval to National Bank of Rwanda when they intend to enter into such material outsourcing arrangement.

3. Risk Analysis

Before entering into, or significantly changing, an outsourcing arrangement, the bank should:

- Analyze how the arrangement will fit with its IT organization and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
- Consider whether the arrangements will allow it to monitor and control its operational risk exposure relating to the outsourcing;
- Conduct appropriate due diligence of the service provider's financial stability, expertise and risk assessment of the service provider, facilities and ability to cover the potential liabilities;

- Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and
- Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms.

4. Data Security

Institutions should enhance the management of IT-related outsourcing by putting in place measures to ensure data security of sensitive information such as customer information. Such measures include;

- Ensure that there is clear separation between outsourced information and other information handled by the service provider;
- The staff of the service provider should be authorized on "need to know" and "minimum authorization" basis;
- Ensure that service provider guarantees that its staff meet the confidential threshold required;
- Ensure all related sensitive information are deleted from the service provider's storage when terminating the outsourcing arrangement.

5. Contingency Plan

The institution should ensure that it has appropriate contingency plans in the event of a significant loss of services from the service provider. Particular issues to consider include a significant loss of resources, turnover of key staff, or financial failure of, the service provider, and unexpected termination of the outsourcing agreement.

4.5.18 Internal Control and Audit

1. Systems Audit

Depending on the nature, scale and complexity of their business, it may be appropriate for institutions to combine their internal systems audit with the internal audit function. However, institutions that have capacity and the relevant competences are advised to separate systems audit from internal audit function.

The internal audit function should be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the institution and have appropriate access to the institution's records.

2. Role of Internal Audit

Whether performed by a separate specialized IT audit function or as a function within the internal audit, the responsibilities of the IT audit function are:

- To establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the institution's systems and internal control mechanisms and arrangements;
- To issue recommendations based on the result of work carried out;
- To verify compliance with those recommendations;
- To carry out special audit on the information system. This involves investigating, analyzing and reporting on the information system as a result of an information security incident or from a risk assessment report by the internal audit or risk management function.

3. Frequency of IT Internal Audit

Based on the nature, scale and complexity of its business, deployment of information and communication technology and Technology risk assessment, institutions should determine the scope

and frequency of IT internal audit. However, a comprehensive IT internal audit shall be performed at a minimum once every **2 years**.

4. Implementing System Development

Institutions should engage their Internal Audit and Risk Management functions when implementing system development of significant size and scale to ensure it meets the IT Risk standards of the institution.

4.5.19 IT External Audit

The IT external audit should at minimum cover the following aspects:

- Risk assessment of the IT systems.
- Review of the IT Policies, strategy and direction.
- Business continuity management program.
- Systems change control process.
- Reporting, logging and auditability of the systems.
- Input-process-output controls.
- Adequacy of identification and authentication system.
- Protection against malicious malware.
- Operations and network management.

Institutions should ensure that the IT external auditor reviews and examines institutions hardware, software, documentation and data to identify all potential IT risks.

Institutions should ensure that the IT external auditors strictly comply with the law and regulations by maintaining the confidentiality of private information accessed while conducting the IT audit. IT audits may be carried out by external auditors or specialized firms and should be conducted at least once every two years.

4.6 STRATEGIC RISK MANAGEMENT

4.6.1 Introduction

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. It is a risk that could significantly impact on the achievement of the institution's vision and strategic objectives as documented in the strategic plan.

This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.

The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities.

In strategic management, the organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental.

Strategic risk management is the process of identifying, assessing, measuring, monitoring and managing the risk in the institution's business strategy. Strategic risk management involves evaluating how a wide range of possible events and scenarios will affect the strategy and its execution and the ultimate impact on the institution's value.

4.6.2 Board & Senior Management Oversight

1. **Specific responsibilities for the Board**

The Board has specific responsibilities for overseeing an institution's strategic risk management process. These includes:-

- Ensuring that risk management practices are an integral part of strategic planning;
- Ensuring that the institution has in place an appropriate strategic risk management framework which suits its own circumstances, business needs and risk tolerance;
- Ensuring that the institution's strategic goals and objectives are clear and are set in line with its corporate mission and values, culture, business direction and risk tolerance;
- Approving the institution's strategic plan (including strategies contained therein) and any subsequent changes, and reviewing the plan (at least annually) to ensure its appropriateness;
- Ensuring that the institution's organization structure, culture, infrastructure, financial means, managerial resources and capabilities, as well as systems and controls are appropriate and adequate to support the implementation of its strategies; Reviewing high-level reports periodically submitted to the Board on the institution's overall strategic risk profile;
- Ensuring that any material risks and strategic implications identified from those reports are properly addressed; and
- Ensuring that senior management is competent in implementing strategic decisions approved by the Board, and supervising such performance on a continuing basis.

2. Specific responsibilities of senior management

In ensuring effective strategic risk management within an institution, senior management should, among other things:

- Establish and implement the institution's strategic risk management framework based on criteria and standards set by the Board;
- Assist the Board in developing strategies to meet the institution's strategic goals and objectives;
- Formulate the institution's strategic plan and related implementation plans (such as business, development and operating plans);
- Ensure adequate implementation of the institution's strategic plan, as approved by the Board;
- Implement an effective performance evaluation system;
- Ensure that any strategic issues and material risks arising from environmental changes or implementation of the institution's strategies are reported to the Board on a timely basis.

4.6.3 Policies, Procedures & Limits

Effective management of strategic risk requires that policies, procedures and limits be established to ensure objective evaluation of and responsiveness to a bank's business environment. Policies on business strategy are critical in defining the business segments that the institution will focus on, both in the short and long run. There should be clear guideline on frequency and procedure for review of the institution's business strategy.

Procedures for defining and reviewing the institutions' business strategy are intended to ensure that the following aspects are given adequate consideration:

- The institution's inherent strengths;
- Its identified weaknesses;

- Opportunities external to the institution;
- External factors that pose threats to the institution.

Limits are necessary in defining:

- Exposure to different sectors;
- Growth of business and staff strength;
- Network expansion program.

4.6.4 Strategic risk management process

An effective strategic management process should include the following:

1. Strategic Planning

Strategic planning is the process whereby an institution determines the overall direction and focus of their organization, establish medium and long-term priorities in line with their corporate mission and goals, and translate those priorities into appropriate strategies for achieving stated goals and objectives. This process culminates in the development of a strategic plan. Strategic planning provides a process for institutions to identify and assess potential risks posed by their strategic plan, and consider whether they have adequate capacity to withstand the risks. It also facilitates institution in responding on a timely basis to any adverse changes in circumstances (whether internal or external) that may undermine the achievement of their plan or affect their future development.

A strategic planning process has three basic elements

- A process to set strategic goals and objectives,
- A process to evaluate the institutions strategic position and develop appropriate strategies, and
- A process to translate those strategies into action plans.

2. Setting of Strategic goals and objectives

In setting strategic goals and objectives, institutions should be guided by their corporate mission which outlines the broad directions that the institution is to follow, and reflect the vision and values upheld by the institution. Strategic goals generally reflect an institution's aspirations in relation to achieving growth and return, efficiency, and competitive advantage within the environment it operates.

In setting strategic goals and objectives, institutions should identify and take into account the needs and aspirations of their major stakeholders and changes in operating environment (eg. political, legal, economic, social and technological changes).

3. Development of strategies

Institutions should have a process for evaluating their strategic position and developing appropriate strategies to achieve their strategic position and developing appropriate strategies to achieve their strategic goals and objectives.

The process involves understanding of the general banking, business and economic environment that an institution operates in, assess its strength and weaknesses and analyze its position and possible strategies that can be considered having regards to its stated goals and objectives and risk tolerance.

4. Formulation of strategic plan

Institutions should have a process for formulating and approving the strategic plan. This process and all related procedures, including the responsibilities of the Board and senior management and other staff concerned, should be clearly documented, approved by the Board, and subject to periodic review to ensure their appropriateness.

Strategic decisions agreed upon during the planning process should form the basis of the strategic plan. Apart from describing what strategies the institution will take and how the institution will implement them to meet its strategic goals and objectives, the plan may also provide other information, such as the institution's philosophy towards its business, its growth targets, the extent of its financial risk-taking, and other relevant factors (institutional and environmental) affecting its growth and development. The depth and coverage of the strategic plan should be commensurate with the institution's scale and complexity of business.

In the case of a local banking group with regional presence, the strategic plan should be prepared on a consolidated basis (i.e. including the positions of subsidiaries and overseas branches).

Institutions, which are branches or subsidiaries of a foreign bank, should have their own strategic plan for strategic risk management purposes if the group's strategic plan is not adequate to fully reflect their local situation, needs and activities.

5. Alignment and change management

Before implementing their strategies, institutions should ensure that they have made proper alignment of internal resources and processes and, if necessary, managed all change issues (such as those arising from organizational or cultural changes) to facilitate the achievement of desired outcomes. Interdependencies between processes across departments (e.g. reconciliation of transaction information between front and back offices using a more advanced IT system) should also have been addressed so that they can be properly understood and accounted for during the implementation.

Ensuring proper alignment of internal resources and processes means, for example, checking to see whether:

- sufficient resources (financial and non-financial) have been allocated to undertake the necessary tasks;
- the right people have been put in the right place; and
- the organization and risk management structure, systems, infrastructure and technology are in the right shape to support the new initiatives.

4.6.5 Measuring and Monitoring Strategic Risk

In order to ensure an effective strategic risk management process, every institution shall deploy an integrated management information system that enables management monitor:

- Current and forecasted economic conditions, (e.g. economic growth, inflation, foreign exchange trends, etc.);
- Current and forecasted industry and market conditions, such as:
  - Increasing competition by new market entrants;
  - Number and size of mergers and acquisitions;
  - Changing customer behavior;
  - New products/substitutes;

- Exposure to different sectors, and associated sector risks

- Exposure to different sectors, and associated sector risks

1. Performance evaluation and feedback

Comparison of actual performance to desired outcomes serves as an important check on the success of implementing approved strategies, and allows management to take timely remedial actions to address significant deviations from set targets. Therefore, institutions are expected to develop a performance evaluation system that tracks progress towards achieving both financial and non-financial targets.

In order to ensure efficient and continuous performance evaluation, at the setting of strategic goals and targets stage, long term goals and targets should be broken down in short term (preferably yearly) measurable goals and targets.

2. Other Supporting Processes

a) Planning and Management of Capital and Funding needs

Inadequate planning of capital and funding needs is an obstacle to implementing strategic decisions and can have a disruptive effect on an institution operations and its ability to meet strategic goals and objectives. As such, institutions should view such planning as a crucial element of the strategic planning process.

Capital planning should be risk-based and forward-looking, and take into account such factors as an institution's current and future capital needs, anticipated capital expenditures, dividend payment forecasts, desirable capital levels, and external capital sources (e.g. available supply of capital and capital raising options).

b) Management Information System

In a competitive banking environment, the ability to effectively manage information is crucial to an institution's ability to remain competitive, introduce new products and services, and achieve desired goals. Institutions should therefore ensure that they have sufficient and robust MIS to support their strategic planning and decision making processes.

c) Human resources management and development

Human resources management has a strategic focus in that it is involved in gaining commitments to an institution's goals and shaping its corporate culture. By developing policies to meet future needs, human resources management enables the adoption of a forward-looking approach to deal with change and growth and to anticipate future problems.

d) Succession Planning

The institution's management should develop management succession plans to cater for staff turnover and retirement. This is particularly essential for banks to cater for major turnover in senior and middle management, whether due to transfer, resignation or retirement.

The institutions' board of directors should also maintain succession plans for critical positions such as Chairman of the Board and the institution's Chief Executive Officer.

4.6.6 Internal Controls and Audit

Institutions need strong internal control systems to ensure that they are not unduly exposed to strategic risks. Internal controls are required to ensure that:

- The organization structure establishes clear lines of authority;
- The institution's systems and structures provide for business continuity planning;
- The process of setting up and reviewing strategic plans and comprehensive and is carefully adhered.

The results of such audit reviews, including any issues and weaknesses identified should be reported to the Board and senior management directly. Both the Board, and a delegated committee (e.g. Board Audit Committee), and senior management should be sufficiently engaged in the process to determine whether such reviews and audits are effectively performed (e.g. whether the performing staff are independent and have sufficient authority to perform their duties) and identified issues are addressed.

4.7. LEGAL AND COMPLIANCE RISK MANAGEMENT

4.7.1 Introduction

Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, prudential guidelines, supervisory recommendations and directives, rules, related self-regulatory standards and codes of conduct applicable to its bank activities.

Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to staff members.

In addition to the legal and regulatory framework put in place by the home regulatory agencies, institutions operating across borders must also ensure compliance with the applicable legal and regulatory requirements in the other jurisdictions they conduct business.

4.7.2 Impact of Compliance Risk

Non-compliance with the legal and regulatory framework exposes an institution to payment of fines, penalties, damages, and the violation of contracts. It can also lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential and an inability to enforce contracts. Furthermore, public knowledge of legal and regulatory violations can cause substantial harm to a bank's reputation contributing to a loss of public confidence.

4.7.3 Compliance risk management framework

The risk management framework for compliance risk must include: board and senior management oversight, policies and procedures, MIS and an independent review.

1. **Board and senior management oversight**

The Board is responsible for overseeing the management of the bank's compliance risk. The board shall approve the institution's compliance policy, including a formal document establishing a permanent and effective compliance function. The board shall regularly assess the extent to which the institution is managing its compliance risk.

a) Specific responsibilities of the Board

Effective Board oversight is the cornerstone of an effective compliance risk management process. The Board shall understand the nature and level of compliance risk to which the bank is exposed and how its risk profile fits within the overall business strategy.

The responsibilities of the board of directors shall encompass the following:

- defining the compliance risk management system and ensuring that the system is aligned with overall business activities;
- approving the bank's compliance policy including a formal document establishing a permanent and effective compliance function;
- reviewing the extent to which the bank is managing its compliance risk;
- oversee the implementation of the compliance policy including ensuring that compliance issues are resolved effectively and expeditiously; and
- ensuring that management takes steps necessary measures to identify measure, monitor and control compliance risk.

b) Specific responsibilities of senior management

Senior management is responsible for the effective management of a bank's compliance risk. As such, senior management is responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff and explains the main processes by which compliance risks are to be identified and managed at all levels of the organization.

Senior management shall, with the assistance of the compliance function:

- identify and assess the main compliance risk issues facing the institution and plans to manage any shortfalls as well as the need for any additional policies or procedures to deal with new compliance risks;
- ensure that the institution's compliance risk management framework has clear lines of authority, reporting and communication;
- periodically report to the board of directors or a committee of the board on management of compliance risk;
- report promptly to the board of directors or a committee of the board on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss or loss to reputation);
- ensure that there is sufficient depth and skill in staff resources to manage legal and compliance risk;
- provide reasonable assurance, through the audit function, that all activities and all aspects of legal and compliance risk are covered by the institution's risk management process;
- at least once a year conduct a compliance risk assessment, and;
- periodically review the organization's compliance risk management framework to ensure that it remains appropriate and sound;

The board and senior management should ensure that there is an effective, integrated compliance risk management framework. This includes establishment of an independent compliance function.

c) Organization of Compliance Function

All instutitions shall establish an independent compliance function which facilitates efforts to comply with legal and regulatory requirements by tracking and documenting compliance. The function should also be sufficiently resourced and its responsibilities should be clearly specified.

The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is therefore, expected that where compliance staff perform non- compliance tasks, institutions ensure that conflict of interest is avoided.

The Compliance Function shall have the following characteristics:

- a formal status within the institution;
- a head of compliance with overall responsibility of co-ordinating the management of the institution's compliance risk;
- Compliance function staff placed in positions where there is no possible conflict of interest between their compliance responsibilities and any other responsibilities they may have;
- Staff shall have access to information and personnel necessary to carry out their responsibilities.

The Compliance Function shall be sufficiently and appropriately resourced with compliance staff having the requisite qualifications, experience and professional qualities to enable them carry out their specific duties.
The organization and structure of the Compliance Function and its responsibilities shall be consistent with applicable laws and regulations in all jurisdictions in which they conduct business.

To give the Compliance Function its appropriate standing, authority and independence, the following issues with regard to the function shall be addressed either in the bank's compliance policy or in any other formal document and communicated to all staff:

- Its roles and responsibilities, to ensure its independence and its relationship with other risk management functions within the institution and with the internal audit function;
- In cases where compliance responsibilities are carried out by staff in different departments, to determine how responsibilities are to be allocated among the departments;
- Its right to obtain access to information necessary to carry out its responsibilities and the corresponding duty of the institution's staff to co-operate in supplying the information;
- Its right to conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform this task if appropriate;
- Its right to be able to freely express and disclose its findings to senior management and the Board of directors;
- Its formal reporting obligations to the board of directors or a committee of the board

d) Compliance Function responsibilities

The function's responsibilities are to assist senior management to effectively manage the institution's risk. This includes advising senior management on compliance laws, rules and standards, developments in the area, educating staff on compliance issues and acting as a contact point for compliance queries from staff. The allocation of responsibilities to each department shall be clear.

The responsibilities of the Compliance Function shall be carried out under a risk based compliance program that sets out its planned activities, and is subject to oversight by the Head of Compliance to ensure appropriate coverage across businesses and coordination among risk management functions.

Specific tasks of the Compliance Function may be outsourced e.g. the interpretation of laws and regulations but they must remain subject to appropriate oversight by the Head of Compliance. Regardless of the extent to which specific tasks of the Compliance Function are outsourced, the board of directors and senior management remain responsible for the institution's compliance management process.

e) Head of Compliance

Each bank shall have a Head of Compliance with overall responsibility for co- coordinating the identification and management of the institution's compliance risk and for supervising the activities of other compliance staff.

2. Policies and Procedures

Banks must have policies, processes and procedures to control or mitigate compliance risks. Authority and accountability for compliance must clearly defined and enforced.

An institution's compliance policy must explain the main processes by which compliance risk is to be identified and managed through all levels of the institution's organizational structure. The policy should also define the compliance function as an independent function, with specific roles and responsibilities of the compliance staff, and detailing the compliance officer's communication methods with the management and staff in the various business units.

Compliance risk management policy must be part of the overall risk management policy of the institution, and should precisely determine all important processes and procedures in minimizing the institution's compliance risk exposure. The policy should be clearly formulated and in writing. The policy must contain, at least the following:

- Definition of compliance risk;
- Objectives of compliance risk management;
- Procedures for identifying, assessing, monitoring, controlling and managing Compliance risks;
- Well defined authorities, responsibilities and information flows for compliance risk Management at all management levels; and
- Clear statement of the banks accepted tolerance for compliance risk exposure.

3. Measuring, Monitoring, Control and reporting of Compliance Risk

The compliance function shall on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships.

The compliance function should also report to the National Bank of Rwanda the compliance status as required from time to time.

The function shall consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. The Compliance Function shall also assess the appropriateness of the bank's compliance procedures and

guidelines, promptly follow up any identified deficiencies, and where necessary, formulate proposals for amendments.

Banks shall have in place a system that ensures that deficiencies identified by the compliance function are promptly managed and meaningful corrective action implemented. Training programs shall include developments in the legal and regulatory frameworks to ensure that control of compliance risk is effective. All the necessary resources should be provided to support the compliance function.

Banks' management shall show preparedness towards anticipation of compliance risk and ability to respond well to changes in the market, technology or regulatory framework.

The Compliance Function shall monitor and test compliance by performing sufficient and representative compliance testing. The results of the testing shall be reported up through the Compliance Function reporting line in accordance with the bank's internal risk management procedures.

The head of compliance shall report on a quarterly basis to the board on compliance matters with reports referring to the compliance risk assessment that has taken place during the reporting period including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarized identified breaches and/or deficiencies, corrective measures recommended to address them and corrective measures already undertaken.

4. Management Information System

Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc). The institution's management information systems should therefore be sound to be able to capture aspects of non-compliance. This is possible when the bank have a strong control culture. Compliance considerations should be incorporated into product and system development and modification processes, including changes made by outside service providers or vendors.

4.7.4 Internal Controls

An effective system of internal control for compliance risk shall include appropriate reporting lines, segregation of duties, periodic testing of the control framework, reporting of compliance testing exceptions and independence of the compliance function.

4.7.5 Independent review

The Compliance Function shall be subject to periodic review by the Internal Audit Function. Compliance risk shall be included in the risk assessment methodology of the Internal Audit Function and an audit program that covers the adequacy and effectiveness of the bank's Compliance Function shall be established, including testing of controls commensurate with the perceived level of risk.

This implies that the compliance and audit function shall be separate and there shall be a clear understanding within the bank as to how risk assessment and testing activities are divided between the compliance and audit functions and shall be documented.

The Audit Function shall keep the Head of Compliance informed of any audit findings related to compliance.

4.8 COUNTRY AND TRANSFER RISK MANAGEMENT

4.8.1 Introduction

1. Background

- When an institution engages in international lending, establishes a subsidiary or a branch in a foreign country or incurs a cross-border exposure, it is exposed to not only customary credit risk but also country risk. Country risk is the primary factor that differentiates international lending from domestic lending. It encompasses all the uncertainties arising from the economic, social and political conditions of a country that may cause borrowers in that country to be unable or unwilling to fulfil their external obligations.

- Country risk may arise from deteriorating economic conditions, political and social upheavals, nationalization or expropriation of assets, government repudiation of external indebtedness, exchange controls and currency devaluation.
- Country risk is a special form of risk over which institutions can exercise little direct influence. Institutions should therefore ensure that they have adequate systems and expertise to manage their cross-border exposures and avoid taking undue concentration risks on such exposures.

- The level of sophistication of an institution's country risk management system should be commensurate with the size, nature and complexity of its cross-border exposures.

2. Definitions

Country risk is the risk that economic, social, and political conditions and events in a foreign country will adversely affect an institution's financial condition. For example, financial factors such as currency controls, devaluation or regulatory changes, or stability factors such as mass riots, civil war and other potential events that contribute to institutions' operational risks.

In addition to the negative effect that deteriorating economic conditions and political and social unrest may have on the rate of default by obligors in a country, country risk also includes the possibility of nationalization or expropriation of assets, government repudiation of external indebtedness, sudden changes in exchange control policies, and currency depreciation or devaluation.
Transfer risk is the risk that a borrower may not be able to secure foreign exchange to service its external obligations. Where a country suffers economic, political or social problems, leading to drainage in its foreign currency reserves, the borrowers in that country may not be able to convert their funds from local currency into foreign currency to repay their external obligations.

3. Types of country and transfer risk

Banks should be aware of the different types of country risk to which they may be exposed. The following are the types:

- Sovereign risk denotes a foreign government's capacity and willingness to repay its direct and indirect (i.e. guaranteed) foreign currency obligations.
- Contagion risk arises where adverse developments in one country lead to a downgrade of rating or a credit squeeze not only for that country but also other countries in the

region, notwithstanding that those countries may be more creditworthy and that the adverse developments do not apply to them.

- Currency risk - the risk that a borrower's domestic currency holdings and cash flow become inadequate to service its foreign currency obligations because of devaluation;
- Indirect country risk – the risk that the repayment ability of a domestic borrower is endangered owing to the deterioration of the economic, political or social conditions in a foreign country where the borrower has substantial business relationship or interests.
- Macroeconomic risk – the risk that the borrower in a country may, for example, suffer from the impact of high interest rates due to measures taken by the government of that country to defend its currency.

4.8.2 Board and Senior Management Oversight

The board and senior management are responsible for defining the level of country and transfer risk the institution can undertake and to ensure that the institution has an effective risk management framework consistent with the level of the institution's cross-border exposure. Towards this end, the board should ensure that there are well-defined policies, procedures and processes to identify measure, evaluate, monitor, report and control or mitigate country and transfer risk.

4.8.3 Policies and Procedures

Banks (having significant cross-border exposure) should have adequate policies and procedures for identifying, monitoring and controlling country risk and transfer risk in their international lending and investment activities and for maintaining appropriate reserves against such risks. The details to be included in the policy, and any procedures drawn up in respect of them, depend on the nature and scope of a bank's cross-border activities.
Generally, banks must set out the business strategy in overseas countries, the parameters under which such business is carried out, its risk appetite and risk tolerances in the light of available financial resources, staff skills and systems for country risk identification, measurement, monitoring, reporting and provisioning.

The policies and any corresponding procedures would normally include, but not limited to the following the following:

- Clear lines of authority (including approval of cross-border lending and exceptions), responsibility and accountability for country risk management;
- Types of country risk which may be incurred by the institution and the policies and procedures for managing them (in particular whether the institution's country risk management process is centralized or decentralized and integrated with the overall credit risk management);
- The overall limits and sub-limits for cross-border exposures;
- The standards and criteria which the institution will use to analyze the risk of particular countries;
- The internal country rating system, if any, or how the country risk elements are factored into the institution's existing loan classification system;
- The method to be used in measuring country risk exposures;
- The country risk provisioning policy and methodology;
- Types of and criteria for acceptable collateral and guarantees, financial instruments and

hedging strategies (e.g. credit derivatives or netting arrangements) which are allowed to be used for the mitigation of country risk and the requirements for perfection of collateral;

- The minimum standard terms and conditions to be incorporated in loan documentation in accordance with the legal requirements of each country;
- The requirement for registration, if applicable, of credit granted and guarantees accepted, noncompliance with which may render the exposure or guarantee not legally enforceable by the institution;
- Lists of designated lawyers for evaluating the legitimacy of documentation and perfection of collateral;
- Procedures for dealing with deteriorating situations in a country, with clear contingency plans and exit strategies; and
- Types of management reports on country and transfer risk.

The policy should be reviewed at least annually to determine if it is still appropriate for the bank's business and compatible with changing market conditions.

Senior management is responsible for monitoring implementation of the policy and developing detailed procedures where necessary to supplement the policy.

4.8.4 Measurement and Monitoring of Country Risk

Each bank must be in a position to identify country risk exposure and monitor the performance of these positions. Systems for measuring country exposure need to be tailored according to the size and complexity of the bank's international lending and investing operations. The objective is to maintain a system comprehensive enough to capture all significant exposures and detailed enough to permit adequate analysis of different types of risk.

1. Measurement System

Banks need to develop country risk measurement system framework which:

a) Makes Allowance for Risk Allocation.

Banks exposed to country and transfer risk should be able to determine where the final risk lies. In addition to allocating each claim according to the residence of the borrower, it will also be necessary to consider how to take into account additional factors which in practice may give the institution a claim on a resident of a different country. The institution's system should therefore be capable of assessing the exposure by country of the borrower and make an allowance for risk transfers.

b) Ensures Consolidation

Banks should measure country and transfer risk on a consolidated basis in order to obtain a picture of overall exposure to foreign borrowers outside its own operations. Consolidation embraces the operations of the institution's branches, subsidiaries, other related institutions and any other institution that assists in the management of overall exposure to country risk. In addition to measuring its country exposure on a consolidated basis, the institution should also take account of the gross country exposure arising from the funding of its individual overseas branches and subsidiaries.

c) Capture the Breakdown and Analysis of Claims by Borrowing Country.

Country exposure consists of all assets including loans, acceptances, placements, securities, etc., which represent claims on residents of another country. A breakdown of residual maturity of claims will assist in providing a comprehensive maturity profile of indebtedness. Additional breakdowns, for example, distinguishing between claims on sovereign borrowers, banks and others, will also assist the bank's management to assess the its country exposure.

Deposits from a country should not ordinarily be offset against credits to that country unless the institution has established a legal right of set-off vis-à-vis the same customer. Some potential claims that may involve risk include letters of credit and legally binding commitments to lend to foreign clients. Fiduciary operations should also be considered where the institution acts as an agent, which may give rise to country exposure.

Banks with considerable foreign exposure and considerable country risk have to periodically review the influence of potential credit deterioration, or payment problems of specific countries or groups of countries, on their statement of financial position and statement of comprehensive income. The findings must be brought to the attention of the senior management officers responsible.

d) Monitoring and reporting

Banks with significant cross-border operations must have robust systems for monitoring economic, social and political developments in the countries to which they have exposure. In assessing the risk of a country, banks should consider both quantitative and qualitative factors of that country and must maintain formal country risk analysis files

In developing quantitative assessments of the risk of a country, banks may take into account the size and maturity profile of its external borrowing as well as its macroeconomic variables (including forecasts), fiscal, monetary, exchange rate and financial sector policies and relevant statistics.

Factors typically used in qualitative assessments of country risk include the quality of the policy-making function, social and political stability and the legal and regulatory environment of the country. In particular, banks should have regard to the country's compliance with international standards and codes.

Banks should give special attention to business dealings and transactions with counterparties from countries that do not sufficiently comply with international standards.

As part of the credit monitoring process banks must have a system in place to monitor their compliance with country exposure limits. Exceptions should be reported, approved and rectified as laid down in the country risk management policy.

Banks must perform periodic credit reviews and monitoring of their overseas exposures to identify unusual developments and, if appropriate, initiate necessary actions to protect their interests.

2. Risk tolerance limits

Banks with foreign exposure must have an adequate limit system in place for country risk. The limits must be regularly reviewed and authorized by the senior management function designated for that purpose. For effective oversight, banks are required to:

- Specify authorized activities and instruments.
- Set up a mechanism to monitor and report the bank's country exposure for senior management and BOD's review.

3. Lending principles

The following principles should be taken into consideration:-

a) Banks should ensure that facilities granted to overseas borrowers are subject to the basic prudent credit granting criteria applicable to domestic exposures. The principle of "Know Your Customer" should be upheld.

b) There are many ways in which exposures can become related to countries and thus create risk concentrations. Banks should therefore ascertain the identity and the ultimate ownership of the borrowers, regardless of their place of incorporation and the complexity of their group structure. Where appropriate, banks should obtain written evidence or confirmation from relevant parties of the identity of borrowers and their shareholder structure in name and percentage terms.

c) Credit should only be granted to creditworthy borrowers and due diligence should be carried out. Banks should not simply lend on the basis of the name or official status of a borrower or rely on any implicit governmental guarantee. Banks should satisfy themselves that the borrowers have sufficient foreign currency assets or income streams to service their foreign currency obligations.

d) Banks should not lend on the basis of inadequate information. While it may be difficult for borrowers in some countries to provide comprehensive financial data and audited accounts compiled in accordance with international accounting standards, banks should not let that difficulty become an excuse not to ask for the information they need to assess a credit proposal.

e) As with all lending, institutions lending to overseas entities should verify what the funds are being used for and assure themselves that the proceeds are not being diverted to speculative investments in commodities, property or stock markets. Where funds are being used for a project, banks should satisfy themselves that funds are not used for purposes other than financing the project. Frequent site visits and drawing by installments can help to prevent the misapplication of funds.

f) Banks should not grant facilities to a particular economic sector purely based on government direction or benefits provided by the government such as tax concessions. They should place greater weight on borrowers' repayment ability and the risks of and return from each transaction.

g) Some countries are undergoing a process of economic development and restructuring. The infrastructure of commercial laws and regulations may not develop at the same pace. In larger countries, owing to the needs of different regions, a lack of uniformity in laws and regulations and the interpretation of central directives by regional and provincial governments may exist. Banks should therefore beware of the assumption that what applies in one region or province applies in

another. In case of need, banks should seek advice from external counsel and get clearance from the relevant authorities.

h) Before accepting collateral covering overseas exposures, banks should ensure that there has been full compliance with statutory procedures to strengthen validity and enforceability. Where tangible collateral such as land and buildings in the country concerned is taken, banks should ensure that the pledgor has good title to the collateral and that any valuation reports are reliable. To this end, banks should retain local lawyers who are familiar with local laws, regulations and practices to check the legitimacy and enforceability of loan agreements, guarantees and other documentation.

4. Country Risk Ratings

A number of institutions may not have the capacity, or it is not feasible for them, given the level of their cross-border exposure, to have internal country risk assessment mechanism. The institutions that have significant cross-border exposure, greater analytical resources and access to better information should consider external rating as an input for their internal ratings. Ratings should be reviewed semi-annually or more frequently if the situation warrants.

Economics or research units in each major bank having significant cross-border and foreign exposure should be entrusted with preparing assessments of the country risk of the countries in which the institution is involved. The analysis, process and the level of resources devoted to it will depend upon the size of foreign exposure and the following may be taken into account:

• A formal country risk analysis should be conducted at least semi-annually for every country which the bank has a significant level of exposure (the significant level may be determined by the board or management).
• The analysis should be properly documented and conclusions reported in a way that provides the decision makers with a reasonable basis for determining the nature and level of the institution's exposure in a country.
• The analysis should cover all exposures and take into account all aspects of broadly defined concepts of country risk.

5. Country Risk Limits

Banks can minimize the country risk inherent in their cross-border exposures by diversification and setting country exposure limits. In setting the country exposure limits the following should be considered:

• Banks should have a system for establishing, maintaining and reviewing country exposure limits.

• Country exposure limits should be set based on prudential grounds. They should not be viewed as business targets to be met. To ensure objectivity, banks should maintain a clear division of responsibility by separating the business development function from the limit setting and monitoring function.

• Since different product lines or activities in the same country carry different levels of risk, it is appropriate to support aggregate country exposure limit with more discrete controls. Such controls might take the form of sub-limits on the basis of business lines, types of obligors or tenor etc.

• There may be separate limits for total country exposure, as well as country foreign currency exposure. However, Foreign Exposure limits as set out in the National Bank of Rwanda Prudential Guidelines on Foreign Exchange Exposure Limits must strictly be adhered to.

• Limits should be periodically reviewed to incorporate changing scenarios.

• Finally, once the limits are set, they should not be breached without going through a procedure for approval from a designated approving authority as identified by the board or policy- making group, which actually approved the policy and the said limits. Banks should establish a mechanism of monitoring compliance with these limits. Any breach of limits should be reported to the senior management and board of Directors who should take appropriate corrective action.

6. Management Information System

Banks are obliged to have adequate information systems to monitor compliance with country risk limits. It must be possible to detect a limit violation in good time and this should result in a report to the senior management and the board of Directors. The employees who are entrusted with controlling country risk limits must have the required knowledge and must be sufficiently independent from the staff whose work they are assigned to monitor.

The systems in place must be able to generate management reports which are detailed enough to permit analysis of different types of risk and cover all aspects of bank's operations. The reports should also identify the exceptions in a timely manner. Banks shall consider not only outstanding exposures but also undrawn commitments as well.

7. Internal Control and Audit

Country risk management process should have an adequate internal control mechanism. To achieve objectivity, the responsibility of marketing and lending personnel should be segregated from responsibilities of personnel who analyze country risk, assign country risk ratings and set limits structure. The internal audit function, in addition to review of compliance with policies /procedures, should ensure the integrity of the reports/information prepared for senior management.

Seen to be annexed to the Regulation nº 2100 /2018 - 009[614] of 25/07/2018 on risk management for banks

Kigali, on 25/07/2018

(sé)
RWANGOMBWA John
Governor

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NGAYABO Evode yakiriwe ku wa 15/05/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana NGAYABO Evode, utuye mu Mudugudu w'Uwigisura, Akagari ka Kabere, Umurenge wa Ruheru, Akarere ka Nyaruguru, mu Ntara y'Amajyepfo, ubarizwa kuri telephone 0788256680/0722447372; ahinduye amazina asanganywe.

Kuva ubu yiswe: **MBABAZI Evode.**

Bikorewe i Kigali, ku wa 03/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya UMUBERA Grace Sarah yakiriwe ku wa 06/06/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu UMUBERA Grace Sarah, utuye mu Mudugudu wa Cercle Sportif, Akagari ka Kiyovu, Umurenge wa Nyarugenge, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0784834629; ahinduye amazina asanganywe.

Kuva ubu yiswe: **UMUBERA BUSHAYIJA Sarah.**

Bikorewe i Kigali, ku wa 12/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya KAZENEZA Gloria yakiriwe ku wa 21/03/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu KAZENEZA Gloria, utuye mu Mudugudu w'Abatarushwa, Akagari ka Rwezamenyo, Umurenge wa Rwezamenyo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0787105096 ahinduye amazina asanganywe.

Kuva ubu yiswe **KAZENEZA Lyne Gloria.**

Bikorewe i Kigali, ku wa 12/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya UWIMANA Théophila yakiriwe ku wa 26/02/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu UWIMANA Théophila, utuye mu Mudugudu w'Intwari, Akagari ka Rwezamenyo I, Umurenge wa Rwezamenyo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone +32 499 423 621/+ 0788558263 ahinduye amazina asanganywe.

Kuva ubu yiswe **NDUWIMANA Aminat.**

Bikorewe i Kigali, ku wa 20/06/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NKUSI Benjamin yakiriwe ku wa 31/01/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana NKUSI Benjamin, utuye mu Mudugudu wa Cyimbazi, Akagari ka Ntunga, Umurenge wa Mwulire, Akarere ka Rwamagana, mu Ntara y'Iburasirazuba, ubarizwa kuri telephone 0785574030 ahinduye amazina asanganywe.

Kuva ubu yiswe **RUTAZIHANA Benjamin.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NDABARAMIYE Heritier yakiriwe ku wa 23/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana NDABARAMIYE Heritier utuye mu Mudugudu w'Inkurunziza, Akagari ka Mbugangari, Umurenge wa Gisenyi, Akarere ka Rubavu, mu Ntara y'Iburengerazuba, ubarizwa kuri telephone 0782796723 ahinduye amazina asanganywe.

Kuva ubu yiswe **NDABARAMIYE Heritier NYIRAZO.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NYIRAMBEBA Philomène yo ku wa 18/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu NYIRAMBEBA Philomène utuye mu Mudugudu wa Ruramba, Akagari ka Masaka, Umurenge wa Rugalika, Akarere ka Kamonyi, mu Ntara y'Amajyepfo, ubarizwa kuri telephone 0788218047, ahinduye amazina asanganywe.

Kuva ubu yiswe **INEZA Philomène.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya January Narcisse yakiriwe ku wa 23/03/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana January Narcisse, utuye mu Mudugudu wa Marembo, Akagari ka Nyarukombe, Umurenge wa Muyumbu, Akarere ka Rwamagana, mu Ntara y'Iburasirazuba, ubarizwa kuri telephone 0788434725/0788521186 ahinduye amazina asanganywe.

Kuva ubu yiswe **MURENZI January Narcisse.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya MUNYANKUSI Lwanga Thierry yakiriwe ku wa 28/03/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana MUNYANKUSI Lwanga Thierry, utuye mu Mudugudu wa Gasabo, Akagari ka Kabuguru II, Umurenge wa Rwezamenyo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0788504592/+32466382461 ahinduye amazina asanganywe.

Kuva ubu yiswe **LWANGA Thierry.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya SEMASAKA Eriel yakiriwe ku wa 12/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana SEMASAKA Eriel, utuye mu Mudugudu wa Rindiro, Akagari ka Kibagabaga, Umurenge wa Kimironko, Akarere ka Gasabo, mu Mujyi wa Kigali, ubarizwa kuri telephone 0786368680; ahinduye amazina asanganywe.

Kuva ubu yiswe **IMANIRAFASHA Samuel.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya BUGINGO Keith yakiriwe ku wa 24/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana BUGINGO Keith, utuye mu Mudugudu w'Imanzi, Akagari ka Bibare, Umurenge wa Kimironko, Akarere ka Gasabo, mu Mujyi wa Kigali, ubarizwa kuri telephone 0785287118; ahinduye amazina asanganywe.

Kuva ubu yiswe **BUJINGO Anthony Keith.**

Bikorewe i Kigali, ku wa 26/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya DUSABE Marie Claire Aimée yakiriwe ku wa 09/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu DUSABE Marie Claire Aimée, utuye mu Mudugudu w'Akanyirazaninka, Akagari ka Mumena, Umurenge wa Nyamirambo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0788304308; ahinduye amazina asanganywe.

Kuva ubu yiswe **MUKARUGWIZA Claire.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya KAYITESI GASANA Melysa yakiriwe ku wa 26/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu KAYITESI GASANA Melysa, utuye mu Mudugudu wa Rwampara, Akagari ka Mumena, Umurenge wa Nyamirambo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0782416260; ahinduye amazina asanganywe.

Kuva ubu yiswe **KAYITESI GASANA Melysa.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya KARARA Paul Alice yakiriwe ku wa 05/06/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu KARARA Paul Alice, utuye mu Mudugudu wa Kigarama, Akagari ka Nyagihinga, Umurenge wa Rusororo, Akarere ka Gasabo, mu Mujyi wa Kigali, ubarizwa kuri telephone 0788301436; ahinduye amazina asanganywe.

Kuva ubu yiswe **KARARA Alice.**

Bikorewe i Kigali, ku wa 12/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NARAME Gaudence yakiriwe ku wa 24/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu NARAME Gaudence, utuye mu Mudugudu wa Kavumu, Akagari ka Nyakiga, Umurenge wa Karama, Akarere ka Nyagatare, mu Ntara y'Iburasirazuba, ubarizwa kuri telephone 0788413232; ahinduye amazina asanganywe.

Kuva ubu yiswe **NARAME Shakira.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya BANDI Emmanuel yakiriwe ku wa 27/02/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana BANDI Emmanuel, utuye mu Mudugudu wa Gatagara, Akagari ka Jango, Umurenge wa Ruli, Akarere ka Gakenke, mu Ntara y'Amajyaruguru, ubarizwa kuri telephone 0788493147 ahinduye amazina asanganywe.

Kuva ubu yiswe **ABANDI NIYONSENGA Emmanuel.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya MBARUSHUMURAGE Boanerge yakiriwe ku wa 06/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Bwana MBARUSHUMURAGE Boanerge, utuye mu Mudugudu wa Murunda, Akagari ka Mburamazi, Umurenge wa Murunda, Akarere ka Rutsiro, mu Ntara y'Iburengerazuba, ubarizwa kuri telephone 0781997724; ahinduye amazina asanganywe.

Kuva ubu yiswe: **MBARUSHUMURAGE Jean Boanerge.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya NYIRAGARUKA Aline yakiriwe ku wa 06/03/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu NYIRAGARUKA Aline, utuye mu Mudugudu wa Rebero, Akagari ka Gahurire, Umurenge wa Kazoo, Akarere ka Ngoma, mu Ntara y'Iburasirazuba, ubarizwa kuri telephone 0780374006; ahinduye amazina asanganywe.

Kuva ubu yiswe **UMUKUNDWA Aline.**

Bikorewe i Kigali, ku wa 12/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

ICYEMEZO GITANGA UBURENGANZIRA BWO GUHINDURA IZINA

Minisitiri w'Ubutegetsi bw'Igihugu;

Ashingiye ku Itegeko nº 32/2016 ryo ku wa 28/08/2016 rigenga abantu n'umuryango, cyane cyane mu ngingo yaryo ya 42;

Ashingiye ku Iteka rya Minisitiri nº 001/07.01 ryo ku wa 17/01/2017 rishyiraho uburyo n'inzira bikurikizwa mu guhindura izina;

Amaze kubona ibaruwa ya KINANI Delphine yakiriwe ku wa 05/04/2018 isaba uburenganzira bwo guhindura amazina asanzwe yanditse mu gitabo cy'Irangamimerere;

Yemeje ko:

Madamu KINANI Delphine, utuye mu Mudugudu w'Ubumwe, Akagari ka Kora, Umurenge wa Gitega, Akarere ka Nyarugenge, mu Mujyi wa Kigali, ubarizwa kuri telephone 0781276421; ahinduye amazina asanganywe.

Kuva ubu yiswe **ABIMANA Delphine.**

Bikorewe i Kigali, ku wa 24/07/2018

(sé)
KABONEKA Francis
Minisitiri w'Ubutegetsi bw'Igihugu

INGINGO Z'INGENZI Z'URWANDIKO RWA INGABIRE Jean Marie Pacifique RUSABA GUHINDURA AMAZINA

Uwitwa **INGABIRE Jean Marie Pacifique** mwene NZABAMWITA Michel na MUJAWASE Velonique utuye mu Mudugudu wa Rukurazo, Akagari ka Kibagabaga, Umurenge wa Kimironko, Akarere ka Gasabo, mu Mujyi wa Kigali;

Yasabye uburenganzira bwo gusimbuza izina INGABIRE Jean Marie izina **RWIBUTSO HIRWA** mu mazina asanganywe, INGABIRE Jean Marie Pacifique akitwa **RWIBUTSO HIRWA Pacifique** mu Irangamimerere;

Impamvu atanga ni uko amazina **INGABIRE Jean Marie** amutera rimutera ipfunwe muri bagenzi be kuko ari amazina akunze kwitwa n'abantu b'igitsina gore kandi we akaba ari umugabo; aho na Jean abantu bahita bamubwira ko ubwo bivuze Jeanne kubera kumwumvana ayo mazina akunze kwitwa abantu b'igitsina gore; bityo agahorana ipfunwe muri bagenzi be;

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, gusimbuza amazina INGABIRE Jean Marie, amazina **RWIBUTSO HIRWA** mu mazina asanganywe, INGABIRE Jean Marie Pacifique akitwa **RWIBUTSO HIRWA Pacifique** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA NYIRANTAMBARA Dative RUSABA GUHINDURA AMAZINA

Uwitwa NYIRANTAMBARA Dative utuye mu Mudugudu w'Uwateke, Akagari ka Rwampara, Umurenge wa Kigarama, Akarere ka Kicukiro, mu Mujyi wa Kigali;

Yasabye uburenganzira bwo guhindurirwa izina NYIRANTAMBARA mu mazina asanganywe NYIRANTAMBARA Dative, maze akitwa **ABIRINGIYIMANA Dative.**

Impamvu atanga ni uko izina NYIRANTAMBARA ari izina ribi kandi rimukomeretsa.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, guhindurirwa izina NYIRANTAMBARA, mu mazina asanganywe NYIRANTAMBARA Dative, maze akitwa **ABIRINGIYIMANA Dative** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA UZAMUKUNDA Beatrice RUSABA GUHINDURA AMAZINA

Uwitwa, UZAMUKUNDA Beatrice mwene RWANGANO Charles na NYIRAKANYANA Ancille utuye mu Mudugudu wa Mubuga, Akagari ka Cyanya, Umurenge wa Cyuve, Akarere ka Musanze, mu Ntara y'Amajyaruguru;

Yasabye uburenganzira bwo kongera izina **MUKOSHA** mu mazina asanganywe, UZAMUKUNDA Beatrice akitwa **UZAMUKUNDA MUKOSHA Beatrice**;

Impamvu atanga ni uko izina MUKOSHA ari izina rya nyirasenge witabye Imana kera. Iri zina bakaba bararimuhimbaga akiri muto ndetse aza kuryandikisha ku byangombwa bye byinshi.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina **MUKOSHA,** mu mazina asanganywe, UZAMUKUNDA Beatrice bityo akitwa **UZAMUKUNDA MUKOSHA Beatrice** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA RWIYEREKA NYIRABURANGA BOKANGA Claire RUSABA GUHINDURA AMAZINA

Uwitwa, **RWIYEREKA NYIRABURANGA BOKANGA Claire**, mwene RWIYEREKA CYIZA Pancras na NYIRABISABO Vénéranda, utuye mu Mudugudu wa Kabutare (Casa Amicus Estate), Akagari ka Nyagahinga, Umurenge wa Rusororo, Akarere ka Gasabo, Umujyi wa Kigali, ubarizwa kuri telefone nº0782286889/0788300166;

Yasabye uburenganzira bwo guhindura amazina ye, **RWIYEREKA NYIRABURANGA BOKANGA Claire,** hagakurwa izina **BOKANGA** mu mazina asanganywe, RWIYEREKA NYIRABURANGA BOKANGA Claire akitwa **Claire NYIRABURANGA RWIYEREKA** mu Irangamimerere;

Impamvu atanga ni uko izina **BOKANGA** ari izina yari yiswe biturutse ku gushyingiranwa kwe n'uwahoze ari umugabo we, MPOKO Albert BOKANGA, ubu bakaba baratandukanye mu buryo bwemewe n'amategeko;

Indi mpamvu ni uko ashaka gusubira ku mazina ye y'ubukobwa ariyo **Claire NYIRABURANGA RWIYEREKA** nk'uko bigaragara mu nyandiko ye ya batisimu yakozwe akiri umwana.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, gukura izina **BOKANGA** mu mazina asanganywe, RWIYEREKA NYIRABURANGA BOKANGA Claire bityo akitwa **Claire NYIRABURANGA RWIYEREKA** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA WIBABARA Diane RUSABA GUHINDURA AMAZINA

Uwitwa **WIBABARA Diane** mwene NZAMURAMBAHO Emmanuel na MUJAWAMARIYA Providence utuye mu Mudugudu wa Rwinyange, Akagari ka Rwimbogo, Umurenge wa Nyarugunga, Akarere ka Kicukiro, mu Mujyi wa Kigali, uboneka kuri telephone 0788689024 / 0784713478;

Yanditse asaba uburenganzira bwo guhindura amazina ye WIBABARA Diane akayongeraho izina NZAMURAMBAHO akitwa **WIBABARA NZAMURAMBAHO Diane** mu Irangamimerere;

Impamvu atanga ni uko izina NZAMURAMBAHO ari izina ry'umuryango wabo rikomoka kuri se witwa NZAMURAMBAHO Emmanuel, akaba ashaka ko rigaragara mu irangamimerere no mu byangombwa bye byose.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina NZAMURAMBAHO ku mazina asanganywe WIBABARA Diane bityo akitwa **WIBABARA NZAMURAMBAHO Diane** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA SIMBI Sandra RUSABA GUHINDURA AMAZINA

Uwitwa **SIMBI Sandra** mwene GASANA Yussuf na MUREKATETE Odette utuye mu Mudugudu wa Gatare, Akagari ka Rugarama, Umurenge wa Nyamirambo, Akarere ka Nyarugenge, mu Mujyi wa Kigali, uboneka kuri telephone 0786704030/ 0788653411;

Yanditse asaba uburenganzira kongera izina **GASANA** mu mazina asanganywe SIMBI Sandra, no guhindura izina SIMBI akarisimbuza **ISIMBI** akitwa **GASANA ISIMBI Sandra** mu Irangamimerere;

Impamvu atanga ni uko izina **GASANA** ari izina rikomoka kuri se witwa GASANA Yussuf rikaba ari izina ry'umuryango wabo;

Naho izina SIMBI, ni uko akivuka yiswe ISIMBI ariko mu myandikire hakaba haragiye handikwa Simbi mu nyandiko zimwe, mu zindi hakandikwa ISIMBI.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina **GASANA** mu mazina asanganywe no guhindura izina SIMBI, rikaba **ISIMBI** bityo akitwa **GASANA ISIMBI Sandra** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA UMULISA Soleil RUSABA GUHINDURA AMAZINA

Uwitwa UMULISA Soleil mwene KAMARERA na NYIRAMWAMI utuye mu Mudugudu wa Gisesa, Akagari ka Busoro, Umurenge wa Karago, Akarere ka Nyabihu, mu Ntara y'Iburengerazuba;

Yasabye uburenganzira bwo gusimbuza izina Soleil izina **Chance** mu mazina asanganywe UMULISA Soleil akitwa **UMULISA Chance**;

Impamvu atanga ni uko izina Soleil ari izina ry'irigenurano rikaba rimutera ipfunwe;

Naho izina SIMBI, ni uko akivuka yiswe ISIMBI ariko mu myandikire hakaba haragiye handikwa Simbi mu nyandiko zimwe, mu zindi hakandikwa ISIMBI.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, gusimbuza izina Soleil izina **Chance** mu mazina asanganywe UMULISA Soleil bityo akitwa **UMULISA Chance** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA BIGONZIKI Jeanne RUSABA GUHINDURA AMAZINA

Uwitwa BIGONZIKI Jeanne mwene BIGONZIKI Aloys na UWISIZE Immaculée utuye mu Gihugu cy'Ububiligi, 56, Avenue des Fleurs, 1950 Kraaienem, uboneka kuri telephone +32 485 739 225;
Mu Rwanda abarizwa mu Mudugudu wa Kanyirazaninka, Akagari ka Munena, Umurenge wa Nyamirambo, Akarere ka Nyarugenge, mu Mujyi wa Kigali; uboneka kuri telefone ya Bwana KABANDANA S. Aimé, 0788300394;

Yasabye uburenganzira bwo guhindura amazina asanganywe BIGONZIKI Jeanne, agasimbuza izina BIGONZIKI izina **WAMBABO** (ryari risanzwe ari **WANGABO**, riza kwandikwa nabi mu Gihugu cy'Ububiligi, biza kumugora kurikosora) akitwa **WAMBABO Jeanne** mu Irangamimerere.

Impamvu atanga ni uko yagiye mu Gihugu cy'Ububiligi ajyanywe no gushakisha imiberebo myiza, biza kuba ngombwa ko asimbuza izina BIGONZIKI, izina **WAMBABO** kugira ngo abone ibyangombwa by'aho no kuhabona akazi, yitwa **WAMBABO Jeanne** mu Irangamimerere mu Gihugu cy'Ububiligi ku buryo ariyo mazina yitwa mu byangombwa bye byose byo muri icyo Gihugu ndetse no mu rwandiko rw'Inzira ("passport"), akaba yifuza ko agira amazina amwe mu Rwanda no mu Bubiligi..

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, gusimbuza izina BIGONZIKI izina **WAMBABO** mu mazina asanganywe BIGONZIKI Jeanne bityo akitwa **WAMBABO Jeanne** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA UWAMAHORO Deborah RUSABA GUHINDURA AMAZINA

Uwitwa UWAMAHORO Deborah, mwene Yoshua NDAGIJIMANA MASASU na UMULISA Lydia MASASU, utuye mu Mudugudu w'Ingenzi, Akagari ka Bibare, Umurenge wa Kimironko, Akarere ka Gasabo, mu Mujyi wa Kigali, ubarizwa kuri telefone 0788353129;

Yasabye uburenganzira bwo guhindura amazina ye, UWAMAHORO Deborah akongera izina **MASASU** mu mazina asanganywe, UWAMAHORO Deborah akitwa **Deborah UWAMAHORO MASASU** mu Irangamimerere;

Impamvu atanga ni uko izina **MASASU** ari izina rikomoka kuri se, Yoshua NDAGIJIMANA MASASU, izina MASASU rikaba ari izina ry'umuryango akomokamo.

Indi mpamvu ni uko kuri we ari ishema kwitiranwa na Se bityo akazakira umurage mwiza wa Se akaba umuvugabutumwa nka se, Pasiteri Yoshua NDAGIJIMANA MASASU.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina **MASASU** mu mazina asanganywe UWAMAHORO Deborah bityo akitwa **Deborah UWAMAHORO MASASU** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA MBISHIBISHI Adolphe RUSABA GUHINDURA AMAZINA

Uwitwa MBISHIBISHI Adolphe mwene BUGINGO MBISHIBISHI na CYIZA Immaculée utuye mu Mudugudu wa Bwiza, Akagari ka Nyakabanda, Umurenge wa Niboye, Akarere ka Kicukiro, mu Mujyi wa Kigali;

Yasabye uburenganzira bwo kongera izina **Liam** mu mazina asanganywe MBISHIBISHI Adolphe akitwa **MBISHIBISHI Adolphe Liam**;

Impamvu atanga ni uko izina **Liam** yaribatijwe mu Itorero rya Zion Temple.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina **Liam** mu mazina asanganywe MBISHIBISHI Adolphe akitwa **MBISHIBISHI Adolphe Liam** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA KABASINGE Barnabe RUSABA GUHINDURA AMAZINA

Uwitwa KABASINGE Barnabe mwene MURENGERANTOZO Jean Chrisostome na KABEGA Marie utuye mu Mudugudu wa Ganza, Akagari ka Kiyovu, Umurenge wa Nyarugenge, Akarere ka Nyarugenge, mu Mujyi wa Kigali, uboneka kuri telefone 0788306618;

Yasabye uburenganzira bwo guhindura amazina asanganywe KABASINGE Barnabe akongeramo izina **MURENGERA** akitwa **KABASINGE MURENGERA Barnabe** mu Irangamimerere;

Impamvu atanga ni uko izina **MURENGERA** ari rimwe mu mazina afite mu mazina ari ku mpamyabumenyi ze yabonye asoza amashuri muri Repubulika Iharanira Demokarasi ya Congo /DRC, **KABASINGE MURENGERA** aho umuryango we wari warahungiye, bityo mu gihe cya "politique de retours a l'authenticité", aho abaturage bo muri iki Gihugu basabwe n'Umuyobozi kwitwa gusa amazina afite inkomoko mu gisekuruza cy'umuryango wabo, amazina y'amanyamahanga (amakirisitu) avanwa mu byangombwa, yitwa **KABASINGE MURENGERA**, iri rikaba ryarasimbuye izina Barnabe;

Indi mpamvu atanga ni uko ashaka guhuza amazina ye yose uko ari atatu mu byangombwa bye kubera ko na none atashye mu Rwanda yakuye izina MURENGERA mu mazina ye yandikwa mu Irangamimerere ku mazina KABASINGE Barnabe kuko yari azi ko hemewe amazina abiri.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, kongera izina **MURENGERA** ku mazina asanganywe KABASINGE Barnabe bityo akitwa **KABASINGE MURENGERA Barnabe** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

INGINGO Z'INGENZI Z'URWANDIKO RWA BARAYAVUGA RUSABA GUHINDURA AMAZINA

Uwitwa **BARAYAVUGA** mwene RUKAZA Damien na NYIRAMAJYERI Eugenie utuye mu Mudugudu w'Umucyo, Akagari ka Kigarama, Umurenge wa Kigarama, Akarere ka Kicukiro, mu Mujyi wa Kigali;

Yasabye uburenganzira bwo gusimbuza izina BARAYAVUGA, izina **NDATIMANA** no kongera izina **Francis** kuri iri zina bityo akitwa **NDATIMANA Francis** mu Irangamimerere;

Impamvu atanga ni uko izina BARAYAVUGA rimutera ipfunwe, n'izina Francis rikaba ari izina yiswe amaze kubatizwa.

Akaba asaba kwemererwa binyuze mu nzira zemewe n'amategeko, gusimbuza izina BARAYAVUGA, izina **NDATIMANA** no kongera izina **Francis** kuri iri zina bityo akitwa **NDATIMANA Francis** mu gitabo cy'Irangamimerere kirimo inyandiko ye y'ivuka.

ICYEMEZO *NºRCA/0388*/2018 CYO KU WA 16/07/2018 GIHA UBUZIMAGATOZI «GATSIBO AGROPROCESSING COOPERATIVE»

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« GATSIBO AGROPROCESSING COOPERATIVE»** ifite icyicaro i Simbwa, Umurenge wa Kabarore, Akarere ka Gatsibo, Intara y'Iburasirazuba;

YEMEJE:

Ingingo ya mbere:

Koperative **« GATSIBO AGROPROCESSING COOPERATIVE »** ifite icyicaro i Simbwa, Umurenge wa Kabarore, Akarere ka Gatsibo, Intara y'Iburasirazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« GATSIBO AGROPROCESSING COOPERATIVE »** igamije guteza imbere imirimo ijyanye no gutunganya ibikomoka ku buhinzi bw'ibigori. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« GATSIBO AGROPROCESSING COOPERATIVE »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 16/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0348*/2018 CYO KU WA 09/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «KORANUMURAVA BUTARE »

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« KORANUMURAVA BUTARE »** ifite icyicaro i Mwimerere, Akagari ka Nyamihanda, Umurenge wa Butare, Akarere ka Rusizi, Intara y'Iburengerazuba;

YEMEJE:

Ingingo ya mbere:

Koperative **« KORANUMURAVA BUTARE »** ifite icyicaro i Mwimerere, Akagari ka Nyamihanda, Umurenge wa Butare, Akarere ka Rusizi, Intara y'Iburengerazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« KORANUMURAVA BUTARE »** igamije gutanga serivisi zijyanye no gufata neza imihanda. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« KORANUMURAVA BUTARE »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 09/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu

ICYEMEZO *NºRCA/0754*/2009 CYO KU WA 27/04/2009 GIHA UBUZIMAGATOZI «COOPERATIVE DE DISTRIBUTION DE FRAISES DE MUHANGA » (CODFM - KOREREJO)

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 16/2008 ryo ku wa 11/06/2008 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« CODFM - KOREREJO»** ifite icyicaro i Gahogo, Umurenge wa Nyamabuye, Akarere ka Muhanga, Intara y'Amajyepfo, mu rwandiko rwe rwo ku wa 02 Gashyantare 2009;

YEMEJE:

Ingingo ya mbere:

Koperative **« CODFM - KOREREJO»** ifite icyicaro i Gahogo, Umurenge wa Nyamabuye, Akarere ka Muhanga, Intara y'Amajyepfo, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« CODFM - KOREREJO»** igamije guteza imbere ubuhinzi bw'inkeri n'ibizikomokaho. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Iki Cyemezo kigira agaciro guhera umunsi cyatangarijweho mu Igazeti ya Leta ya Repubulika y'u Rwanda.

Kigali, ku wa 27/04/2009

(Sé)
MUGABO Damien
Umuyobozi w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0340*/2018 CYO KU WA 06/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «WITINYA RUHANGO » (KOWIRU)

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« KOWIRU»** ifite icyicaro i Nyamagana, Umurenge wa Ruhango, Akarere ka Ruhango, Intara y'Amajyepfo;

YEMEJE:

Ingingo ya mbere:

Koperative **« KOWIRU»** ifite icyicaro i Nyamagana, Umurenge wa Ruhango, Akarere ka Ruhango, Intara y'Amajyepfo, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« KOWIRU»** igamije gutanga serivisi zijyanye no gukodesha sale, imyenda y'abageni na Decoration. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« KOWIRU»** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 09/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0291*/2018 CYO KU WA 04/06/2018 GIHA UBUZIMAGATOZI KOPERATIVE «IMBONEZA - KAVUMU »

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« IMBONEZA - KAVUMU »** ifite icyicaro ku Kivuguza, Akagari ka Rugeshi, Umurenge wa Kavumu, Akarere ka Ngororero, Intara y'Iburengerazuba;

YEMEJE:

Ingingo ya mbere:

Koperative **« IMBONEZA - KAVUMU »** ifite icyicaro ku Kivuguza, Akagari ka Rugeshi, Umurenge wa Kavumu, Akarere ka Ngororero, Intara y'Iburengerazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« IMBONEZA - KAVUMU »** igamije guteza imbere ubworozi bw'inka za kijyambere. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« IMBONEZA - KAVUMU »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 04/06/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0338*/2018 CYO KU WA 05/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «DUFATANYE RUSORORO »

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« DUFATANYE RUSORORO »** ifite icyicaro mu Kagari ka Kabuga II, Umurenge wa Rusororo, Akarere ka Gasabo, Umujyi wa Kigali;

YEMEJE:

Ingingo ya mbere:

Koperative **« DUFATANYE RUSORORO »** ifite icyicaro mu Kagari ka Kabuga II, Umurenge wa Rusororo, Akarere ka Gasabo, Umujyi wa Kigali, Intara y'Iburengerazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« DUFATANYE RUSORORO »** igamije guteza imbere ubuhinzi bw'imboga. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« DUFATANYE RUSORORO »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 05/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0415*/2018 CYO KU WA 27/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «KIGALI AGRICULTURAL AND ENVIRONMENTAL PROTECTION» (KKAEP)

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« KKAEP»** ifite icyicaro i Kimisagara, Umurenge wa Kimisagara, Akarere ka Nyarugenge, Umujyi wa Kigali;

YEMEJE:

Ingingo ya mbere:

Koperative **« KKAEP»** ifite icyicaro i Kimisagara, Umurenge wa Kimisagara, Akarere ka Nyarugenge, Umujyi wa Kigali, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« KKAEP»** igamije guteza imbere ubucuruzi bw'imyaka (ibirayi,…) no kubungabunga ibidukikije (amashyamba, imigezi, ibishanga,…). Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« KKAEP»** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 27/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0401*/2018 CYO KU WA 19/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «DUKOMEZANYE - NKANGA»

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« DUKOMEZANYE - NKANGA»** ifite icyicaro i Nkanga, Umurenge wa Sake, Akarere ka Ngoma, Intara y'Iburasirazuba;

YEMEJE:

Ingingo ya mbere:

Koperative **« DUKOMEZANYE - NKANGA»** ifite icyicaro i Nkanga, Umurenge wa Sake, Akarere ka Ngoma, Intara y'Iburasirazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« DUKOMEZANYE - NKANGA»** igamije guteza imbere ubuhinzi bwa soya n'ibigori. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« DUKOMEZANYE - NKANGA»** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 19/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0113*/2018 CYO KU WA 02/03/2018 GIHA UBUZIMAGATOZI KOPERATIVE « ABABUNGABUNGA INGAGI »

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« ABABUNGABUNGA INGAGI »** ifite icyicaro i Nyabigoma, Umurenge wa Kinigi, Akarere ka Musanze, Intara y'Amajyaruguru;

YEMEJE:

Ingingo ya mbere:

Koperative **« ABABUNGABUNGA INGAGI »** ifite icyicaro i Nyabigoma, Umurenge wa Kinigi, Akarere ka Musanze, Intara y'Amajyaruguru, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« ABABUNGABUNGA INGAGI »** igamije guteza imbere ubugeni (ibihangano n'imbyino gakondo). Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« ABABUNGABUNGA INGAGI »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 02/03/2018

(Sé)
NZAKUNDA Joseph
Umuyobozi w'Agateganyo w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0022/2017* CYO KU WA 12/01/2017 GIHA UBUZIMAGATOZI «COOPERATIVE DE TRANSPORT DE MOTO KIRAMBO» (COOTRAMOKI)

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« COOTRAMOKI»** ifite icyicaro i Kigoya, Umurenge wa Kanjongo, Akarere ka Nyamasheke, Intara y'Iburengerazuba;

YEMEJE:

Ingingo ya mbere:

Koperative **« COOTRAMOKI»** ifite icyicaro i Kigoya, Umurenge wa Kanjongo, Akarere ka Nyamasheke, Intara y'Iburengerazuba, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« COOTRAMOKI»** igamije gutanga serivisi zijyanye no gutwara abantu n'ibintu hakoreshejwe amapikipiki. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **«COOTRAMOKI»** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 12/01/2017

(Sé)
MUNANURA Apollo
Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0341*/2018 CYO KU WA 06/07/2018 GIHA UBUZIMAGATOZI KOPERATIVE «ABAHUJUMURIMO GASANZE»

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« ABAHUJUMURIMO GASANZE»** ifite icyicaro i Gasanze, Umurenge wa Nduba, Akarere ka Gasabo, Umujyi wa Kigali;

YEMEJE:

Ingingo ya mbere:

Koperative **« ABAHUJUMURIMO GASANZE»** ifite icyicaro i Gasanze, Umurenge wa Nduba, Akarere ka Gasabo, Umujyi wa Kigali, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« ABAHUJUMURIMO GASANZE»** igamije gutanga serivisi zijyanye no gupakira no gupakurura imizigo (man - power). Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« ABAHUJUMURIMO GASANZE»** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 06/07/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative

ICYEMEZO *NºRCA/0353*/2018 CYO KU WA 29/06/2018 GIHA UBUZIMAGATOZI KOPERATIVE « SHISHA KIBONDO GITI » (COSHIKIGI)

Umuyobozi w'Ikigo cy'Igihugu gishinzwe guteza imbere Amakoperative;

Ashingiye ku Itegeko nº 50/2007 ryo kuwa 18 Nzeri 2007 rigena ishyirwaho, imiterere n'imikorere y'Amakoperative mu Rwanda, nk'uko ryahinduwe kandi ryujujwe kugeza ubu, cyane cyane mu ngingo yaryo ya 23, igika cya 3;

Ashingiye ku Itegeko nº 48/2013 ryo kuwa 28/06/2013 rishyiraho Ikigo cy'Igihugu gishinzwe guteza Imbere Amakoperative, cyane cyane mu ngingo yaryo ya 3, igika cya 2;

Abisabwe na Perezida wa Koperative **« COSHIKIGI »** ifite icyicaro i Murehe, Umurenge wa Giti, Akarere ka Gicumbi, Intara y'Amajyaruguru;

YEMEJE:

Ingingo ya mbere:

Koperative **« COSHIKIGI »** ifite icyicaro i Murehe, Umurenge wa Giti, Akarere ka Gicumbi, Intara y'Amajyaruguru, ihawe ubuzimagatozi.

Ingingo ya 2:

Koperative **« COSHIKIGI »** igamije guteza imbere ubworozi bw'inka za kijyambere. Ntiyemerewe gukora indi mirimo inyuranye n'iyo iherewe ubuzimagatozi keretse ibanje kubisaba ikanabiherwa uburenganzira.

Ingingo ya 3:

Koperative **« COSHIKIGI »** itegetswe gutangaza iki Cyemezo mu Igazeti ya Leta ya Repubulika y'u Rwanda mu gihe kitarenze iminsi mirongo itatu (30) ikimara kugihabwa.

Kigali, ku wa 29/06/2018

(Sé)
Prof. HARELIMANA Jean Bosco
Umuyobozi Mukuru w'Ikigo cy'Igihugu
gishinzwe guteza imbere Amakoperative