



**PLAN DE CONTINUITE DES ACTIVITES DE LA
COOPERATIVE D'EPARGNE ET DE CREDIT
POUR L'AUTO-DEVELOPPEMENT DES
MILITAIRES (CECADM)**

Bujumbura, août 2020

Table des matières

CHAPITRE I : CONTEXTE ET DEFINITIONS.....	3
I.1. Contexte.....	3
I.2. Quelques Définitions.....	4
CHAPITRE II : TYPES D'ORGANISATION ET SYSTEME DE MANAGEMENT DE CONTINUITE D'ACTIVITES.....	8
II.1. Les types d'organisation de continuité d'activités	8
II.2. Système de Management de Continuité d'Activités	8
CHAPITRE III : SCHEMA DIRECTEUR ET CARTOGRAPHIE DES RISQUES A LA CECADM.....	10
III.1. Schéma directeur de la continuité d'activités	10
III.2. Cartographie des risques à la CECADM	11
CHAPITRE IV : SCENARII DES RISQUES RETENUS A LA CECADM.....	14
CHAPITRE V : CONCLUSION	20



CHAPITRE I : CONTEXTE ET DEFINITIONS

I.1. Contexte

La Coopérative d'Epargne et de Crédit pour l'Auto-Développement des Militaires (CECADM en sigle) est une institution de microfinance créée par les membres de la Force de Défense Nationale du Burundi (FDNB) à l'initiative du Haut Commandement Militaire. A sa création en date du 07/05/2007, elle était une institution de microfinance de première catégorie agréée par la Banque Centrale par l'acte D1/721/2007 du 24/10/2007. Avec la loi N°1/17 de 22/8/2017 régissant les activités bancaires mise en application par le règlement N°001/2018 du 17/08/2018 relatif aux activités de microfinance, les institutions de microfinance de première catégorie dont la CECAD, deviennent des institutions de microfinance de troisième catégorie. A partir du 23/04/2019, la CECAD a changé de dénomination pour devenir une Coopérative d'Epargne et de Crédit pour l'Auto-Développement des Militaires (CECADM en sigle) sous l'acte d'agrément actualisé D1/749/2019.

Dans sa vision, la CECADM se veut une coopérative de référence par sa pérennité et son autonomie. De nos jours, la CECADM est une institution rentable et stable comme les différents indicateurs peuvent le montrer. Toutefois, une organisation telle qu'une institution de microfinance est confrontée à tout moment à de nombreux risques tant internes qu'externes qui pourraient menacer subitement sa stabilité, sa rentabilité et sa pérennité voire même provoquer la cessation de ses activités temporairement ou définitivement, si des mesures qui s'imposent ne sont pas prises à l'avance et à temps.

A titre illustratif, les événements du 11 septembre 2001 ont prouvé que même dans l'éventualité d'événements à impact élevé et à faible probabilité, le rétablissement est possible. Ainsi, malgré la destruction des immeubles et la perturbation de tout un quartier de Manhattan (New York), les entreprises et institutions munies d'un bon plan de continuité ont survécu.

Il est donc primordial que chaque organisation soit dotée d'un plan de continuité des activités élaboré en s'appuyant sur les normes internationales (notamment ISO¹ 22301 et 31000), la législation et la culture du pays.

La CECADM pouvant être sujette aux risques de diverses natures ne peut pas se passer de cet outil, afin de contrôler les sinistres et incidents inopinés pouvant perturber son fonctionnement normal. Par ailleurs, l'article 19 du Circulaire N°12/M/18 de la Banque de la République du Burundi (BRB) relatif au contrôle interne, stipule en son premier paragraphe que:

¹ International Standard Organization

«Les institutions de microfinance, structures faitières et organes financiers doivent se doter d'un plan de continuité d'activités, approuvé par le Conseil d'Administration régulièrement, testé et actualisé par la Direction». De plus, l'article 20 du règlement N°001/2019 de la BRB relatif à la protection des consommateurs des produits et services financiers du 03/01/2019 exige que : *«Le fournisseur de produits et services financiers doit assurer la continuité du fonctionnement des systèmes d'exploitation pour répondre, en tout temps, aux besoins des consommateurs en prévoyant des alternatives en cas de dysfonctionnement des systèmes. La clientèle doit être immédiatement informée et orientée en fonction de la mise en œuvre de l'une ou autre alternative».*

Le présent plan de continuité d'activités revient sur quelques définitions-clé, définit les types d'organisation de la continuité d'activités, le système de management de continuité d'activités et le schéma directeur de la continuité d'activités, dresse la cartographie des risques à la CECADM et propose enfin les mesures curatives relatives à chaque risque. Bien que les normes ISO recommandent un plan de continuité uniquement pour les risques catastrophiques, la CECADM a jugé bon d'élaborer un plan de continuité d'activités englobant les risques critiques, élevés et moyens.

I.2. Quelques Définitions

I.2.1. Plan de continuité d'activités

Le Plan de Continuité d'Activités (PCA en sigle) *pour les établissements financiers* pourrait être défini comme étant *l'ensemble de mesures visant à assurer selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé des prestations essentielles de l'entreprise puis la reprise planifiée des activités*². En d'autres termes, le plan de continuité d'activités est la somme des dispositions prises par l'entreprise pour garantir à l'organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal.

Le circulaire N°12/M/18 de la Banque de la République du Burundi stipule, en son article 2 que : *«Le PCA est un plan d'actions écrit et détaillé décrivant, en cas de perturbation opérationnelle majeure, y compris le choc externe, les procédures et systèmes nécessaires pour maintenir ou rétablir dans un délai prédéterminé les activités et fonctions essentielles de l'institution.»* Le PCA est donc là pour éviter les risques.

² www.alarmetilt.com

Le plan de continuité diffère d'une entreprise à l'autre, étant donné que chaque entreprise a ses moyens et sa culture.

I.2.2. Menace

Une menace est un **danger qui existe** dans l'environnement d'un système, indépendamment de celui-ci³. A titre d'exemples, un accident, une erreur, un manque de conscience constituent des menaces. Ces dernières peuvent être naturelles (inondation, tempête), non intentionnelles (mauvaise manipulation de données) et intentionnelles (abus du profil donné à un utilisateur). Bref, *«une menace est tout ce qui peut arriver»*.

I.2.3. Risque

Un risque est un **danger éventuel**, plus ou moins prévisible, inhérent à une situation ou à une activité. C'est une éventualité d'un événement futur, incertain ou d'un terme indéterminé, ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage⁴. De façon générale, un risque est un événement pouvant modifier le comportement normal d'une activité. Grosso modo, *«un risque est tout ce qui va arriver»*.

✓ De la classification des risques selon le niveau de gravité

Selon le niveau de gravité, les risques sont classés en quatre catégories:

- les risques critiques ou catastrophiques ;
- les risques élevés ou majeurs ;
- les risques moyens ;
- les risques faibles.

Au niveau de l'étendue, les risques critiques ou catastrophiques affectent la capacité d'une grande partie ou de l'ensemble de l'organisation à continuer ses activités. Quant aux risques élevés ou majeurs, ils affectent la capacité de plusieurs unités à continuer leurs activités. Les risques moyens et faibles quant à eux affectent la capacité d'une ou de quelques unités à maintenir leurs activités.

Au niveau de la capacité de réponse pour les risques critiques ou catastrophiques, des orientations stratégiques ou une prise de décision extraordinaire sont nécessaires afin de répondre à l'incident. Des hypothèses de travail sur lesquelles repose le PCA pourraient ne pas être applicables. S'agissant des risques majeurs (élevés), les ressources disponibles sont suffisantes,

³ www.phgarin.wordpress.com

⁴ www.ineris.fr

mais, une coordination est requise entre plusieurs parties prenantes pour rétablir les activités dans un délai raisonnable. Des stratégies non prévues pourraient devoir être mises en place pour les risques moyens et faibles, les ressources disponibles au sein de l'unité ou dans les unités de soutien habituelles sont suffisantes pour continuer ou rétablir les activités dans un délai raisonnable.

Au niveau de la prise en charge, la procédure pour les risques critiques ou catastrophiques est la suivante :

- Le coordonnateur PCA alerte le chef de la cellule de gestion d'incident, et ce dernier mobilise le Directeur Général (DG en sigle), dans le cas où celui-ci n'est pas lui-même le chef ;
- La cellule de gestion d'incident prend en charge la gestion tactique de l'incident ;
- Le Conseil d'Administration (CA en sigle) donne les orientations stratégiques à la cellule de gestion d'incident.

Pour les risques majeurs, la procédure est la suivante :

- Le coordonnateur PCA alerte le chef de la cellule de gestion d'incident, et ce dernier mobilise le DG, dans le cas où celui-ci n'est pas lui-même le chef ;
- La cellule de gestion d'incident prend en charge la gestion tactique de l'incident ;
- Le Conseil d'Administration donne les orientations stratégiques à la cellule de gestion d'incident.

Pour les risques moyens et faibles, la prise en charge se fait par les processus normaux déjà établis (exemple: services informatique, bâtiments, ressources humaines, etc.) ou par le coordonnateur PCA et le gestionnaire de l'unité affectée.

✓ Des types de risque

Les risques peuvent être:

- opérationnels (technologie de l'information, ressources humaines, finances, crédits, etc.) ; ce sont des risques liés aux métiers ;
- des risques d'investissement ; ce sont des risques créés par l'environnement financier ;
- des risques pays (grèves, guerre, tsunامي, tremblement de terre, incendie, indisponibilité de carburant, instabilité politique, corruption, conditions climatiques extrêmes, risques sanitaires, etc.) ; ce sont des risques qui ne dépendent pas ni du métier, ni de l'agent, mais de l'environnement socio-économique.

✓ Du management des risques

Les risques peuvent être traités de façons différentes :

- les risques peuvent être acceptés ;
- les risques peuvent être transférés (cas des assurances) ;
- les risques peuvent être traités (éliminer ou faire éliminer les risques).

I.2.4. De la cartographie des risques

La *cartographie* des risques est une démarche qui consiste à identifier, apprécier leur impact et leur probabilité, classer et surveiller les risques inhérents aux activités d'une organisation. *La cartographie des risques est l'affaire de l'audit et des finances.*

I.2.5. De l'impact d'un risque

L'impact d'un risque se définit comme étant les conséquences négatives engendrées par l'arrivée du risque⁵. Il se calcule à base du chiffre d'affaire. C'est le rapport entre la perte subie et la Durée Maximale d'Interruption Admissible (DMIA en sigle) ou Perte de Données Maximale Admissible (PDMA). C'est une valeur entière variant de 1 à 4.

Il faut pour cela une commission au sein de l'entreprise pour statuer sur ces valeurs.

Le tableau ci-dessous retrace la classification des impacts d'un risque :

VALEUR	IMPACT
1	Faible
2	Moyen
3	Elevé
4	Grave

I.2.6. De la probabilité d'un risque

La probabilité d'un risque est le nombre de fois que celui-ci se produit. En d'autres termes, c'est la fréquence de l'événement. La probabilité d'un risque est une valeur entière variant de 1 à 4.

La fixation de ces valeurs fait également appel à une commission au sein de l'organisation.

Le tableau ci-dessous nous donne la classification de probabilités d'un risque :

⁵ blogplm.com

VALEUR	IMPACT	FREQUENCE
1	Faible	Rarement
2	Moyen	Quelques fois
3	Elevé	Souvent
4	Grave	Toujours

I.2.7. De la valeur d'un risque

La valeur d'un risque est le produit de la valeur de son impact et celle de sa probabilité. C'est à base du tableau des valeurs des risques que l'on détermine le type de risque (faible, moyen, majeur ou élevé et catastrophique ou critique).

I.2.8. De l'activité

Une activité est un ensemble d'une ou de plusieurs tâches ayant une finalité définie. A titre d'exemple, l'octroi de crédit dans une institution financière est une activité.

I.2.9. De la perturbation

Une perturbation est un incident anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la délivrance prévue de produits ou services selon les objectifs d'une organisation.

CHAPITRE II : TYPES D'ORGANISATION ET SYSTEME DE MANAGEMENT DE CONTINUITE D'ACTIVITES

II.1. Les types d'organisation de continuité d'activités

L'organisation d'un plan de continuité peut se faire soit par *processus* (processus d'octroi de crédit), soit par *métier* (métier technologie de l'information, métier ressources humaines, métier logistique). Comme un processus peut faire intervenir plusieurs métiers, il est recommandé d'organiser la continuité par processus.

II.2. Système de Management de Continuité d'Activités

Un Système de Management de Continuité d'Activités (SMCA en abrégé) est un processus de gestion globale qui identifie les menaces potentielles pour l'organisation et les impacts de ces menaces sur les opérations de cette dernière. Il permet de mettre en place des réponses face aux diverses situations d'interruptions partielles ou totales, effectives ou potentielles des activités de

l'entreprise. Le SMCA comprend la Politique de Continuité d'Activités (POCA en sigle), le Comité de Gestion de la Continuité d'Activités (COGCA en sigle) et le Comité de Crise.

De la politique de continuité d'activités

La politique de continuité d'activités comprend :

- les objectifs : ici, on se pose la question de savoir «***pourquoi l'institution veut mettre en place un plan de continuité ?***» ;
- le périmètre de continuité : ici, on se pose la question de savoir «***quels sont les cibles ou les objets de la continuité ?***» (pour une institution de microfinance par exemple: siège uniquement ? ou toutes les agences ?, processus épargne et crédits ? ou tous les processus ?, etc.) ;
- le référentiel de continuité : ici, on se pose la question de savoir «***sur quelles normes on se base pour mettre sur pied un plan de continuité ?***» (norme 22301, norme 22311 par exemple) ;
- la législation : ici, on se pose la question de savoir «***sur quelles lois on se base pour élaborer un plan de continuité ?***» (la législation du pays par exemple) ;
- la responsabilité : ici, on se pose la question de savoir «***qui sera responsable de quoi ?***».

➤ Du comité de gestion de la continuité d'activités

Le Comité de Gestion de Continuité d'Activités est composé :

- du CA qui a pour rôle de **donner** les orientations de la continuité;
- du DG qui a pour rôle d'**instruire** la continuité ;
- du Comité de Direction (CODIR en sigle) qui a pour rôle de **superviser** la continuité ;
- du Directeur Administratif et Financier (DAF en sigle) qui a pour rôle d'**investir** dans la continuité;
- de l'Auditeur qui a pour rôle d'**initier** la continuité ;
- du Directeur des Ressources Humaines (DRH en abrégé) qui a pour rôle de **fournir** les compétences à la continuité ;
- du Risque Manager qui a pour rôle de **garantir** la continuité (fait la cartographie des risques);
- du Responsable IT qui a pour rôle de **déployer** le dispositif de continuité ;

- du Chargé des Affaires Juridiques qui a pour rôle de **légitimer** (conformité à la loi) la continuité ;
- du Responsable de la Continuité qui a pour rôle d'**assurer** et d'**assumer** la continuité (élabore la politique de continuité).

➤ Du comité de crise

Le comité de crise (la cellule de crise) est un regroupement d'individus chargé de décider les actions de communication devant limiter la crise et ses effets sur l'organisation. Le comité de crise joue un rôle clé dans l'activation des dispositifs du PCA qui sont les plus adaptés à la situation. Le comité de crise a deux instances: le comité de crise proprement dit et l'équipe de crise. Le comité de crise est composé du Directeur Général, d'un membre influent du Conseil d'Administration et de tous les managers. L'équipe de crise est composée uniquement d'experts en logistique, en informatique, en finances, en ressources humaines et en services publics (eau, électricité, télécommunication, Internet, etc.).

CHAPITRE III : SCHEMA DIRECTEUR ET CARTOGRAPHIE DES RISQUES A LA CECADM

III.1. Schéma directeur de la continuité d'activités

Pour chaque risque, il faut inventorier les différents scénarii possibles, et pour chaque scénario, il faut un dispositif approprié. Les scénarii sont les mesures (décisions, dispositions) à prendre pour un risque déterminé tandis que le dispositif est la transformation des décisions en infrastructures matérielles.

Le tableau ci-dessous constitue un exemple formel d'un schéma directeur de continuité d'activités:

CARTOGRAPHIE	PCA	DISPOSITIF
Risque A	Scénario A	Projet PCA A
	Scénario A'	
	Scénario A''	
Risque B	Scénario B	Projet PCA B
Risque C	Scénario C	Projet PCA C

Remarque:

Si les scénarii d'un risque ne marchent pas, on passe en **mode dégradé**. A titre illustratif, l'activité de «formation» exige de l'électricité. S'il n'y a pas d'électricité, on recourt à un groupe électrogène, et en cas de manque de carburant, on se rabat sur les panneaux solaires. Si aucune des solutions n'est disponible, on doit s'arranger à ce que la formation continue avec des moyens de bord. En d'autres termes, si tous les scénarii d'un risque échouent, on passe au **service minimal**.

III.2. Cartographie des risques à la CECADM

Le tableau ci-dessous répertorie les risques pouvant être rencontrés à la CECADM. Toutefois, cette liste n'est pas exhaustive. Pour toutes fins utiles, rappelons ce qui suit :

- les risques peuvent être critiques (catastrophiques), élevés (majeurs), moyens ou faibles ;
- la valeur du risque est égale au produit de son impact et de sa probabilité ;

Le risque est critique si sa valeur est comprise entre 12 et 16, il est élevé quand sa valeur est comprise entre 8 et 11, il est moyen quand sa valeur est comprise entre 4 et 7 et il est faible quand sa valeur est comprise entre 1 et 3.

Cartographie des risques à la CECADM

SERIE	CATEGORIE DE RISQUE	IMPACT	PROBA BILITE	VALEUR	TYPE
	RISQUES PAYS				
1.	Tremblement de terre	4	1	4	M
2.	Manque de courant électrique	4	3	12	C
3.	Surtension et sous-tension électrique	3	2	6	M
4.	Inondation	4	1	4	M
5.	Tsunami	4	1	4	M
6.	Manifestations	4	1	4	M
7.	Conditions de température extrême	2	1	2	F
8.	Pollution	3	1	3	F
9.	Foudre	3	2	6	M
10.	Rayonnement électromagnétique	2	1	2	F
11.	Pandémies	4	1	4	M

12.	Actes terroristes	4	1	4	M
13.	Braquage	2	1	2	F
RISQUES INSTITUTIONNELS					
1.	Perte des données informatiques	4	1	4	M
2	Crash disque serveur	4	1	4	M
3	Intrusion	4	1	4	M
4	Perte de configuration	3	1	3	F
5	Indisponibilité de personne clé	3	2	6	M
6	Départ massif du personnel	4	1	4	M
7	Indisponibilité du réseau informatique	4	1	4	M
8	Risque de non-conformité à la législation	2	2	4	M
9	Départ massif des membres	3	1	3	F
10	Incendie de l'immeuble	4	1	4	M
11	Manque de courant électrique	4	3	12	C
12	Surtension et sous-tension électrique	3	2	6	M
13	Cambriolage	4	1	4	M
14	Braquage	2	1	2	F
RISQUES FINANCIERS					
1	Manque de liquidité	4	2	8	E
2	Obsolescence du matériel	2	1	2	F
3	Risque de contrepartie	2	1	2	F
4	Concurrence locale	2	2	4	M
5	Cambriolage	4	1	4	M
6	Risque de marché	2	1	2	F
7	Faillite des banques ou des établissements financiers partenaires	4	1	4	M
RISQUES OPERATIONNELS					
1	Manque d'entretien du matériel	2	1	2	F
2	Mauvaise utilisation d'outils informatiques	2	1	2	F

3	Erreur de programmation	4	1	4	M
4	Défaillance de la climatisation	1	1	1	F
5	Obsolescence du matériel	2	1	2	F
6	Absence de sauvegarde	4	1	4	M
7	Insuffisance de protection du matériel	4	1	4	M
8	Manque d'archivage	4	1	4	M
9	Vol interne	3	1	3	F
10	Conditions de température extrême	2	1	2	F
11	Faillite des banques ou des établissements financiers partenaires	4	1	4	M
12	Perte des lignes de transmission des données	4	1	4	M
13	Manque de courant électrique	4	3	12	C

Le tableau des risques ci-dessus montre que le niveau de risque le plus rencontré à la CECADM est le niveau «moyen». Cela se justifie par le fait que les risques inventoriés ont une faible probabilité (ils surviennent rarement) même si l'impact est moyen, élevé ou grave. Comme le PCA est recommandé uniquement pour les risques critiques, et que très peu de risques à la CECADM tombent dans cette catégorie, la CECADM juge bon d'élaborer les scénarii pour les risques critiques, élevés et moyens.

CHAPITRE IV : SCENARI DES RISQUES RETENUS A LA CECADM

Risque	Niveau du risque	Mesures préventives	Durée maximale d'interruption de service acceptable	Mesures curatives mises en place à la CECADM	Mesures curatives supplémentaires envisagées	Responsables
Manque de courant électrique, surtension et sous-tension	C	- Acquisition de générateur de courant de secours avec inverseur automatique - Onduleurs	4 heures	- Disponibilité de deux (2) générateurs de courant au siège et disponibilité d'un groupe électrogène pour chaque agence et guichet ; - Constitution d'un stock stratégique de carburant ; - Disponibilité d'un agent de maintenance de groupe électrogène.	- Mise en place de panneaux solaires ; - Contrat de maintenance des équipements électriques avec une maison spécialisée ; - Disponibiliser les régulateurs de tension.	DAF + CHSCT ⁶
Manque de liquidité	E	Mise en place d'un plan de trésorerie mensuel	15 jours	- Diversification des banques partenaires ; - Suivi régulier des liquidités ; - Recours à l'emprunt.	- Priorisation dans l'octroi des crédits - Encadrement des charges - La cassation des placements.	DG + DAF + DO ⁷
Incendie de l'immeuble	M	- Assurance incendie et risques connexes - Extincteurs		- Souscription à la police d'assurance incendie et risques connexes à une maison d'assurance locale ; - Disponibilité d'un extincteur par bloc administratif et par agence et guichet.	- Achat de détecteurs de fumée ; - Formation du personnel sur l'utilisation des extincteurs ; - Elaboration d'un plan de relocalisation des activités vers un site de secours alternatif ou location temporaire d'un local ; - Achat d'un appareil extincteur mobile ;	DAF + CHSCT + BI ⁸

⁶ Comité d'Hygiène, de Sécurité et des Conditions de Travail

⁷ Direction des Opérations

⁸ Bureau de l'Informatique

					• Disponibilité de deux (2) bacs à sable et leurs accessoires (pelle et seau) par bloc ; • Aménagement d'un issu de secours ; • Porter à la connaissance du personnel le numéro de secours de la police de protection civile ; • Prévision d'une cellule d'urgence médico-psychologique.	
Tremblement de terre	M	-	15 jours	-	• Elaboration d'un plan de relocalisation des activités vers un site de secours alternatif ou location temporaire d'un local ; • Prévision d'une cellule d'urgence médico-psychologique.	DG + DAF + BI
Inondation	M	-	15 jours	-	• Elaboration d'un plan de relocalisation des activités vers un site de secours alternatif ou location temporaire d'un local ; • Prévision d'une cellule d'urgence médico-psychologique.	DG + DAF + BI
Perte de données informatique	M	• Backup et restauration de la base de données	1 jour	• Deux sauvegardes par jour sur un disque dur externe (à l'ouverture et à la fermeture de l'agence) ; • Deux sauvegardes sur un support inamovible par jour (à l'ouverture et à la fermeture de l'agence).	• Multiplier la fréquence des sauvegardes ; • Instaurer un système de réplication (miroir) ; • Sauvegarde sur Cloud.	DAF + BI
Crash disque serveur	M	• Réinstallation du système d'exploitation ;	1 jour	• Trois serveurs disponibles (un de production, un de test et	• Instaurer un système de réplication (miroir) ; • Disponibilité des copies	DAF + BI

		Backup et restauration de la base de données ;		de réserve et un de formation) ;	du système d'exploitation et du Core Banking System ;	
Concurrence locale	M	- Taux débiteur préférentiel ; - Accès facile au crédit.	-	- Taux débiteur bas par rapport aux taux débiteurs pratiqués ailleurs ; - Temps relativement court dans le traitement du dossier de crédit ;	- Augmentation de la durée du crédit ; - Diminution progressive du taux débiteur ; - Diversification des produits et des moyens de paiement ; - Garantie de la couverture nationale.	DG + DO
Tsunami	M	-	-	-	- Elaboration d'un plan de relocalisation des activités vers un site de secours alternatif ou location temporaire d'un local ; - Prévision d'une cellule d'urgence médico-psychologique.	DG + DAF + BI
Cambriolage	M	Système de surveillance et de sécurité		- Equipe de gardiennage ; - Existence de caméras de surveillance au siège ; - Accès limité aux endroits sensibles.	- Installation de caméra de surveillance dans toutes les agences et guichets ; - Monitoring permanent du système de surveillance ; - Installation d'un système d'alerte dans chaque agence et guichet ; - Souscription à une police d'assurance.	DAF + CHSCT
Intrusion informatique	M	Mise en place d'un système informatique de protection.	5 jours	- Equipements informatiques protégés par des mots de passe complexes ; - Accès physique au local informatique limité ; - Installation des anti-virus ; - Mise à jour fréquente du	- Actualisation régulière de la charte informatique ; - Utilisation des moyens de protection récents ; - Renforcement des capacités du personnel IT	BI

				- Core Banking System ; - Charte informatique élaborée. - Sensibilisation du personnel.		
Erreur de programmation	M	Tests de discordance.	5 jours	- Tests de discordance effectués régulièrement ; - Disponibilité d'un serveur de test.	Tests de discordance réguliers.	CODIR
Faillite d'une banque ou d'un établissement financier partenaire	M	Multiplication des partenaires financiers.	-	Existence de neuf (9) partenaires financiers.	Suivi régulier de la santé financière des partenaires financiers.	DG + DAF
Manifestations	M	-	-	-	- Elaboration d'un plan de relocalisation des activités vers un site de secours alternatif ou location temporaire d'un local ; - Prévision d'un service minimum.	DG + DAF + BI
Indisponibilité des lignes de transmission des données	M	Existence d'une ligne secondaire.	15 jours	Existence d'une seule ligne de transmission de données.	- Duplication des lignes de transmission de données ; - Duplication de câblage au niveau du réseau local.	DAF + BI
Foudre	M	Installation des paratonnerres et des parafoudres.	2 jours	- Des paratonnerres et des parafoudres sont dans certaines agences et guichets ; - Existence de la charte informatique.	Installation des paratonnerres et des parafoudres dans les agences et guichets qui n'en ont pas.	DAF + Comité de sécurité
Indisponibilité de personnel clé	M	Prévision des remplaçants.	2 jours	La plupart des chefs de services ont des suppléants.	Renforcement des capacités des suppléants pour les services clé ;	CA + DG + DAF
Absence de sauvegarde	M	Prévision d'une politique de sauvegarde.	-	Deux sauvegardes par jour : une sur le système lui-même et une autre sur disque amovible.	- Elaboration d'une politique de sauvegarde externe notamment sur le Cloud ; - Automatisation de la sauvegarde (sauvegarde programmée).	DAF + BI

Insuffisance de protection du matériel informatique	M	• Prévision d'une protection physique et logicielle ; • Sensibilisation des utilisateurs.	-	• Une charte informatique a été élaborée.	• Sensibilisation permanente des utilisateurs ; • Acquisition du matériel de protection à la page.	DAF + BI
Manque d'archivage des documents	M	• Prévision d'une politique d'archivage.	-	• Des containers sont prévus pour la conservation des dossiers de crédit et des pièces comptables ; • Des étagères et des armoires sont prévues pour classer les autres documents.	• Acquérir un outil logiciel pour archiver électroniquement les différents documents.	DG + DAF + CODIR
Départ massif du personnel	M	• Existence des conditions de travail adaptées au personnel.		• Motivation du personnel par des primes ; • L'octroi de crédit à un taux préférentiel ; • Uniformes supportées totalement par l'institution ; • Etc.	• Création des conditions de travail adaptées aux besoins du personnel ; • Planification d'une bonne gestion de la carrière.	CA + DG
Indisponibilité du réseau informatique	M	• Maintenance des équipements ; • Configuration adéquate ; • Protection assurée ;	-	• Entretien réguliers ; • Réseau protégé.	• Duplication du câblage réseau ; • Maintenance permanente du matériel ; • Stock de sécurité des éléments indispensables ; • Formation et disponibilité du personnel IT ; • Amélioration de la protection des équipements réseau.	DAF + BI
Pandémies	M	• Prise des mesures préventives d'hygiène	-	• Quelques mesures préventives ont été prises (installation des robinets à l'entrée de l'institution pour se laver les mains, distribution des masques au personnel etc.)	• Informer et sensibiliser le personnel ; • Doter le personnel d'un équipement approprié.	CA + DG + DAF + CHSCT

Risque de non-conformité à la législation	M	Se conformer à la législation.	-	- Les circulaires et les règlements édictés par la Banque Centrale sont mis en application dans les délais réglementaires ; - Les statuts, les règlements et les manuels de l'IMF ont été élaborés en tenant compte des codes et des lois régissant les banques et les institutions de microfinance.	- Vulgariser les circulaires, les statuts et les règlements au sein du personnel ; - Mettre jour les différents textes réglementaires chaque fois que de besoin ; - Consulter régulièrement le site de l'autorité de supervision pour s'enquérir des nouveautés et des mises à jour éventuelles ;	DG + DAF + CJ ⁹
Actes terroristes (cambriolage)	M	Renforcement des mesures de sécurité	-	- Enceintes clôturées et renforcées par des fils barbelés ; - Mise en place des check points ; - Installation de caméras de surveillance ; - Mise en place d'une équipe de gardiennage ; - Installation des buses remplies de sable le long de la clôture des enceintes.	- Aménagement et organisation adéquats des check points ; - Prévision d'une cellule d'urgence médico-psychologique.	DG + DAF + CHSCT

⁹ Conseiller Juridique

CHAPITRE V : CONCLUSION

Le Plan de continuité des activités de la CECADM est un outil qui sert de guide dans la prévention et la gestion des risques. Il donne des orientations qui comprennent l'identification, l'analyse, la mesure, le suivi et le contrôle des risques.

Des méthodes quantitatives permettent d'identifier, de suivre et de contrôler les différents facteurs qui sont utilisés pour évaluer les risques.

Le plan de continuité des activités de la CECADM permet alors de prendre des mesures de prévention pour empêcher la survenance d'une perturbation éventuelle.

Sa mise en œuvre pourra contribuer à renforcer la crédibilité de la CECADM et générer de nouvelles opportunités de croissance.

Des mesures de précaution sont prises pour se prémunir contre les impacts d'un risque survenu. L'objectif étant d'assurer une reprise rapide des activités normales et d'éviter qu'une perturbation des procédures n'ait des répercussions sur l'ensemble du système.

Il implique les organes de gestion et le personnel en cas de survenance d'une perturbation majeure pouvant ébranler la bonne marche des activités de la Coopérative.

Il requiert une mise à jour régulière pour l'adapter aux nouvelles circonstances relatives à l'apparition de nouveaux risques significatifs pouvant compromettre la pérennité de la CECADM.

Fait à Bujumbura, le 13.août 2020

Pour le Conseil d'Administration

Le Secrétaire

Nestor BIGIRIMANA

Lieutenant-Colonel



Le Vice-président

Bonaventure MATORE

Lieutenant-Colonel



Le président

Audace NDUWUMUNSI

Général-Major

