**PLAN DE REPRISE D’ACTIVITÉ (PRA)**

**Microfinance Batata**

**1. OBJECTIFS DU PRA**

* Assurer la **continuité des services financiers essentiels** (crédit, épargne, transferts).
* Protéger la **donnée client**, la **réputation** et la **situation financière**.
* Permettre une **reprise rapide et contrôlée** des activités après un sinistre.
* Satisfaire aux **exigences réglementaires** (BCEAO, normes ISO 22301, RGPD, etc.).
* Instaurer une **culture de résilience** organisationnelle et technologique.

**2. CHAMP D’APPLICATION**

* **Unité concernée** : l’ensemble du réseau (siège + agences).
* **Activités critiques** couvertes :
  + Traitement des transactions (dépôts, retraits)
  + Services de crédit
  + Paiements digitaux et mobile money
  + Reporting réglementaire
  + Plateforme Core Banking et outils CRM
* **Écosystème** : clients, prestataires IT, partenaires, fournisseurs de connectivité.

**3. ANALYSE D’IMPACT MÉTIER (BIA)**

| **Processus critique** | **RTO** | **RPO** | **Impact financier** | **Impact réputationnel** |
| --- | --- | --- | --- | --- |
| Traitement dépôts/retraits | 2 h | 30 min | Fort | Très élevé |
| Paiements digitaux | 4 h | 1 h | Élevé | Élevé |
| Traitement des crédits | 12 h | 2 h | Élevé | Moyen |
| Rapport BCEAO | 24 h | 8 h | Moyen | Faible |
| Support client | 6 h | 1 h | Moyen | Élevé |

**4. CARTOGRAPHIE DES RISQUES**

| **Risque** | **Probabilité** | **Gravité** | **Mesures préventives** |
| --- | --- | --- | --- |
| Cyberattaque (ransomware) | Élevée | Élevée | Antivirus, firewall, MFA, formation |
| Incendie dans une agence | Faible | Élevée | Extincteurs, plan d’évacuation, backups |
| Panne serveur principal | Moyenne | Élevée | Hébergement redondant, PRA |
| Coupure internet généralisée | Moyenne | Moyenne | Fournisseurs multiples, routeurs 4G |
| Défaillance humaine | Élevée | Moyenne | Procédures, formations, supervision |

**5. GOUVERNANCE DU PRA**

**Comité de gestion de crise :**

| **Poste** | **Nom** | **Contact** | **Rôle** |
| --- | --- | --- | --- |
| Directeur général | M. Diallo | 77 123 45 67 | Activation PRA, communication |
| Responsable IT | Mme Ndiaye | 78 987 65 43 | Coordination technique |
| Responsable conformité | M. Diop | 76 456 78 90 | Veille réglementaire |
| Responsable RH | Mme Sarr | 77 345 67 89 | Mobilisation du personnel |
| Chargé de communication | M. Ba | 70 112 34 56 | Communication interne/externe |

**6. RESSOURCES TECHNIQUES ET LOGISTIQUES CRITIQUES**

* Core Banking System (CBS)
* Base de données SQL / PostgreSQL
* Application mobile
* Backup cloud (AWS S3 / Wasabi)
* Systèmes de messagerie sécurisés (e.g. ProtonMail)
* UPS, générateurs, routeurs 4G
* Site de repli opérationnel (agence secondaire ou coworking sécurisé)

**7. STRATÉGIES DE CONTINUITÉ & REPRISE**

**Scénarios & réponses**

| **Scénario** | **Réponse immédiate** | **Plan de continuité** |
| --- | --- | --- |
| Perte totale du serveur CBS | Bascule automatique serveur miroir | Reconfiguration en moins de 1 h |
| Cyberattaque | Isolement réseau, audit forensics | Reprise via backup journalier |
| Incendie siège | Déclenchement alerte & repli | Bascule agence secondaire |
| Rupture Internet/énergie | FAI secondaire, groupe électrogène | VPN mobile, site secours si besoin |

**8. TESTS & SIMULATIONS**

* **Tests trimestriels** de bascule serveur + restauration backup.
* **Exercice annuel** de simulation de crise (cyberattaque, panne réseau).
* **Audit externe** de conformité PRA tous les 2 ans.
* **Tableau de bord de résilience** :

| **Indicateur** | **Cible** | **Résultat actuel** |
| --- | --- | --- |
| Temps de bascule Core Banking | < 2 h | 1h45 |
| Disponibilité globale système | > 99,5% | 99,7% |
| Taux de succès des backups | 100% | 100% |
| Taux de formation du personnel | 90% / an | 82% |

**9. COMMUNICATION EN CAS DE CRISE**

| **Cible** | **Message clé** | **Canal** | **Responsable** |
| --- | --- | --- | --- |
| Clients | Service temporairement suspendu | SMS, WhatsApp, app | Resp. communication |
| Partenaires | Situation sous contrôle, plan activé | Email, téléphone | Resp. partenariat |
| Personnel | Procédures PRA activées | Intranet, Email | Resp. RH |
| Régulateur | Notification incident + rapport détaillé | Email, plateforme BCEAO | Resp. conformité |

**10. DOCUMENTATION & MISE À JOUR**

* Version actuelle : v1.2 (Mai 2025)
* Prochaine révision : Novembre 2025
* Responsable de la mise à jour : Responsable IT + Comité de crise
* Format de conservation : papier + numérique (intranet sécurisé)

**11. ANNEXES**

* 📑 Annexe A : Fiche d'activation PRA
* 📑 Annexe B : Arbre décisionnel d'incident
* 📑 Annexe C : Cartographie des dépendances critiques
* 📑 Annexe D : Procédure de restauration système
* 📑 Annexe E : Liste contacts d’urgence (personnel, prestataires, régulateurs)