**📑 Plan de Continuité d’Activité (PCA) – OptiValue**

*(version 1.0 – juillet 2025)*

Le PCA décrit **comment préserver les processus métiers critiques** d’OptiValue lorsqu’un événement perturbe gravement les ressources habituelles (locaux, personnel, SI, fournisseurs). Il complète le PRA – axé sur la restauration technique – en couvrant l’**organisation globale de la continuité**.

**1. Introduction**

* **Contexte :** OptiValue traite des données sensibles pour ses clients ; une interruption prolongée affecterait fortement sa chaîne de valeur.
* **Référentiels :** ISO 22301, ISO 27001, NIS2, RGPD, exigences clients.

**2. Objectifs**

| **Objectif** | **Indicateur** | **Seuil** |
| --- | --- | --- |
| Maintenir les processus critiques | Taux de disponibilité | ≥ 99,5 % |
| Limiter l’impact financier d’une crise | Pertes < 0,5 % CA annuel | 72 h |
| Protéger l’image de marque | Nombre d’articles négatifs | 0 majeur |

**3. Gouvernance de la continuité**

| **Rôle** | **Titulaire** | **Responsabilités** |
| --- | --- | --- |
| *Business Continuity Manager* (BCM) | RSSI | Piloter PCA, organiser exercices |
| *Crisis Manager* | COO | Décider déclenchement PCA, coordonner cellules |
| *Process Owner* | Managers métiers | Maintenir fiches de continuité |
| *Communication Officer* | Dir. Marketing | Messages internes / externes |

**4. Périmètre et hypothèses**

* **Sites concernés :** Siège Paris, Data Center 1 (Paris-DC1), Data Center 2 (AMS-DC2), plateformes cloud (AWS eu-west-3).
* **Processus classés critiques (BIA) :**
  1. Traitement de données client (plateforme OptiAnalytics)
  2. Support client 24/7
  3. Facturation et cash-flow
  4. Gestion des accès / identité (IAM)
* **Hypothèses** : indisponibilité max. 30 jours d’un site physique ; personnel clé réduit de 40 % ; réseau Internet national toujours partiellement accessible.

**5. Analyse d’impact métier (BIA) – synthèse**

| **Processus** | **RTO** | **RPO** | **Impact (€/jour)** | **Solution de continuité** |
| --- | --- | --- | --- | --- |
| OptiAnalytics | 4 h | 15 min | 150 k€ | Bascule cloud active-active |
| Support client | 1 h | 0 | 50 k€ | Routage téléphonie vers centre partenaire |
| Facturation | 24 h | 4 h | 25 k€ | SaaS doublé + exports S3 |
| IAM | 2 h | 0 | 75 k€ | Cluster redondant multi-régions |

**6. Stratégie de continuité**

1. **Préventif** : redondance active-active de l’infra, sauvegardes chiffrées 3-2-1, réplication continue (DR-DB, S3-cross-region).
2. **Réactif** : bascule manuelle ou automatique (selon service) dans un délai < RTO.
3. **Organisationnel** : contrat « work-from-anywhere », hotline RH, accès VPN SD-WAN prioritaire.

**7. Organisation de crise**

* **Cellule de crise** (15 m après alerte) : Crisis Manager, BCM, DSI, RH, Communication.
* **Cellule support IT** : DSI + équipes Ops / SRE.
* **Cellule métier** : Process Owners.
* **Escalade** : si incident dépasse 6 h ou touche la donnée perso → notification CNIL et clients.

**8. Procédures de continuité par processus**

**8.1 OptiAnalytics**

1. Détection de panne sur DC1 → déclenchement failover vers AWS eu-west-3 (Route 53 health-check).
2. SRE vérifie cohérence base + files Kafka (mirror-maker).
3. Communication interne : Slack #crisis-tech, statut « limited ».

*(Fiche détaillée en annexe PCA-F01)*

**8.2 Support client**

* Routage téléphonie Genesys → site partenaire Maroc.
* Agents « OptiAssist » se connectent via VDI Citrix hébergé en Europe.

**8.3 Facturation**

* Export quotidien chiffré (PGP) → Bucket S3-dr.
* Si ERP on-prem indisponible > 8 h : activation licence SaaS « ERP-Cloud-Lite ».

*(…procédures similaires pour chaque processus…)*

**9. Plans de communication**

* **T0** : message interne Teams + mail « Incident en cours, PCA activé ».
* **T0+1 h** : point client via portail status.optivalue.com.
* **T0+6 h** : communiqué presse conditionnel (pré-rédigé).

**10. Exercices et tests**

| **Type** | **Fréquence** | **Exemples** |
| --- | --- | --- |
| Table-top « papier » | Trimestriel | Simulation coupure locale |
| Test technique | Semestriel | Bascule OptiAnalytics AWS ↔ DC1 |
| Exercice de crise (live) | Annuel | Scénario ransomware |

**11. Maintenance & amélioration continue**

* Revue PCA après chaque incident majeur.
* Audit interne ISO 22301 annuel.
* KPI : % réussite objectifs RTO/RPO, temps moyen de décision.

**12. Annexes PCA**

* **PCA-F01** Fiche OptiAnalytics (30 pages)
* **PCA-F02** Fiche Support client
* **PCA-C01** Check-list cellule crise
* **PCA-T01** Scripts d’automatisation bascule infra

**🛠️ Plan de Reprise d’Activité (PRA) – OptiValue**

*(version 1.0 – juillet 2025)*

Le PRA détaille **comment rétablir les ressources informatiques** d’OptiValue après un sinistre majeur (panne, cyber-attaque, incendie). Il est technique, orienté « retour à la normale ».

**1. Objectifs**

* **Remettre en production** tous les services IT dans les RTO/RPO définis.
* Limiter la **perte de données** via stratégies de sauvegarde.
* Assurer une **traçabilité** complète des actions (journal de reprise).

**2. Scénarios de sinistre couverts**

| **Code** | **Scénario** | **Probabilité** | **Gravité** | **Note** |
| --- | --- | --- | --- | --- |
| S-01 | Panne électrique majeure DC1 | Moyenne | Élevée | UPS 30 min |
| S-02 | Ransomware étendu | Faible | Critique | Double extorsion possible |
| S-03 | Incendie locaux siège | Faible | Élevée | Sauvegardes off-site |
| S-04 | Défaillance Cloud Provider zone eu-west-3 | Très faible | Élevée | Multi-region |

**3. Architecture de secours**

* **Infra on-prem** : cluster VMware vSAN en double site (Paris, Amsterdam).
* **Cloud** : AWS multi-Account : prod-eu-west-3, dr-eu-central-1.
* **Sauvegardes** :
  + Base de données → Snapshots horaires (7 jours) + journaux WAL → Glacier (30 jours).
  + Fichiers → Object-lock S3 (immutabilité 14 jours).
  + Config Git → GitHub Enterprise + mirror privé.

**4. Matrice RTO / RPO système**

| **Service / Composant** | **RTO** | **RPO** | **Backup / Replica** | **Procédure** |
| --- | --- | --- | --- | --- |
| PostgreSQL Prod | 4 h | 15 min | pgBackRest + multi-AZ | PRA-DB-01 |
| Kafka | 3 h | 0 | MirrorMaker2 cross-region | PRA-MQ-02 |
| Active Directory | 2 h | 1 h | AD-DS sites & services | PRA-ID-03 |
| ERP | 24 h | 4 h | Snapshots VM + scripts IaC | PRA-ERP-04 |

**5. Déclenchement du PRA**

1. **Déclaration** : DSI ou SOC émet un *Incident P1* et contacte le CSR (Crisis Manager).
2. **Analyse rapide (15 min)** : gravité ≥ S-02 ou indisponibilité ≥ RTO → décision de déclencher PRA.
3. **Enregistrement** dans l’outil ITSM « ServiceNow-DR ».

**6. Phases de reprise**

| **Phase** | **Délai cible** | **Responsable** | **Actions clés** |
| --- | --- | --- | --- |
| **Confinement** | 0-2 h | SOC | Isolement réseau, arrêt VM infectées |
| **Éradication** | 2-6 h | SRE Lead | Patching, suppression backdoors |
| **Restauration minimale** | 6-12 h | DBA & CloudOps | Démarrage services critiques (liste priorisée) |
| **Validation métier** | 12-18 h | Process Owners | Tests fonctionnels, données |
| **Retour à la normale** | ≤ RTO total | DSI | Bascule trafic, déclaration fin PRA |

**7. Procédures techniques (extraits)**

**PRA-DB-01 : Restauration PostgreSQL**

1. **Pré-requis** : VM template « db-dr-node » via Terraform, storage EBS gp3.
2. **Étapes** :
   * Créer instance serveur DR (AWS eu-central-1).
   * Restaurer dernier *base backup* + rejouer WAL jusqu’à timestamp T-RPO.
   * Lancer script checksum\_verify.sh ; attendre sortie « OK ».
3. **Validation** : exécuter requête SELECT count(\*) FROM health\_check; → résultat = 1.

**PRA-MQ-02 : Reprise Kafka**

* Lancer ansible-playbook start\_kafka\_dr.yml (parallelism = 10).
* Vérifier ISR ≥ 3 via kafka-topics.sh --describe.

*(Procédures détaillées pour chaque composant en annexes PRA-Sxx)*

**8. Gestion des sauvegardes**

* **Politique 3-2-1 :** 3 copies, 2 supports, 1 hors-site immuable.
* **Chiffrement** : AES-256 pour dumps, TLS 1.3 en transit.
* **Test de restauration** : chaque sauvegarde aléatoire testée mensuellement (script *backup-drill*).

**9. Communications et reporting**

* **Canal principal** : Bridge Zoom dédié « DR-WarRoom ».
* **Journal de reprise** : Google Sheet partagé + export JSON.
* **Post-mortem** : dans 5 j ouvrés, incluant RCA, actions correctives, leçons apprises.

**10. Tests PRA**

| **Test** | **Périmètre** | **Méthode** | **Résultat attendu** |
| --- | --- | --- | --- |
| *Black Start* DC1 | Énergie coupée | Groupe électrogène + failover | Services critiques < 4 h |
| Simulation ransomware | VM bac à sable | Red Team + restore | 0 perte > RPO |
| Migration région AWS | Prod → DR | Route 53 switch | < 30 min interruption |

**11. Maintenance**

* Revue technique trimestrielle : versions, dépendances, IaC.
* Mise à jour RTO/RPO après chaque changement majeur.
* Audit externe biennal (ISO 27031).

**12. Annexes PRA**

* **PRA-S01** Script Terraform DR
* **PRA-S02** Playbook Ansible Kafka
* **PRA-Check-01** Liste de contrôle validation reprise
* **PRA-RCA-template** Modèle post-mortem

**➡️ Prochaines étapes**

1. **Validation interne** : faites relire PCA & PRA par les Process Owners et le Comité SSI.
2. **Signature de la Direction** pour engagement officiel.
3. **Planification des tests** (calendrier semestriel).