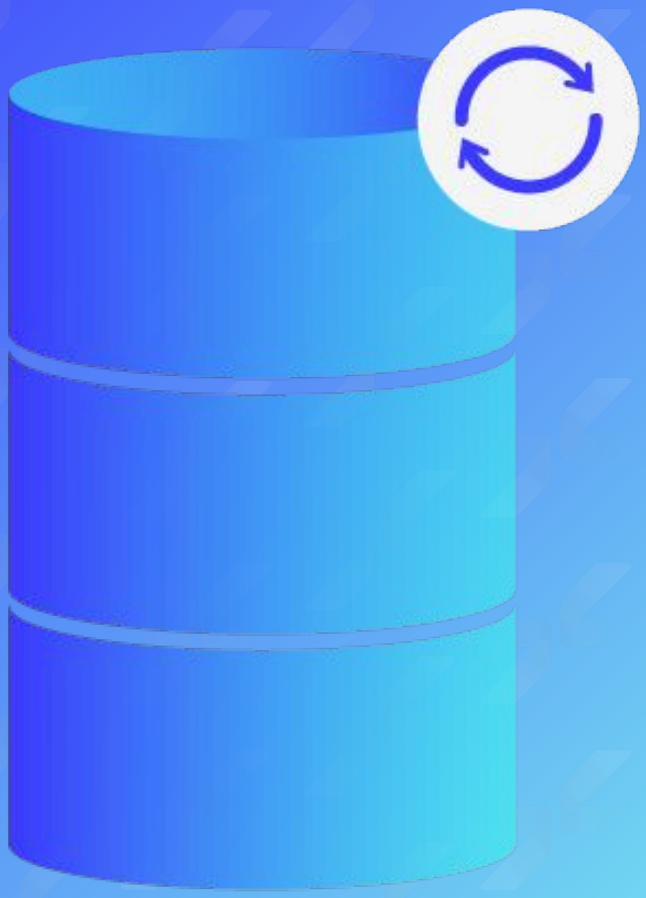
Vytalx

# Checklist de revue : Plan de reprise d'activité

Valider la capacité de reprise, mesurer les délais réels, prioriser les actions (30 minutes)



Vytalx

# Comment utiliser cette checklist ?

**Cochez chaque point selon votre situation.**
**L'objectif étant d'identifier rapidement les zones à risque**
**et de prioriser les actions qui améliorent réellement la capacité de restauration.**

## Mode d'emploi

1. **Choisissez un périmètre :**
   commencez par vos services les plus critiques (ex. serveurs/VM, fichiers, messagerie Microsoft 365, sites distants).

2. **Cochez chaque point :**
   - ✅ Oui = mis en place et fonctionnel
   - ⚠️ Partiel = mis en place mais incomplet / pas fiable / pas systématique
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   commencez par vos services les plus critiques (ex. serveurs/VM, fichiers, messagerie Microsoft 365, sites distants).

## Exemple

**"Tests de restauration mensuels"**
- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

## Scoring simple

**Barème**
- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

## Les 5 preuves attendues

1. Test PRA daté (scénario + résultat)
2. Mesure RTO/RPO réel (même approximatif)
3. Runbook (ordre + étapes)
4. RACI / contacts + escalade
5. Critères de retour en prod (failback) documentés

**Objectif :** Vérifier la reprise en cas d'incident cyber :
restaurer sur un environnement sain, éviter la réinfection,
prouver la restaurabilité.

Vytalx

# Périmètre PRA

**Un PRA efficace commence par un périmètre clair :**
**ce qui doit repartir en priorité, dans quels délais, avec quelles dépendances.**

## Vos services critiques

**Listez vos 8-10 éléments les plus critiques** (ex: ERP / messagerie / données sensibles ou réglementaires / auth / hyperviseur) **:**

_____
_____
_____
_____
_____
_____
_____
_____

## Objectifs de reprise (RPO / RTO)

- **RPO :** perte de données acceptable (ex. 4h) : _____
- **RTO :** durée d'arrêt acceptable (ex. 8h) : _____

**Consigne :** Renseignez un objectif "cible" pour chaque service critique (même approximatif).

| Service / Actif | Criticité | RPO cible | RTO cible | Dépendances clés | Mode de reprise prévu | Dernier test PRA |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Signaux de risque immédiat

- RTO/RPO non définis sur le top 5
- Mode de reprise non écrit (ou dépendances inconnues)
- Aucun test PRA récent sur les services critiques
- Reprise possible "sur le papier" mais accès d'urgence non prévu
- Failback (retour en prod) non envisagé

Vytalx

# Checklist : Fondations PRA

| Point de contrôle | Oui ✅ | Partielle ⚠️ | Non ❌ | N/A | Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté |
|---|---|---|---|---|---|
| Le PRA existe et est “propriétarisé” (version, date, responsable, périmètre) | ☐ | ☐ | ☐ | ☐ | |
| Le périmètre du PRA est clair (top services critiques + exclusions assumées) | ☐ | ☐ | ☐ | ☐ | |
| Les objectifs RTO/RPO sont définis pour les services critiques. | ☐ | ☐ | ☐ | ☐ | |
| Les scénarios couverts sont explicités (cyber, panne infra, site indisponible, erreur humaine) | ☐ | ☐ | ☐ | ☐ | |
| L’ordre de reprise est défini (dépendances : AD/DNS → réseau → apps → données) | ☐ | ☐ | ☐ | ☐ | |
| Les dépendances techniques sont documentées (DNS, certificats, VPN, hyperviseur, stockage, licences) | ☐ | ☐ | ☐ | ☐ | |
| Le mode de reprise est défini par service (site secondaire, cloud, restauration, contournement manuel) | ☐ | ☐ | ☐ | ☐ | |
| La capacité de reprise est disponible (compute, stockage, bande passante) ou planifiée | ☐ | ☐ | ☐ | ☐ | |
| Les accès d’urgence (“break-glass”) sont prévus (si AD indispo / comptes compromis) | ☐ | ☐ | ☐ | ☐ | |
| La documentation PRA est accessible hors SI (si le SI principal est indisponible) | ☐ | ☐ | ☐ | ☐ | |
| Les responsabilités sont définies (technique + métier + validation) | ☐ | ☐ | ☐ | ☐ | |
| Le plan de communication existe (qui prévenir, quand, comment) | ☐ | ☐ | ☐ | ☐ | |

**À ne pas oublier :** Un PRA non testé finit toujours par se comporter comme “pas de PRA”.

Vytalx

# Checklist : Exécution (runbook & opérationnel)

| Point de contrôle | Oui ✅ | Partielle ⚠️ | Non ❌ | N/A | Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté |
|---|---|---|---|---|---|
| Le runbook est exploitable (étapes numérotées, prérequis, ordre de reprise) | ☐ | ☐ | ☐ | ☐ | |
| Le déclenchement du PRA est cadré (qui décide, critères, escalade) | ☐ | ☐ | ☐ | ☐ | |
| Les accès nécessaires sont connus et disponibles (VPN, bastion, comptes, clés, certificats) | ☐ | ☐ | ☐ | ☐ | |
| Le PRA fonctionne en mode dégradé (ex. AD indispo, messagerie indispo) | ☐ | ☐ | ☐ | ☐ | |
| Les prérequis réseau sont documentés (DNS, routage, VLAN, firewall, NAT, proxies) | ☐ | ☐ | ☐ | ☐ | |
| Les prérequis applicatifs sont documentés (licences, secrets, connecteurs, flux) | ☐ | ☐ | ☐ | ☐ | |
| La reprise multi-sites / sites distants est prévue (si concerné) | ☐ | ☐ | ☐ | ☐ | |
| La reprise est possible sans IT sur place (si sites distants) | ☐ | ☐ | ☐ | ☐ | |
| Les critères de succès sont définis (quand dit-on “c’est reparti” ?) | ☐ | ☐ | ☐ | ☐ | |
| Un point de non-retour / rollback est prévu (si reprise partielle ou instable) | ☐ | ☐ | ☐ | ☐ | |
| Le retour en production (failback) est envisagé (même à haut niveau) | ☐ | ☐ | ☐ | ☐ | |
| Les actions post-incident sont prévues (durcissement, changement d’accès, audit) | ☐ | ☐ | ☐ | ☐ | |

**Piège classique :** Le runbook existe… mais les accès, certificats ou dépendances ne sont pas disponibles le jour J.

Vytalx

# Checklist : Tests & preuves

| Point de contrôle | Oui ✅ | Partielle ⚠️ | Non ❌ | N/A | Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté |
|---|---|---|---|---|---|
| Un calendrier de tests PRA existe (trimestriel / semestriel selon criticité) | ☐ | ☐ | ☐ | ☐ | |
| Un test PRA complet récent a été réalisé (≤ 6 mois sur services critiques) | ☐ | ☐ | ☐ | ☐ | |
| Les tests couvrent plusieurs scénarios (panne infra, erreur humaine, cyber, site indispo) | ☐ | ☐ | ☐ | ☐ | |
| Le RTO réel est mesuré (chronométré) et comparé au RTO cible | ☐ | ☐ | ☐ | ☐ | |
| Le RPO réel est mesuré (point de reprise) et comparé au RPO cible | ☐ | ☐ | ☐ | ☐ | |
| La validation inclut un contrôle applicatif (pas seulement “la VM démarre”) | ☐ | ☐ | ☐ | ☐ | |
| La validation inclut une validation métier (utilisateur/key user) | ☐ | ☐ | ☐ | ☐ | |
| Les écarts identifiés donnent lieu à des actions correctives (avec suivi) | ☐ | ☐ | ☐ | ☐ | |
| La reprise est testée en conditions dégradées (accès limités, AD indispo, etc.) | ☐ | ☐ | ☐ | ☐ | |
| Un scénario “incident cyber” est prévu (restaurer sur environnement sain / isolé) | ☐ | ☐ | ☐ | ☐ | |
| Les preuves sont conservées et exportables (audit interne, direction, conformité) | ☐ | ☐ | ☐ | ☐ | |
| Un test de retour en production (failback) est défini (même partiel) | ☐ | ☐ | ☐ | ☐ | |
| Les dépendances et prérequis sont révisés après test (DNS, certificats, accès, flux) | ☐ | ☐ | ☐ | ☐ | |
| Les tests sont adaptés aux changements (MCO/projets : infra, applis, sites) | ☐ | ☐ | ☐ | ☐ | |

Un test daté + un RTO mesuré valent plus qu’un PRA “parfait” non testé.

Vytalx

# Synthèse :
# Vos priorités de sécurisation

## Votre résultat

**Score total :** ____ / ____

**Niveau :** ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

| **Barème :** | **Calcul :** |
|---|---|
| ✅ Oui = 2 pts<br>⚠️ Partiel = 1 pt<br>❌ Non = 0 pt | **Score obtenu** = somme des points<br>**Score Max** = 2 × (nb de lignes évaluées) |

## Zones rouges

Notez ici les points en ❌ / ⚠️ sur vos services les plus critiques :

_____

_____

_____

_____

_____

## Points bloquants

- Aucun test PRA daté (≤ 6 mois)
- RTO/RPO non définis pour le top 5
- Runbook non exploitable (étapes / dépendances / accès)
- Accès d'urgence absent (break-glass)
- Failback non envisagé (retour en production)

## Plan d'action

Phase 1 : Cadrage

- Finaliser le périmètre (top services critiques) et les RTO/RPO cibles
- Nommer un propriétaire PRA + mettre à jour la version / date
- Identifier les dépendances (AD/DNS, réseau, accès, certificats)

Phase 2 : Runbook exécutable

- Rédiger / simplifier le runbook (ordre de reprise + check de succès)
- Mettre en place les accès d'urgence et tester l'accès (break-glass)
- Documenter prérequis réseau/applicatifs essentiels

Phase 3 : Test mesuré

- Réaliser 1 test PRA sur un service critique (scénario réaliste)
- Chronométrer (RTO réel) + mesurer RPO réel
- Produire un compte rendu + ouvrir les actions correctives

Phase 4 : Industrialisation

- Planifier les tests récurrents (calendrier)
- Mettre à jour le runbook après test + créer le kit de reprise
- Définir un principe de failback (même haut niveau)