Vytalx

Checklist de revue : Dispositif de sauvegarde

Vérifier la sauvegarde, la protection contre la suppression et les preuves de restauration.
(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 de restauration daté (quoi, quand, résultat)
2. Rapport de taches OK/KO sur les 7 derniers jours
3. Politique de rétention (durées + justification)
4. Protection contre la suppression / le chiffrement (ex. immutabilité ou mécanisme équivalent)
5. Procédure de reprise : qui fait quoi, dans quel ordre, avec quels accès

Objectif : Passer d'une sauvegarde "déclarée" à une restauration "prouvée".

Vytalx

Périmètre de revue

Avant de cocher la checklist, listez ce qui doit absolument repartir en cas d'incident. Cette étape évite de "cocher des cases" sur des systèmes non prioritaires.

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	Sauvegarde en place ?	Dernier test de restauration

Signaux de risque immédiat

- Critique + pas de test de restauration
- Critique + sauvegarde dans le même domaine / mêmes accès admin
- RPO/RTO "inconnus" sur les 5 services les plus critiques
- Sauvegardes OK mais restauration non maîtrisée (qui / comment / combien de temps)

Vytalx

Checklist : Fondations (couverture & pilotage)

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Les services critiques sont tous couverts par une sauvegarde (serveurs/VM, fichiers, M365 si concerné, sites distants)	☐	☐	☐	☐	
La sauvegarde inclut les composants “socle” (annuaire/auth, DNS, hyperviseur, configs clés)	☐	☐	☐	☐	
La stratégie de copies est définie (ex. 3 copies dont 1 hors site / hors prod)	☐	☐	☐	☐	
La rétention est définie et justifiée (opérationnelle + légale si besoin)	☐	☐	☐	☐	
Les fenêtres de sauvegarde respectent la production (pas d’impact notable).	☐	☐	☐	☐	
Les jobs sont supervisés (alertes en cas d’échec, dérive, absence de run).	☐	☐	☐	☐	
Un reporting simple existe (quotidien/hebdo : OK/KO, volumes, tendances)	☐	☐	☐	☐	
Les échecs de sauvegarde sont traités avec un délai cible (ex. 24—48h)	☐	☐	☐	☐	
Les accès admin sauvegarde sont maîtrisés (MFA, comptes dédiés, moindre privilège)	☐	☐	☐	☐	
Les identifiants sensibles sont protégés (coffre-fort, rotation si applicable)	☐	☐	☐	☐	
La capacité de stockage est pilotée (seuils, croissance, purge maîtrisée).	☐	☐	☐	☐	
La documentation de reprise existe (contacts, ordre de restauration, dépendances)	☐	☐	☐	☐	

Attention : Une sauvegarde “ ✅ ” ne prouve pas la restauration.

Vytalx

Checklist : Résilience ransomware

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Une copie est protégée contre la suppression/modification (ex. immutabilité ou mécanisme équivalent)	☐	☐	☐	☐	
Les comptes admin de sauvegarde sont séparés et protégés (MFA, comptes dédiés, moindre privilège)	☐	☐	☐	☐	
Les identifiants de sauvegarde ne dépendent pas du domaine compromis (ou plan B si l'AD tombe)	☐	☐	☐	☐	
Le dépôt de sauvegarde est isolé (réseau, ACL, accès strictement nécessaires)	☐	☐	☐	☐	
Les postes utilisateurs n'ont pas d'accès direct au stockage de sauvegarde	☐	☐	☐	☐	
Les sauvegardes critiques existent hors site / hors prod (site secondaire, cloud, autre)	☐	☐	☐	☐	
Une alerte existe sur comportements anormaux (pics de changements, échecs massifs, croissance brutale)	☐	☐	☐	☐	
La console de sauvegarde est durcie (accès restreint, journalisation, mises à jour)	☐	☐	☐	☐	
Un scénario "environnement compromis" est prévu (restaurer sans réinfecter)	☐	☐	☐	☐	
Les sauvegardes incluent les configurations de sécurité clés (pare-feu, hyperviseur, configs applicatives critiques)	☐	☐	☐	☐	
Vous avez une procédure "break-glass" (accès d'urgence documenté, testé, limité).	☐	☐	☐	☐	
Les droits sur les dépôts sont revus périodiquement	☐	☐	☐	☐	

Erreur fréquente : Une sauvegarde stockée sur un partage accessible depuis le domaine peut être chiffrée ou supprimée en même temps que la production.

Vytalx

Checklist : Restaurabilité & preuves

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Un test de restauration a été réalisé récemment (≤ 3 mois sur les services critiques)	☐	☐	☐	☐	
Les tests couvrent plusieurs niveaux (fichier / VM / service applicatif)	☐	☐	☐	☐	
Les délais réels de restauration sont mesurés (et comparés au RTO cible)	☐	☐	☐	☐	
La perte de données réelle est évaluée (et comparée au RPO cible)	☐	☐	☐	☐	
La restauration est faisable sans accès “normaux” (ex. AD indisponible / accès dégradé)	☐	☐	☐	☐	
La restauration est granulaire quand nécessaire (fichier/objet/mailbox selon besoin)	☐	☐	☐	☐	
Les restaurations sont validées “métier” (pas seulement “la VM démarre”)	☐	☐	☐	☐	
Un ordre de reprise est défini (dépendances : AD/DNS → apps → données)	☐	☐	☐	☐	
Les rôles et responsabilités sont clairs (qui déclenche, qui exécute, qui valide)	☐	☐	☐	☐	
Sites distants : la reprise est possible sans équipe IT sur place (si concerné)	☐	☐	☐	☐	
Les preuves sont exportables et conservées (rapports, logs, tickets de test).	☐	☐	☐	☐	
Un “kit de reprise” existe (accès d’urgence, liens, docs, chemins, contacts)	☐	☐	☐	☐	
Vous savez quoi restaurer en priorité (top 5 systèmes + données)	☐	☐	☐	☐	
Un test “incident cyber” a été envisagé (restaurer sur environnement propre / isolé).	☐	☐	☐	☐	

✅ ≠ **restauration prouvée** : Un seul test daté vaut mieux que dix suppositions.

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 ⚠️ Partiel = 1 pt ❌ Non = 0 pt	**Score obtenu** = somme des points **Score Max** = 2 × (nb de lignes évaluées)

Zones rouges

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

Plan d'action

Phase 1 : Visibilité & hygiène

- Corriger les ❌/⚠️ récurrents et mettre une alerte sur l'échec ou absence d'exécution
- Valider la couverture des 5 services critiques (page 3)
- Clarifier RPO/RTO (même approximatifs) pour le top 5

Phase 2 : Résilience ransomware

- Protéger une copie contre la suppression (immutabilité / équivalent)
- Sécuriser les comptes admin (MFA, séparation, accès restreint)
- Vérifier l'isolement des dépôts (droits / réseau)

Phase 3 : Restaurabilité prouvée

- Réaliser 2 tests de restauration (1 fichier + 1 VM/service)
- Mesurer les délais réels (RTO) et la perte réelle (RPO)
- Documenter le résultat (preuve simple : compte rendu + captures)

Phase 4 : Industrialisation

- Écrire / mettre à jour le runbook (ordre de reprise + contacts + RACI)
- Créer un kit de reprise (accès d'urgence, docs, chemins, procédures)
- Planifier les tests récurrents (mensuel/trimestriel)

Planifier une revue de 30 minutes

Passez en revue vos zones à risque et repartez avec une priorisation claire : couverture, résilience ransomware et tests de restauration adaptée à vos contraintes (multi-sites, équipes réduites, environnements sensibles).

contact/vytalx.fr contact@vytalx.fr