**ÉLÉMENTS POUR L’ÉLABORATION D’UN**

**PCA/PRA**

**DÉMARCHE D’ÉLABORATION D’UN PCA**



**DÉMARCHE SYNTHÉTIQUE D’UN PCA/PRA**

1. Nommer un RPCA, qui dispose d'une bonne connaissance des métiers de l'entreprise : responsable qualité, DAF, etc.
2. Effectuer un inventaire des ressources matérielles et humaines, des applications utilisées
3. Réaliser un audit de criticité, de l'exposition au risque assortie d'une étude d'impact
4. Etablir une hiérarchisation, délimiter un périmètre en intégrant les pertes financières et aussi le coût des solutions pour répondre aux différents scénarios d'exposition aux risques
5. Fixer un RTO : Recovery Time Objectif (temps de coupure)
6. Fixer un RPO : Recovery Point Objectif (temps en termes de pertes de données), point de reprise des données (fraîcheur des données)
7. Construction du plan : ordonnancement du redémarrage des services
8. Tester le plan, éprouver les solutions de secours – consigner les résultats - 1 fois par an
9. Revoir le PCA – mettre à jour le document en fonction des évolutions du périmètres : 1 fois par an

**LES PROCÉDURES DE SECOURS**

**RTO / RPO : LES INDICATEURS DE SECURITE EN CAS DE SINISTRE**

En cas de situation critique, les systèmes d'information sont protégés en amont par des indicateurs d'objectifs de pertes.

**RTO : Recovery Time Objective ou Temps de Rétablissement**

Le RTO peut se traduire par la durée maximale d'interruption admissible.

Le RTO définit au sein du groupe BVA est de **4 Heures**.

**RPO: Recovery Point Objective ou Point de Rétablissement.**

Le RPO peut se traduire par la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne.

Le RPO définit au sein du groupe BVA est de 24 heures ou de **4 heures pour des demandes spécifiques de haute disponibilité**.



Des procédures écrites définissent les déclenchements de basculement, de remise en condition opérationnelle, l’organisation et les matrices de responsabilité

* Informatiques (description des solutions de secours, …)
* Retour à la normale
* Conditions de tests (test de restauration, test de basculement,)
* Conditions de maintien en conditions opérationnelles

**LES OUTILS AWS**

* CloudEndure Disaster Recovery : [LIEN](https://aws.amazon.com/fr/disaster-recovery/)

**MODÈLE DE DOCUMENT PCA & PRA**

Fournit par AWS si on utilise CloudEndure Disaster Recovery.

À faire si on utilise les outils d’AWS sans utiliser CloudEndure Disaster Recovery.

**DIFFÉRENCE ENTRE PCA & PRA**

* Le Plan de Continuité d'Activité permet, en cas de crise, de continuer l'activité sans perte de service, ou avec une légère dégradation acceptable.
Exemple : télétravail en cas de grèves, d'épidémies, ...
* Le Plan de Reprise d'Activité permet, en cas de crise majeure ou sinistre, de pouvoir reconstruire ou de basculer sur un système de relève - sur une durée déterminée - qui fournira les services nécessaires à la survie de l'entreprise. Il est souvent lié à un risque défini de perte de données (RPO) et durée d'interruption acceptable (RTO).
Exemple : basculement d'un datacenter sur un site de secours en cas d'incendie.