Enezis

ITIL
Gestion de la continuité des services informatiques

Sommaire

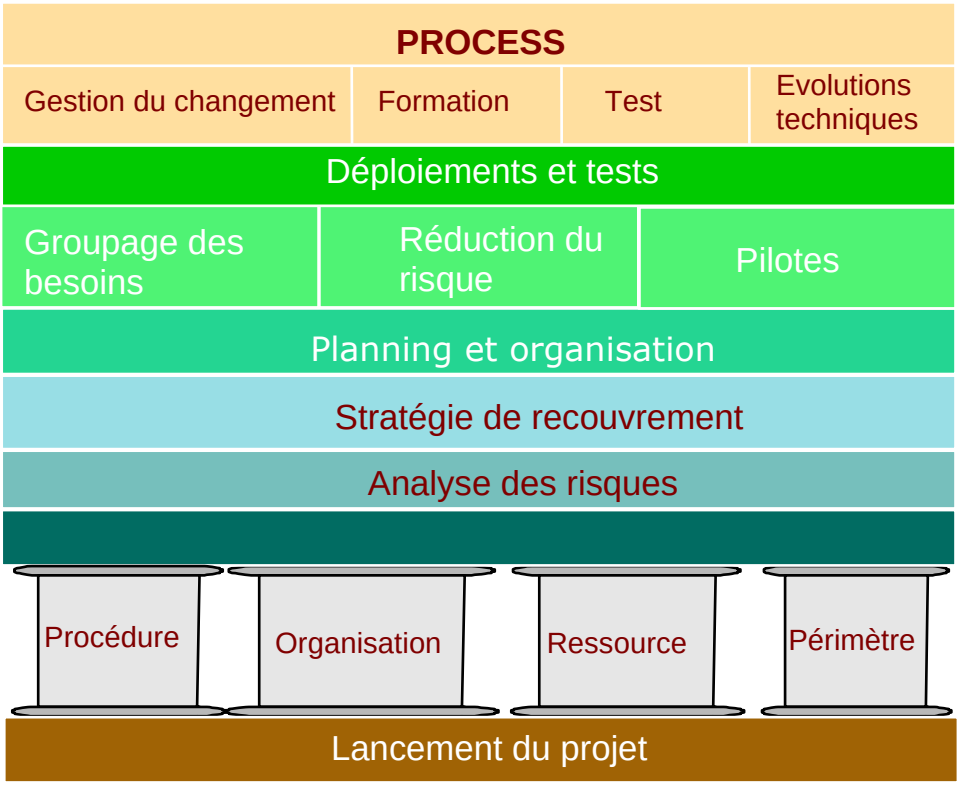
1 Généralités

Nous utilisons les meilleures pratiques du module ‘Gestion de la continuité des services informtiques’ d’ITIL (Information Technology Infrastructure Library) pour définir le cadre dans lequel s’inscrivent nos prestations de définition de Plan de Continuité de Services.

Objectifs de la gestion de la continuité des services informatiques définis par ITIL :

- Réduction des risques identifiés
- Réduction de la vulnérabilité de l'organisation
- Planification de la reprise des processus Business
- Implication éventuelle de tiers pour assurer la réduction maximale des risques
- Réduction de la menace de catastrophes potentielles

Les activités du Plan de Continuité de Services (PCS) sont globalement décrites dans le schéma ci-dessous (en partant du bas) :



2 Présentation de la prestation

La prestation initiale ne couvre que les aspects **non opérationnels de l'établissement du PCS** et doit servir de base au développement de ces procédures.

1. Analyse d'impact
2. Analyse de risque
3. Stratégie globale
4. Groupage des besoins et propositions techniques

1. Analyse d'impact

Pour chaque service au sein des directions fonctionnelles, il sera nécessaire d'agréger les éléments suivants :

- Définition de l'effet de l'indisponibilité en fonction des périodes
- Détermination du temps disponible avant de ressentir les effets en fonction des périodes
- Évaluation des exigences de reprise minimales
- Evaluation du RTO (Recovery Time Objective – temps de rétablissement du service) et du RPO (Recovery Point Objective – perte de données acceptable)

2. Analyse de risque

Domaines habituellement couverts :

- Dommages et refus d'accès
- Perte de services de support critiques
- Défaillance de fournisseurs critiques
- Erreur humaine
- Erreur technique
- Fraude, sabotage, extorsion, espionnage
- Virus ou autres violations de la sécurité
- Conflit social
- Catastrophes naturelles

Les risques peuvent généralement être classifiés dans les quatre catégories suivantes :

	Désastres	Incidents matériels localisés	Indisponibilité applicative	Autres incidents
Périmètre	Interruption illimitée de l'activité de l'entreprise	Interruption temporaire de l'activité de l'entreprise	Système, bases de données, bogues, erreurs humaines	Évènement externe imprévisible
Cible à traiter	Indisponibilité illimitée d'un composant critique	Indisponibilité temporaire d'un composant critique	Dysfonctionnement d'une application	Dépendances externes de l'activité de l'entreprise
Exemples d'évènements	Feu, inondation, panne d'un serveur consolidé	Panne du backbone réseau	Corruption de bases de données, dégradations importantes des performances	Interruption des flux d'informations financières dans une salle de marchés
Exemple de parades	Transfert de l'activité sur un autre site (PRA)	Basculement sur un réseau de secours	Procédure manuelle	Disponibilité d'une seconde source d'information

3. Stratégie globale

- Quels services en bénéficieront ?
- Quelles sont les options de reprise et de prévention disponibles ?
- Quels sont les coûts pour chacune d'entre elles ?
- Quels sont les services et applications à redémarrer en priorité ?

La stratégie globale sera déterminée par le DSI ainsi que par le management des directions métiers.

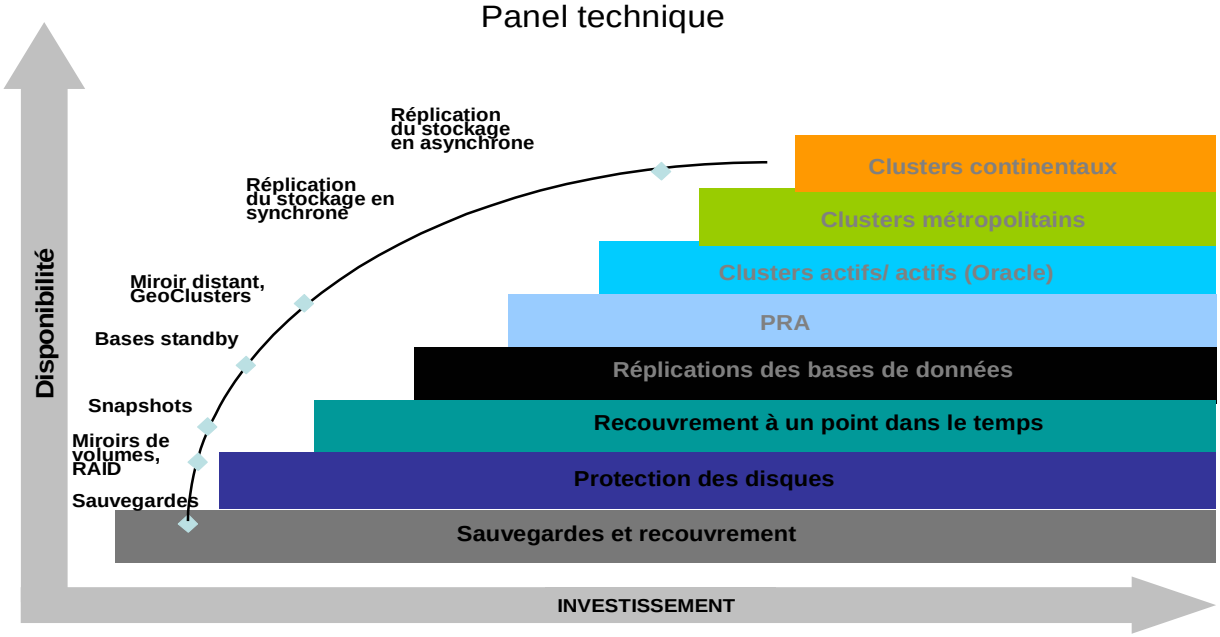
4. Groupage des besoins et propositions techniques

- Groupage des applications et des services par RTO/RPO/investissement dans la continuité de service voisins.

- Détermination des options organisationnelles : externalisation / internalisation

- Détermination des options techniques en fonction des besoins. Le panel des solutions couvre l'ensemble des dispositifs techniques de continuité de services :
  - Elimination des « spofs » (Single Point of Failure)
  - Réplication (inter et intra baies) du stockage
  - Réplication 'host based' (volume manager)
  - Solutions de bases de données (Oracle DataGuard et Flashback recovery, log shipping Ms SqlServer, etc.)

Panel technique



3 Modalités de la prestation

1. Pré requis :

- Toute documentation permettant d'analyser les vulnérabilités des processus métiers.

- Au minimum : schéma de principe des applications à inclure dans le périmètre de l'étude :

  - Flux logiciels
  - Composants hardware et logiciels

2. Entretiens avec les directeurs des services

- Chaque entretien sera synthétisé dans des fiches d'analyse d'impact et d'analyse de risque qui permettront de déterminer les besoins globaux.

3. Livrable

Le livrable comprendra :

- Fiches d'analyse des risques
- Fiches d'analyse d'impact

- Stratégie globale
- Options organisationnelles (externalisation)
- Options techniques