2 juillet 2013

Centre de Calcul de l'IN2P3

Projet PCA

Pierre Larrieu

Qu'est-ce qu'un PCA ?

- PCA = Plan de Continuité d'Activité
- Face à une situation de crise, que faire ?
  1. Improviser

  2. S'appuyer sur un PCA => pallier aux conséquences d'interruption d'activité
- Couvre :
  - Défaillance infrastructure, du réseau
  - Santé, sécurité du personnel et utilisateurs (pandémies)
  - Perte de compétences, de savoir faire (grèves)
  - Destruction du site, accidents industriels (ex: AZF)
  - Catastrophes naturelles : crues, séismes, etc…
  - Terrorisme, conflits internationaux, sabotage

Organisation du PCA

- **PGC (Plan de Gestion de Crise)**

  Coordination et communication (interne/externe) entre les parties. Prise en compte de la protection des personnels. ACMO sera impliqué

- **PCO (Plan de Continuité Opérationnel)**

  Pour ceux qui assurent la mis en œuvre de la continuité/reprise en fonction des objectifs opérationnels

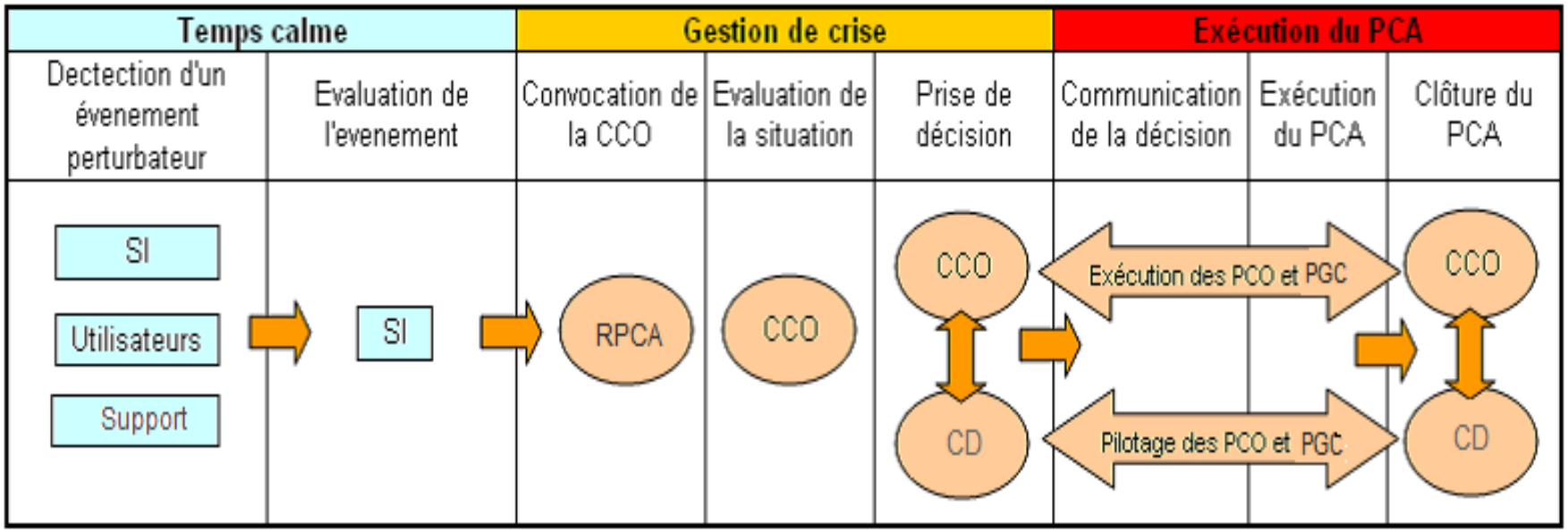
Il incombe à la direction du CC de définir :

- Les orientations de gestion des risques, d'en définir l'acceptabilité
- les délégations nécessaires : responsable PCA, coordinateur de cellule de crise opérationnelle et leurs remplaçants…

Mise en oeuvre

Alerte majeure détectée - Situation de crise

- Remédier à une situation anormale
- Mise en œuvre du PCA ou pas…



Diagnostics

- Etape indispensable dans la rédaction du plan
- Un simple incident a la faculté d'impacter un ensemble de services
- Questionnement
  - Evènements déjà survenus
    - Y-a-t-il eu des crises ?
    - Matérialisation
  - Sécurité des données
    - Gestion des accès, qui dispose des autorisations ?
  - Infrastructure informatique
    - Gestion des sauvegardes/restauration
    - Existence de contrats maintenance pour chaque composant ?
  - Aspect métier
    - Obligations contractuelles : Ranater, lyonix…
    - Habitudes de travail, obligations règlementaires : ZZR

Evaluation des risques

Objectifs :

- déterminer les scénarios de sinistre les plus probables
- mettre en place des actions pour rendre le risque résiduel acceptable.

Visualiser la probabilité d'occurrence et l'impact:

- cartographie des risques

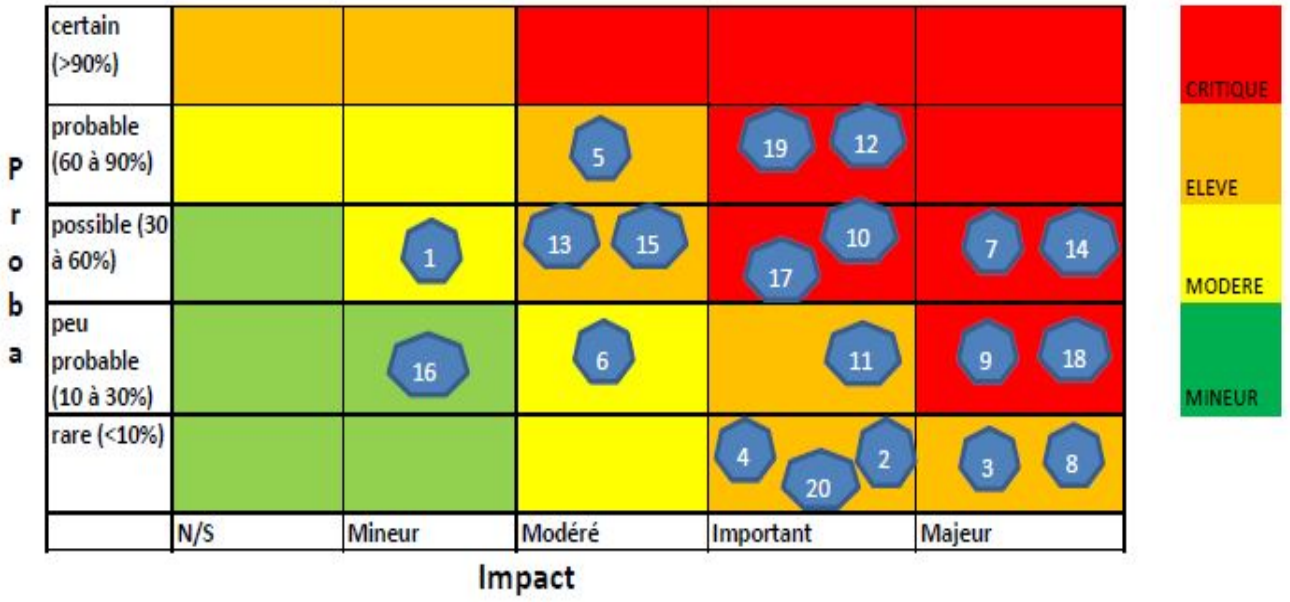
puis

- Analyse des conséquences

Id	Type de sinistre
	Evènement naturel
1	Situation climatique extrême (froid, canicule, etc)
2	Tremblement de terre
3	Inondation
4	Foudre
5	Neige
	Sinistre
6	Dégât des eaux
7	Incendie
8	Explosion
	Perte de ressource d'infrastructure
9	Problème d'alimentation électrique
10	Problème des lignes réseau
11	Problème de climatisation
	Problème technique sur SI
12	Pannes matérielles critiques (routeur, robot)
13	Pannes logicielles majeures (HPSS, GPFS, etc…)
14	Corruption de données (DB)
	Origine humaine non malveillante
15	Fausse manip critiques
16	Grève
17	Pandémie
	Intrusions/malveillance
18	Vol d'équipements critiques
19	Attaque informatique (service deny, intrusion)
20	Sabotage de matériel ou de l'infrastructure

Cartographique des risques

Id	Type de sinistre
	Evènement naturel
1	Situation climatique extrême (froid, canicule, etc)
2	Tremblement de terre
3	Inondation
4	Foudre
5	Neige
	Sinistre
6	Dégât des eaux
7	Incendie
8	Explosion
	Perte de ressource d'infrastructure
9	Problème d'alimentation électrique
10	Problème des lignes réseau
11	Problème de climatisation
	Problème technique sur SI
12	Pannes matérielles critiques (routeur, robot)
13	Pannes logicielles majeures (HPSS, GPFS, etc…)
14	Corruption de données (DB)
	Origine humaine non malveillante
15	Fausse manip critiques
16	Grève
17	Pandémie
	Intrusions/malveillance
18	Vol d'équipements critiques
19	Attaque informatique (service deny, intrusion)
20	Sabotage de matériel ou de l'infrastructure



Menaces et conséquences

MENACE	SOUS CRITERE	CONSEQUENCES
Evènement naturel		
Conditions climatiques extrêmes	Canicule	Atteinte des limites de performances des équipements de production de froid. Limiter la puissance appelée sur les serveurs – VILL1 et/ou VILL2
	Froid extrême	Gel et éclatement des circuits d'eau, de refroidissement extérieurs – VILL1 et VILL2
Tremblement terre		
Inondation	<10cm VILL1	Les faux planchers onduleur et pieds au TGBT permet de continuer d'exploiter. Pompage possible. Arrêt de VILL1
	>10cm VILL1	VILL1 est innondé. VILL2 peut continuer mais quid des services critiques
	<10cm VILL2 >10cm VILL2	VILL1 et VILL2 est innondée – Arrêt des 2 bâtiments
Foudre	En standard	Les parafoudres et mise à la terre font leur travail
	Situation rare	Capacité des protections mise à mal - Surtensions sur nombre d'équipements d'infrastructure et de serveurs – Matériels endommagés – Reprise peut s'avérer impossible
Neige	<20cm	Difficultés d'accès – Accès possible – Personnel réduit
	>20cm	Accès impossible autrement qu'à pied – Absence importante de personnel. Accès des fournisseurs/maintenance compromis

Menaces et conséquences (2)

Sinistre		
Dégât des eaux	VILL1 VILL 2	La probabilité d'atteindre un niveau d'eau de 10cm dans VILL1 est quasi-nulle : le site est occupé en journée. Les rondes de nuit noteront toute défaillance. VILL 2 encore moins
Incendie	VILL1 VILL2	Les équipements réseau sont détruits. Problématique du réinvestissement d'équipement critiques
Explosion	VILL1	Détection H2 du local batterie défaillante. Accumulation suffisante d'H2 dans un délai court peu probable (ventilation). Dans le cas contraire, dégâts majeurs.

Menaces et conséquences (3)

Perte de ressource d'infrastructure		
Pb alimentation électrique	Ligne 6 MW	On bascule sur le secours garanti à 2MW. Situation confortable tant que les puissances restent au niveau 2013 i.e. 1,5MW environ
	Secours garanti	Ne fonctionne pas après basculement : mais que fait ErDF !
	GE	On bascule sur le GE, qui ne distribuera que les services critiques. Sinon le CC est dans le noir complet
Pb lignes réseau		Entrées de fibres en 2 points du bâtiment permettent de fonctionner en mode dégradé.
Pb climatisation	VILL1	Le système de climatisation de VILL1 est indépendant de celui de VILL2. Une redondance des GF existe. Il faudra néanmoins envisager d'arrêter certains services : stockage GPFS, Dcache, HPSS
	VILL2	Même indépendance vis-à-vis de VILL1. La montée en température peut être assez rapide. Arrêt des serveurs nécessaire dans l'heure suivante selon les conditions climatiques

Menaces et conséquences (4)

Problème technique SI		
Pannes matérielles critiques	Routeur Robot	Echange standard en H+2 des sous-ensembles défectueux. Si le fond de panier est défaillant, le GTR peut dépasser la journée. Accès aux services du CC impossible. Intervention H+2 si gravité 1 Oracle. Dégradation des services possible si panne sur contrôle robot 1. Vérifier
Pannes logicielles majeures		Probabilité ~ 0
Corruption de données (DB)		Corruption données sur baie Pillar. Remontées sauvegarde sous un délai à préciser.

Menaces et conséquences (5)

Origine humaine non malveillante		
Fausse manip critiques	VILL1 VILL2	Etude de cas à effectuer
Grève	<50% personnel >50% personnel	Situation similaire à une période de congés d'été – Durée excédant quelques semaines peu probable Situation possible dans des conditions économiques exceptionnelles (Grèce)
Pandémie	<60% personnel >60% personnel	Situation similaire à une période de congés d'été à la différence qu'une intervention ponctuelle des personnels absents bien que joignables est inenvisageable. Compétences très réduites. Pas de ressource humaine supplémentaire disponible. Tout incident additionnel extrêmement difficile à gérer
Intrusions/malveillance		
Vol d'équipements critiques		Peu probable de voir disparaitre ccpn-inter, ccpn-cora ou le robot.
Attaque informatique: deni de service, intrusion		Ralentissement/Blocage des services courants. Atteinte à l'image du CC. Collecte des traces. Durée d'interruption des services difficile à estimer
Sabotage de matériel ou de l'infrastructure	VILL1 VILL2	Les routeurs et le robot sont critiques L'ensemble des fibres entrant dans le CC via VILL1 sont critiques. Néanmoins, la probabilité est faible mais non nulle pour que les 2 entrées fibres : nord et sud-est soient impactées. Baie Pillar : perte d'accès grande partie DB. Services majeurs indisponibles. L'impact est économique, non pas technique

Exemple : trame PCA pandémie

- Point de départ : liste des missions du CC
- Hiérarchisation des missions pouvant être assurées en toutes circonstances
- Identification ressources matérielles/humaines nécessaires à la continuité d'activité
- Etablissement d'un état des effectifs (au regard des missions prioritaires, possibilité de télétravail, poste en situation dégradé, suppléances et renforcements possibles)
- Méthodes et moyens de protection des personnels (qui est le + exposé ?)
- Organisation pour le maintien de l'activité (fournisseurs alternatifs, stocks en sus, transports alternatifs, réorganisation de la méthode de travail : télétravail, horaires, mesures visant à limiter la contagion, etc…)
- Acquisition préalable (produits d'hygiène) et validation du matériel nécessaire au télétravailleur
- Tests de réalisation
  - Retour d'expérience et ajustement du dispositif
  - Retour à la normale

Un PCA au CC ?

- Une trame est existe
- Mise en place d'un groupe de validation
- Rédaction détaillée
- Tests fin 2013

Le rédactionnel reste à peaufiner…

Et maintenant
Il faut gratter !