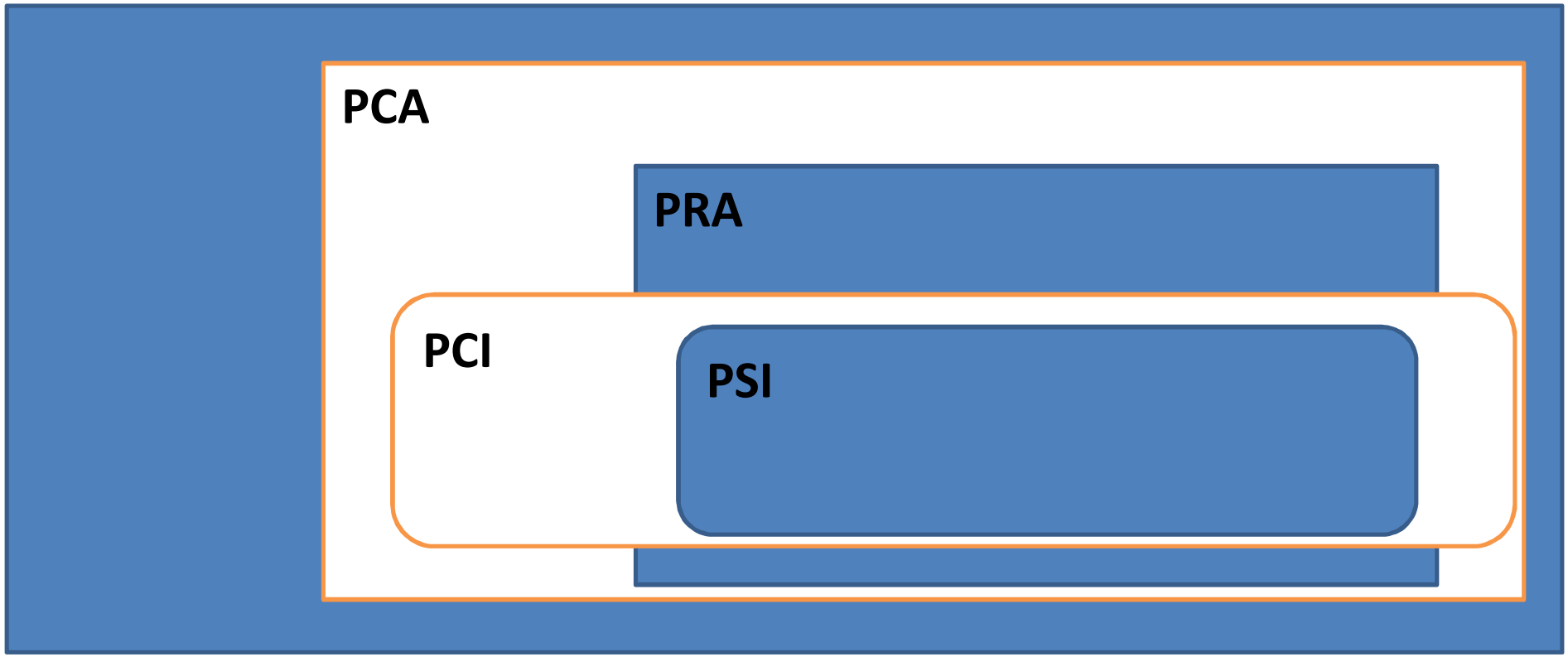
Définitions

- **PCA** : Plan de Continuité d'Activité / BCP : Business Continuity Plan
  PCI : Plan de Continuité Informatique
  PCO: Plan de Continuité Opérationnelle
  (Continuité ou reprise des opérations métiers)
  PCA=PCO+PCI
  PCS : Plan de Continuité de Services
- **PRA** : Plan de Reprise d'Activité (Plan de Récupération Après Sinistre)
  DRP : Disaster Recovery Plan
  PRI : Plan de Reprise Informatique
  PSI : Plan de Secours Informatique
- PRU : Plan de Reprise des Utilisateurs
  PSA : Plan de Sauvegarde de l'Activité
  PRN : Plan de Retour à la Normale
  BIA : Bilan d'Impact sur les Activités

PCA, PRA, PCI, PSI : où ça ?

Le PCA s'insère dans le cadre de la politique générale de Sécurité.



Différence entre PCA et 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.

Quelques chiffres

Même s'il convient de rester prudent sur des données fournies par des entreprises dont le PRA s'insère dans leurs prestations…

- Selon Adista, la moitié des entreprises victimes d'un sinistre majeur de leur système d'information disparaissent dans les trois ans qui suivent l'incident.
- Or, 58% des PME ne disposent pas de PRA, selon une étude Freeform Dynamics réalisée pour le compte de Quest Software auprès de 160 responsables informatiques en France, en Allemagne et au Royaume-Uni. Source : Indexel.

L'émergence du PCA / PRA

Le PRA s'est imposé du fait de la dépendance accrue des organisations vis-à-vis du système d'information automatisé. Un coup de pelle et...
L'exposition à des risques systémiques s'est accrue avec :

- la disparition des architectures distribuées-réparties,
- le degré d'intégration des solutions retenues,
- l'accroissement de la complexité (la virtualisation et le cloud n'arrangent rien à l'affaire),
- la prégnance de l'utilisation d'Internet,
- le développement du phénomène Bring Your Own Device (BYOD).

Obligations réglementaires

- Loi du 31 juillet 2002 (Pub. L. No. 107-204, 116 Stat. 745) dite Sarbanes-Oxley Act (SOX)
- Réglementation CRBF2004-02 (issue de IASB-Bâle II) : obligation d'un plan de secours opérationnel pour les établissements financiers, banques et assurances.
- Grippe H1N1 : circulaire DGT (Direction Générale du Travail)2007/18 du 18 décembre 2007 / circulaire DGT 2009/16 du 3 juillet 2009, recommandant l'institution d'un PCA.
- Le code du commerce prévoit une conservation des documents comptables durant 10 ans.
- Conservation des logs des prestataires d'hébergement (Décret du 24 mars 2006)

Démarche

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 (exemple : groupes électrogènes)

Menaces

Elles peuvent toucher aussi bien l'humain que le matériel.

- Risques naturels : crues, séismes, marnières,
- Pandémies, intoxications,
- Grève(s),
- Actes de sabotage,
- Accidents industriels (AZF Toulouse), accidents nucléaires (Fukushima-Daiichi),
- Servitudes : rupture de canalisation d'eau, coup de pelles, panne de courant, défaillance de la climatisation.
- Défaillance matérielle au niveau des serveurs, des stations de travail, du réseau, de l'internet et de la téléphonie,
- Virus informatiques, rootkits,

MEHARI
Méthode Harmonisée d'Analyse du Risque

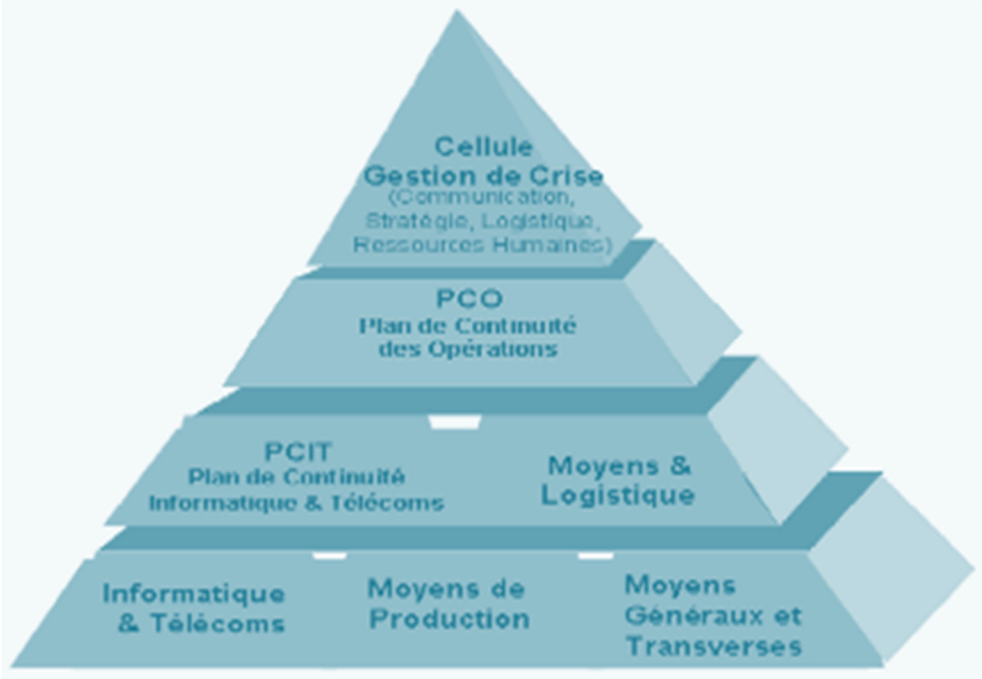
- Mesure de l'exposition au risque : potentialité
- Mesures de réduction de la potentialité
- Mesure de l'impact (Disponibilité, Intégrité, Confidentialité)
- Mesures de réduction de l'impact
- Grilles Potentialité / Impact / Gravité

PRA : la gestion de crise

La cellule de crise a pour objectif de :

- gérer la communication (institutions, presse, clients, fournisseurs, ...), organiser le PRA,
- assurer les moyens logistiques et la mise à disposition de ressources humaines.

A cet effet, il convient de prévoir un hébergement disposant de tous les moyens de communication usuels.



Domaines du SI

Hors servitudes (électricité, climatisation), le SI peut être segmenté en plusieurs domaines :

- réseau / LAN,
- accès Internet / WAN,
- messagerie
- serveurs d'infrastructure : DHCP, DNS, Wins, authentification, supervision
- applications / serveurs d'applications
- base de données
- téléphonie

Solutions

- Informatique répartie
- Spare
- Images à froid : Clonezilla, Acronis True Image, Symantec Ghost
- Redondance (Spanning Tree, …)
- Stockage : SAN
- P2V, V2P : Vmware Converter, System Recovery (Symantec)
- Virtualisation : Vmware, Hyper-V, KVM, Xen, etc
- Sauvegardes externalisées (oodrive) : volumétrie ?
- SaaS (Service as a Software) : Google Apps, Microsoft Office 365, … Patriot Act ?
- Télétravail
- Virtualisation du stockage : et les performances ???

Offre Google Drive

Old storage plans	New storage plans
Free storage: • 7+ GB in Gmail • 1 GB in Google Docs (uploaded files only) • 1 GB in Picasa • Unlimited in Google+	Free storage: • 10 GB in Gmail • 5 GB in Google Drive • 1 GB in Picasa • Unlimited in Google+
Purchased storage shared across: • Gmail • Google Docs • Picasa	Purchased storage shared across: • Google Drive (synced/uploaded files only) • Picasa • Automatically get additional but separate Gmail storage.
Automatically renew *yearly* Non-refundable Storage can't be transferred to a different account	Automatically renew *monthly* Non-refundable Storage can't be transferred to a different account
▾ Pricing structure (prices are yearly) • 20 GB - $5 • 80 GB - $20 • 200 GB - $50 • 400 GB - $100 • 1 TB - $256 • 2 TB - $512 • 4 TB - $1024 • 8 TB - $2048 • 16 TB - $4096	▾ Pricing structure (prices are monthly) • 25 GB - $2.49 • 100 GB - $4.99 • 200 GB - $9.99 • 400 GB - $19.99 • 1 TB - $49.99 • 2 TB - $99.99 • 4 TB - $199.99 • 8 TB - $399.99 • 16 TB - $799.99

Logiciels de sauvegarde

- EMC Networker
- Symantec Backup Exec
- Atempo Time Navigator
- Arkeia Network Backup

Services d'hébergement de machines virtuelles

Offre	Prestataire	Prix par machine virtuelle
Synaptic Compute as a Service	AT&T	Tarification sur mesure
Colt Dynamic Infrastructure Services	Colt	Tarification sur mesure
EC2	Amazon	220 $ par mois ou 10 centimes par heure
BT Virtual Data Center	BT Global Services	200 € par mois
ClaraCloud	Claranet	220 € par mois
Flexible Computing	Orange	A partir de 90 € par mois
Dedibox	Proxad	A partir de 15 € par mois
Gandi Hébergement	Gandi.net	A partir de 15 € par mois ou 3 centimes par heure
Kimsufi	OVH	A partir de 15 € par mois
AWS	Amazon	
Orange Business	Orange	
SFR Business	SFR	

Site de repli ?

- site chaud : redondance
- site tiède : infrastructure présente, mais mise à jour des données
- site froid ou dormant: site existant ne disposant d'aucune installation

Réplication

Fonction	Exemples de produits
Géocluster : cluster entre machines situées sur des sites distants	Double-Take (Vision Solutions), RepliStor (EMC), Veritas Cluster Server (Symantec), SteelEye DataKeeper (SIOS Technology), Cluster Server (Microsoft), ... Fonction également intégrée à certaines applications telles que les SGBD et serveurs de messagerie
Réplication synchrone de baie à baie, via un SAN Fiber Channel	Fonction intégrée à la plupart des baies de stockage : fonction SRDF chez EMC, protocole PPRT chez IBM et HDS chez Hitachi
Réplication asynchrone de système à système via un réseau IP	Double-Take (Vision Solutions), Veritas Replicator (Symantec), Netvault Replicator (Quest Software), Backup & Replication (Veeam Software) pour Vmware
Sauvegarde de l'image du système et redémarrage sur un site distant	VSS Volume Shadow copy Service (Microsoft)
Réplication de données	NetApp SnapMirror, Rsync (Open Source)

Livres

- **Plan de continuité d'activité et système d'information**
  Vers l'entreprise résiliente,
  par *Matthieu Bennasar* (Dunod)
- **Management de la Continuité d'Activité**,
  par *Emmanuel Besluau* (Eyrolles)
- **Réaliser le plan de continuité d'activité de son entreprise**
  P.C.A guide opérationnel,
  par *Olympe Cavallari et Olivier Hassid* (Maxima)
- **Plan de continuité d'activité**
  Secours du système d'information,
  par *Patrick Boulet* (Hermes Science Publications)

Sources

- **http://blogs.orange-business.com/cloud-computing/**
- http://droitdutravail.blog.capital.fr/index.php?action=article&id_article=422971
- **http://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9_d%27activit%C3%A9_%28informatique%29**
- **http://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9**
- http://infochronologie.blogemploi.com/pra/2008/09/le-projet-pra-p.html
- **http://itil.fr/DRP/PCA/drppca-mettre-en-oeuvre-un-plan-de-continuite-dactivite.html**
- **http://www.clusif.asso.fr/fr/production/mehari/download.asp**
- http://www.journaldunet.com/solutions/0506/050628_pca.shtml
- **http://www.journaldunet.com/solutions/securite/pca-et-pra/**
- http://www.journaldunet.com/solutions/systemes-reseaux/dossier/realiser-un-plan-de-reprise-d-activite-10-conseils-d-experts/realiser-un-plan-de-reprise-d-activite-10-conseils-d-experts.shtml
- http://www.mag-securs.com/Communiqu%C3%A9s/tabid/65/id/28117/La-virtualisation-et-le-cloud-computing-compliquent-la-reprise-d-activites-apres-incident.aspx
- http://www.stanfeel.com/Front/plan-de-continuite-d-activite_18.php
- http://www.systemes-information.fr/
- http://www.vmware.com/fr/solutions/datacenter/business-continuity/
- **www.hsc.fr/presse/clubpca/LIVRE-BLANC-CCA.pdf**

Annexe : trame d'un PCA (grippe H1N1)

- Analyse des missions assurées par l'entreprise
- Hiérarchisation des missions devant être assurées en toutes circonstances
- Identification des ressources matérielles et humaines nécessaires à la continuité de l'activité jugée indispensable
- Etablissement d'un état des effectifs (compétence au regard des missions et fonctions prioritaires, possibilité de télétravail, poste occupé en situation dégradée, possibilités de suppléance, possibilités de renforcement….)
- Méthodes et moyens de protection et d'information des personnels (mise à jour du document unique, identification des personnels les plus exposés, information…)
- Modes d'organisation pour le maintien de l'activité (fournisseurs alternatifs, renforcement des stocks, solutions alternatives de transport, liste des moyens techniques et logistiques à prévoir, mesures visant à limiter la contagion, réorganisation du travail – audioconférence, télétravail-, aménagement des horaires, outils d'information collective, plan de communication, utilisation du courrier électronique…)
- Acquisitions préalables (produits d'hygiène, équipements pour le travail à domicile…)
- Exercices de réalisation
- Suivi, retour d'expérience et ajustement du dispositif
- Reprise des opérations à l'issue de phase aigüe de la crise