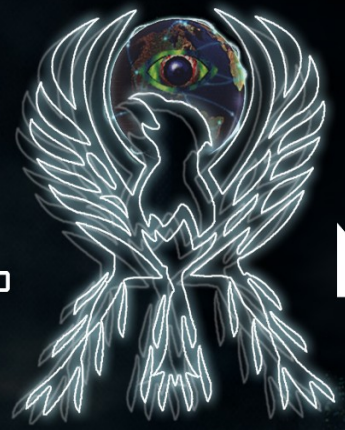

DIGITAL NETWORK

PCA et PRA

Christophe Casalegno

Groupe Digital Network

PCA et PRA

PRA et PCA : définition

Les plans de continuité d'activité (PCA) et les plans de reprise d'activité (PRA) sont des concepts composés de documents et de procédures, destinés à permettre le fonctionnement d'une entité en cas d'incident ou de désastre.

Le PRA vise à permettre la reprise de l'activité, à plein régime ou en mode dégradé, au bout d'un certain temps, lui même défini dans les procédures qui le composent.

Le PCA vise à assurer la continuité de l'activité, à plein régime ou en mode dégradé. Au contraire du PRA, le PCA n'autorise pas de coupure intégrale du service : la continuité, au moins partielle doit être assurée.

PCA et PRA

Attention, bien que différents, on considère généralement que le PRA est une partie intégrante du PCA, le plan de continuité prenant en compte toutes les mesures permettant d'assurer la continuité des services métiers.

Généralement, dans le domaine de l'entreprise, la mise en place de telles procédures commence par l'établissement d'un PRA dans lequel sera ensuite considéré la haute disponibilité afin de réduire l'exposition aux risques.

- Cependant, on trouve au sein de nombreuses entités des mesures techniques permettant d'assurer une haute disponibilité et/ou une reprise d'activité informatique sans pour tant que ces plan existent (mais où parfois rien n'existe concernant les processus métier)

PCA et PRA

- Bien qu'un PCA ou qu'un PRA puissent exister à différents niveaux, c'est du point de vue du système d'information qu'ils seront principalement traités ici. Ce type de plan partie intégrante du PCA/PRA est également couramment appelé PSI (Plan de Secours Informatique) ou PCI (Plan de Continuité Informatique).

- Les plans de reprise et de continuité d'activité peuvent aussi bien s'appliquer à de mini systèmes d'information (par exemple un serveur) qu'à des systèmes composés de milliers d'équipements et multi-sites.

- Bien que ces notions soient conceptuellement très anciennes, on a vu leur mise en place se généraliser dans les systèmes d'informations après les attentats du 11 septembre 2001.

PCA et PRA

Le PRA et le PCA sont composés de 3 grandes parties :

- - Le PCO (Plan de continuité opérationnelle)
- - Le PGC (Plan de Gestion de Crise)
- - Le PCI/PSI (Plan de Continuité Informatique)
- Ce triangle rassemble l'ensemble des mesures visant à assurer, face à différents scénarios de crise et de sinistres, le maintient des activités essentielles de l'entreprise de manière dégradée ou non dégradée

PCA / PRA

Attention il existe de nombreuses méthodes différentes pour les PRA, la vision précédente est une version simplifiée et commune à l'ensemble de ces méthodes.

Dans la pratique on dénombre plus de 7 plans (tirés de leurs équivalents anglophones) :

- PCA : Plan de Continuité d'Activité
- PRA : Plan de Reprise d'Activité
- PCO : Plan de Continuité des Opérations
- PCC : Plan de Communication de crise
- PRII : Plan de réponse aux Incidents Informatiques
- DRP : Disaster Recovery Plan
- PIU : Plan d'Intervention d'Urgence

PCA et PRA

LE PCO

Le plan de continuité opérationnelle

PCA et PRA

Le PCO ou Plan de Continuité opérationnelle est la première étape du PCA/PRA.

Il a pour objectif de définir les modes opératoires ainsi que les exigences métiers de la continuité de l'activité tout en tenant compte des objectifs opérationnels.

Concrètement le Plan de Continuité opérationnelle évalue les différents scénarios liés aux activités métiers critiques, puis définit et met en œuvre les moyens préventifs adaptés.

PCA et PRA

LE PGC

Le plan de gestion de crise

PCA et PRA

- Le PGC (Plan de Gestion de Crise) est à proprement parler le plan qui intègre les moyens ainsi que l'ensemble des procédures organisationnelles et techniques permettant de se préparer et de faire face à l'apparition d'une crise.

- Ce plan évolue à la survenance de chaque crise, s'améliorant à partir de l'expérience de chacune des crises précédentes permettant une meilleure vision prospective de la gestion de crise.

- Dans quelques cas exceptionnels, ce plan intègrera également une série d'actions à mener en cas de « crise parfaite », c'est à dire une crise où l'ensemble des pires facteurs sont combinées et déclenchant généralement la fin définitive de l'entité qui la subit.

PCA et PRA

LE PCI

Le plan de continuité informatique

PCA et PRA

Le PCI (Plan de Continuité Informatique) ou PSI (Plan de Secours Informatique) est nécessaire si :

- - Le bon fonctionnement de l'entité est lié ou dépendant du bon fonctionnement de son système d'information. Il convient pour cela de se poser l'ensemble des questions nécessaires comme : « L'arrêt de fonctionnement de ma messagerie durant 48H00 a t'il un impact sur le fonctionnement de l'entité? »

- - Dès que la réponse à l'une des questions posées sera « - non », cela signifiera que le PCI est obligatoire. Dans le cas contraire, c'est à dire si le fonctionnement de l'entité ne dépend pas de son système d'information (de plus en plus rare) un PCA/PRA sans PSI est suffisant.

PCA et PRA

- Le PSI (Plan de Secours Informatique) ou PCI (Plan de Continuité Informatique) a pour but de garantir la survie du système d'information. Il permettra la continuité (en mode dégradé ou non) ou le redémarrage de l'activité le plus rapidement possible et avec un minimum de pertes de données.

- Le PSI/PCI est non seulement souvent l'un des composants essentiel d'un PCA/PRA mais ce dernier figure également en général au sein de la politique de sécurité de l'entité.

- Il est principalement constitué d'une analyse des risques et de leurs impacts, d'une stratégie composées de mesures préventives et curatives mais également de procédures de « crash test » afin de s'assurer de la validité technique de la procédure.

PCA / PRA

Les différents plans et leurs équivalents anglophones.

PCA → BCP (Business Continuity Plan)
PRA → BRP (Business Recovery (Resumption) Plan)
PCO → COOP (Continuity of Operations Plan)
PCC → CCP (Crisis Communications Plan)
PRII → CIRP (Cyber Incident Response Plan)
DRP → DRP (Disaster Recovery Plan)
PIU → ERP (Emergency Response Plan)

PCA / PRA

On peut résumer les objectifs des différents plans et leur périmètre de la manière suivante.

LE PCA / BCP

Plan de Continuité d'Activité / Business Continuity Plan

PCA / PRA

PCA / BCP

- Plan de Continuité d'Activité
- Business Continuity Plan

Fournir les procédures nécessaires au maintient des activités essentielles suite à un incident, un désastre ou une perturbation.

Périmètre : Processus métier. Les processus IT ne sont traités que si et seulement si ils supportent les processus métier de l'entité.

PCA et PRA

LE PRA / BRP

Plan de Reprise d'Activité / Business Continuity Plan

PCA / PRA

- **PRA / BRP**
  Plan de Reprise d'Activité
- Business Continuity Plan

- Fournir les procédures nécessaires à la reprise des activités immédiatement après un incident ou un désastre.

- <u>Périmètre :</u> Processus métier. Les processus IT ne sont traités que si et seulement si ils supportent les processus métier de l'entité (d'où la possible confusion avec les PRII lorsque c'est le cas).

PCA et PRA

LE PCO / COOP

Plan de continuité des opérations / Continuity of Operations Plan

PCA / PRA

- **PCO / COOP**
  Plan de continuité des opérations
- Continuity of Operations Plan

- Fournir les procédures et les moyens nécessaires pour transférer et maintenir les fonctions stratégiques et essentielles d'une entité vers un autre site.

Périmètre : Sous-ensemble des missions de l'entité considérées comme critiques. Ce plan est totalement indépendant du domaine IT (Technologies de l'information) et dépend généralement directement de la direction

PCA et PRA

LE PCC / CCP

Plan de communication de crise / Crisis Communications Plan

PCA / PRA

- **PCC / CCP**
  Plan de communication de crise
- Crisis Communications Plan

- Fournir les procédures nécessaires à la diffusion des rapports de situations aussi bien en interne que vis à vis de tiers identifiés ainsi que du public. Le PCC/CCP peut en fonction de sa réussite ou de son échec diminuer ou augmenter gravement les impacts de la crise traversée.

- Périmètre : Le périmètre est ici humain. Il comprend le personnel (dans son ensemble et par services et/ou d'accréditation en fonction de la classification de l'information), d'autres entités (partenaires, fournisseurs, clients...) et le public.

PCA et PRA

LE PRII / CIRP

Plan de réponse aux incidents informatiques / Cyber Incident Response Plan

PCA / PRA

PRII / CIRP
Plan de réponse aux incidents informatiques
Cyber Incident Response Plan

Fournir les stratégies nécessaires à la détection, la réponse et la compartimentation des incidents qu'ils soient mal-veillants ou accidentels.

Périmètre : Le périmètre se limite généralement aux réponses aux incidents informatiques ayant un impact sur la sécurité de l'information sur les systèmes et réseaux.

PCA et PRA

LE DRP

Disaster Recovery Plan

PCA / PRA

DRP / DRP
Disaster Recovery Plan
Disaster Recovery Plan

Fournir les procédures détaillées nécessaires à la facilitation de la reprise des activités à partir d'un site de secours.

Périmètre : Le périmètre est souvent cantonné aux systèmes d'informations et de télécommunications. On le limite généralement aux désastres importants ayant des conséquences à long terme (exemple destruction du bâtiment).

PCA et PRA

LE PIU / ERP

Plan d'intervention d'urgence / Emergency Response Plan

PCA / PRA

PIU / ERP
Plan d'intervention d'urgence
Emergency Response Plan

Fournir les procédures qui permettront la réduction des pertes que ce soit en vie humaines ou en actifs mobiliers et/ou immobiliers en cas de menace physique

Périmètre : Le périmètre est ici focalisé sur le personnel et les biens quelque soit leur nature avec une priorité sur la limitation des pertes humaines.

PCA et PRA

LE RTO

Recovery Timage Objective

PCA / PRA

Durée maximale d'interruption admissible
RTO (Recovery Timage Objective)

- La durée maximale d'interruption admissible (en anglais RTO pour Recovery Time Objective) définit le temps maximum acceptable durant lequel une ressource technique (informatique par exemple) ou humaine peut être indisponible après un incident majeur.

- Le RTO en conjonction avec le RPO/PDMA (Recovery Point Objective / Perte de Données Maximale Admissible) permet de déterminer le temps total d'interruption d'une ressource après un incident majeur.

PCA / PRA

Durée maximale d'interruption admissible
RTO (Recovery Timage Objective)

Le délai d'interruption de service est décomposé du :

- Délai de détection de l'incident
- Délai de décision du passage en secours (manuel ou auto)
- Délai de mise en œuvre des procédures de secours
- Délai de contrôle et relance des services et applications

La somme de ces délais doit être inférieure au RTO

PCA et PRA

LE PDMA / RPO

Perte de données maximale adminissible / Recovery Point Objective

PCA / PRA

Perte de données maximale admissible
PDMA / RPO
- Recovery Point Objective

- Le RPO quantifie les données que le système d'information peut être amené à perdre suite à un incident.

- Généralement le RPO exprime une durée entre l'incident à l'origine de la perte de données et la date la plus récente des données qui pourront être utilisées en remplacement lors de leur restauration.

- Cette durée est généralement exprimée en heures ou en minutes.

PCA / PRA

Perte de données maximale admissible
PDMA / RPO
- Recovery Point Objective

Le RPO est souvent déterminé par le type et la fréquence des sauvegardes effectuées sur les ressources informatiques.

Les données perdues ne sont pas toujours restaurer à partir de backup. Elles peuvent également issu d'un processus de réplication ou encore reconstruites à partir de journaux de transaction et/ou de réparation (exemple : système de fichiers ou base de données)

PCA et PRA

PCA / PRA

Les grandes étapes

PCA et PRA

Élaborer un PCA ne s'improvise pas, et bien qu'il existe de nombreuses manières d'élaborer un PCA efficace, la philosophie de sa conception et de sa mise en œuvre reste semblable dans les différentes configurations existantes

1) Nomination d'un chef de projet ou correspondant PCA

Idéalement, tout comme dans le cadre d'un correspondant sécurité, le responsable qui sera nommé pour prendre la direction du projet PCA doit pouvoir bénéficier d'une grande autonomie ainsi que d'une grande indépendance vis à vis notamment de la DSI.

PCA et PRA

- En effet, au cours de sa mission, il aura notamment pour fonction de réaliser des audits et des analyses qui déboucheront en toute logique sur un certain nombre de préconisations organisationnelles et techniques à la manière que l'effectuerait un consultant externe (ce qui peut également être un choix, mais un correspondant PCA devra toutefois être nommé).

- Cette mission, il devra l'effectuer au sein des différents départements dits « critiques » de l'entité.

- Ce chef de projet un peu particulier est généralement détaché par la direction générale auprès du département de gestion des risques (lorsque l'entité en dispose évidemment...)

PCA et PRA

2) Audit de l'entité

Avant de pouvoir commencer l'élaboration du PCA, il convient de disposer d'un état des lieux précis concernant les activités de l'entité considérés comme critiques.

Si la ou les mission(s) principale(s) d'une entité ne peut plus être effectuée correctement, suite à l'arrêt d'une activité, alors on peut considérer cette dernière comme « critique ».

Le chef de projet aura dans ce cadre notamment la fonction d'auditer précisément ces activités, et procèdera notamment aux interviews des responsables de chacune des activités concernées.

PCA et PRA

3) Synthèse

Suite aux audits, analyses et interviews effectuées, le chef de projet réalisera un premier document afin de synthétiser les résultats de son travail.

Il y formalisera notamment une classification des différentes activités par niveau de criticité tout en précisant de manière exhaustive les différents liens entre ces activités, ces dernières pouvant être inter-dépendantes.

- Il est important de prendre en compte l'ensemble des facteurs, y compris humains pour éviter tout blocage lors de la mise en œuvre du plan de continuité.

PCA et PRA

4) Validation de la classification par niveau ce criticité

Afin de limiter les risques de cette étape importante, la classification des activités est soumise à la validation d'un comité de pilotage.

On trouve généralement dans ce groupe, en dehors du chef de projet PCA, des représentants de la DSI, de la Direction Générale, de la direction Administrative et Financière et de toute autre département pouvant figuré lui même dans les activités jugées critiques (exemple: département juridique, commercial, etc...)

Les éventuels points de la synthèse nécessitants une modification seront fixés lors de cette validation.

PCA et PRA

5) Élaboration du cahier des charges

La synthèse précédemment validée va permettre la réalisation d'un cahier des charges.

Au sein de ce dernier, et pour chaque activité critique, on trouvera la liste des éléments nécessaires à la reprise, aussi bien en terme d'infrastructure (postes de travail, serveurs, équipements réseaux, téléphones), que d'applications (outils métiers) ou de ressources humaines (compétences nécessaires, mobilisation, déplacement de personnel, transport, etc..)

Des niveaux de tolérance seront établis en terme de RTO et de RPO.

PCA et PRA

6) Choix des prestataires

Dans la mise en œuvre du PCA, comme dans la fourniture de certains services, il est souvent préférable de faire appel à des prestataires.

- En effet, l'utilisation de prestataires spécialisés peut offrir des garanties de moyens et/ou de résultats accompagnées de contre-parties financières tout en diminuant les coûts du PCA via la mutualisation appliquée par le prestataire (exemple : Datacenter)
- Externaliser permet également de s'assurer que les ressources seront allouées aux bons endroits, ce qui n'est pas toujours le cas lors d'une gestion interne...

PCA et PRA

7) Formalisation du PCA

Au cours de cette phase, le chef de projet devra décrire de manière claire et formelle, l'ensemble des processus à mettre en place, aussi bien en terme de site de secours que de profils humains et/ou de moyens techniques et logistiques pour les supporter.

- Les processus de gestion de crise devront eux aussi être clairement définis ainsi que la « cascade » des alertes et processus à activer lors de l'incident.
- De même, devront y figurer toutes les procédures de mise en place d'une cellule de crise, tout comme sa composition et la communication qui devra y être associée.

PCA et PRA

8) Validation du PCA

Le PCA une fois terminé devra encore être validé par le comité de pilotage afin de s'assurer de sa validité théorique.

Les éventuelles objections ainsi que les compléments d'information nécessaires seront formulés au cours de cette étape.

Une fois que les éventuelles dernières modifications auront été apportées, le comité entérinera alors la validation du PCA qui existe officiellement à partir de ce moment.

PCA et PRA

9) Tests et maintenance

Malgré sa validation, il ne faut pas oublier que le bon fonctionnement du PCA n'est à ce moment que théorique.

Il conviendra alors afin d'assurer un passage en production réussi de ce dernier de mettre en place une batterie de tests (et de crash tests) qui permettront d'évaluer les réelles difficultés aussi bien techniques ou logistiques qu'humaines qui pourraient se poser.

- Il faudra également assurer la « maintenance » du PCA, c'est à dire s'assurer de continuer à adapter ce dernier en fonction des différentes évolutions au sein de l'entité. Une historisation des opérations effectuées devra être réalisée.

PCA et PRA

Récapitulatif des étapes :

1) Nomination d'un chef de projet ou correspondant PCA
2) Audit de l'entité
3) Synthèse
4) Validation de la classification par niveau ce criticité
5) Élaboration du cahier des charges
6) Choix des prestataires
7) Formalisation du PCA
8) Validation du PCA
9) Tests et maintenance

PCA et PRA

Pour s'assurer de la réussite de son PRA et notamment dans le domaine informatique, il convient d'aborder le problème sous le bon angle.

1) Toujours penser au pire

Réussir à imaginer le pire, pour certains, c'est un métier, et qui plus est, n'est pas à la portée de tout le monde. Elaborer un PCA réussi nécessite de se pencher sur les scénarios les plus improbables, ceux que personne ne souhaite voir se produire.

Cette première étape est absolument indispensable à la réalisation d'un PRA réussi.

PCA et PRA

Il faut réussir à penser l'impensable, imaginer l'inimaginable : incendie, tremblement de terre, météorite, inondation, attentat terroriste, contamination bactérienne du système de ventilation : ce n'est pas parce qu'il est improbable qu'un incident arrive qu'il n'arrivera jamais.

Imaginer l'impensable, c'est ce qui va permettre d'imaginer les meilleurs scénarios de reprise : cela ne peut pas arriver, et pourtant c'est lorsque cela arrivera qu'il faudra un plan.

Il ne faut également pas oublier, que les PRA sont également utiles lors d'évènements mineurs mais pouvant impacter le bon fonctionnement de l'entité de la coupure électrique à la défaillance des systèmes d'aération...

PCA et PRA

2) Prévoir la gouvernance du risque

- Il s'agit d'un autre point capital où l'échec peut conduire à l'échec du PRA : qui fait quoi en cas de problème ?

- Il convient de prédéfinir la responsabilité et le rôle de chacun en cas de crise, tout en tenant compte des possibles indisponibilités humaines et notamment de la direction et/ou de la DSI.

- Il faut donc penser à sélectionner ceux qui agiront en cas de crise, qui pourra les remplacer en cas d'indisponibilité et quel sera le rôle et les compétences de chacun.

- Sans son volet humain, le PRA sera un échec total.

PCA et PRA

3) Ne pas négliger l'inventaire applicatif

C'est une étape importante qui concerne plus particulièrement le risque informatique : réaliser une cartographie des risques avec leurs conséquences et les solutions appropriées.

Pour réussir ce challenge il faut procéder à une cartographie des processus informatiques : chaque module applicatif devra être évalué afin de déterminer sa criticité et quelles sont les opérations à mener pour concevoir la préparation aux incidents.

On commencera donc par les applications pour descendre de couche en couche, jusqu'à l'OS puis au hardware.

PCA et PRA

- <u>Pourquoi cette étape est elle si importante ?</u>

- Simplement parce que c'est au cours de ce mapping détaillé que l'on va se rendre compte que tel ou tel autre processus métier ne peut pas fonctionner même en mode dégradé lorsque l'application y ne fonctionne plus : il s'agit bel et bien d'un travail de fourmis.

- Pour chaque application, on devra définir un RTO et un RPO avec une priorisation en fonction de la criticité et sans toutefois oublier les multiples dépendances en cascade existantes.

- C'est un travail long mais essentiel pour éviter l'échec au niveau du système d'information en cas de crise.

PCA et PRA

4) Définition des priorités et des moyens

- Lorsque l'on pose la question à un DSI ou directement à la direction concernant la perte de données en cas de crash, la plupart vous répondront qu'ils ne veulent perdre aucune donnée, et qu'ils ne veulent aucune rupture de service.

- Malheureusement nous ne sommes pas dans le monde des Bisounours : il faut savoir rester pragmatique et autoriser l'indisponibilité lorsque c'est plus judicieux : dans bien des cas, arrivé à un certain niveau, gagner une minute voire quelques secondes de disponibilité peut doubler voire tripler le prix de l'infrastructure.

PCA et PRA

- En fonction des métiers et des services, les exigences vis à vis du système d'information peuvent être complètement différentes.

- Choix d'une disponibilité toujours plus haute et/ou possibilité de fonctionner en mode dégradé sont autant d'options qu'il convient de penser dès le début de la conception du PRA.

- C'est de ces choix que devront découler les solutions techniques à mettre en place et non le contraire.

- Choix des systèmes de sauvegarde, de réplication et surtout du budget alloué qui va également conditionner et limiter les solutions possible : tout compte.

PCA et PRA

- Concrètement cette étape va consister à déterminer les meilleures technologies possibles qui correspondent aux RTO et au RPO choisis.

- Ces données vont indiquer quelles solutions peuvent être choisi : qu'est ce qui peut être sauvegarder à travers le réseau, sur bande ou sur support optique, qu'est ce qui nécessite d'autres systèmes (réplication de base et/ou de systèmes de fichiers)

- Après cette analyse, il restera donc à calculer et à négocier les prix de mise en œuvre de ces solutions. Le coût de ces solutions peut très vite exploser lorsque l'on veut se rapprocher du taux de panne 0

PCA et PRA

- 5) Faire des choix de matériel adaptés

- Dans certains PRA notamment de grands comptes ou d'administrations, ces derniers prévoient la mise en œuvre d'un site distant, soit au sein d'une autre unité de l'entité, soit de manière externalisée chez un prestataire (exemple : Datacenter).

- Il faut cependant pendre en compte que par définition, une crise est souvent d'une durée définie : les solutions sont là pour permettre un fonctionnement en mode dégradé ou pas le temps de retrouver une situation « normale ».

- C'est pour cette raison qu'il est souvent inutile de doubler l'ensemble de son matériel principal.

PCA et PRA

- En effet, faire un « copier /coller » du matériel existant sur un site distant ne veut pas dire faire le meilleur choix : le matériel destiné à reprendre l'activité doit être adapté à la situation de crise. Tout est après une question de budget.

- Par exemple une solution déjà redondée sur le site principal n'aura pas besoin de l'être au même niveau sur le site de secours.

- Le matériel devra être en permanence prêt à l'emploi : hors de question de perdre du temps en cas de crise. Même chose pour les choix d'opérateurs : le site principal est connecté un réseau multi-opérateur, mais un site mono-opérateur peut suffire pour un site de secours.

PCA et PRA

- 6) Crash test

- La majorité des entreprises qui disposent de backups ou autre solutions de reprise n'ont jamais fait de Crash Test. Or lorsque l'on pratique ce dernier, on se rend compte alors que plus de 7 cas sur 10 (étude réalisée par Digital Network sur plus de 100 entreprises ayant souscrit à différentes solution de backup) ne sont pas capables de remettre en route leur système d'information.

- C'est principalement pour cette raison que plus de 80% des entreprises ayant subit un sinistres informatique disparaissent dans les 3 ans.

PCA et PRA

- Une fois un PRA mis en place, il est en effet capital d'effectuer des tests de manière régulière afin de pouvoir évaluer sa fiabilité.

- Certaines directions sont frileuses à cause de l'aspect financier d'un Crash Test, c'est pourquoi cet aspect doit lui aussi être pris en compte lors de la conception du PRA.

- Lorsque l'on effectue un Crash Test, on se rend souvent compte que certains aspects ont été oubliés et qu'il faut remettre en question, adapter et mettre à jour son PRA.

- On conseille d'effectuer cette opération 1 fois par semestre : il ne faut pas oublier que le système d'information évolue très vite (versions de logiciels, os, upgrade matériel, etc...)

PCA et PRA

- 7) Adapter le PRA aux changements

- Un PRA partage un point commun avec l'audit : il est réalisé à un instant précis pour répondre à des contraintes précises. Il ne faut pourtant pas oublier que toute entité évolue, et particulièrement au niveau de son système d'information.

- Chaque changement applicatif, évolution majeure ou mineure, changement de matériel, mise à jour de l'OS : autant de paramètres qui peuvent nécessiter des adaptations du PRA.

- De même ces choix devront toujours être effectués dans un soucis de cohérence avec le PRA existant afin de minimiser les modifications.

PCA et PRA

8) Apprendre de ses erreurs

Nous n'avons vu plus tôt, effectuer des tests est capital pour s'assurer de la réussite d'un PRA. Cependant encore faut-il que les incidents rencontrés au cours de ces tests soient correctement signalés et transmises aux responsables concernés.

Beaucoup préfère « masquer » les échecs : ce n'est bien entendu pas positif pour un PRA. La mise en place d'une base de connaissance avec une journalisation des incidents est une bonne solution pour s'assurer de ce point.

L'amélioration du PRA doit être priorisée par rapport aux sanctions qui peuvent découler de son échec.

PCA et PRA

- 9) Ne pas oublier la règlementation

- On ne peut pas tout faire n'importe comment : bien souvent, un PRA est demandé par des autorités de régulation de secteurs particuliers tel que la Banque ou la Finance.

  Dans d'autres cas, ce sont au contraire ces derniers qui le demanderont à leur client pour minimiser les risques financiers.

- Il convient donc le cas échéant de se renseigner sur la réglementation administrative éventuellement en place tel que Bâle II qui est un dispositif destiné à mieux appréhender les risques bancaires.

PCA et PRA

- 10) Ne pas limiter le PRA à la DSI

- Comme expliqué en début de document, le PRA concerne tous les aspects de l'entité et pas seulement l'aspect systèmes d'informations et de télécommunications.

Le PRA est un processus transverse. Un désastre n'est pas toujours informatique, il peut être social (grève), climatique (inondation, températures anormales) ou médical (pandémie, contamination bactérienne du système de climatisation).

PCA et PRA

- Pour résumer :
-
- 1) Toujours penser au pire
- 2) Prévoir la gouvernance du risque
- 3) Ne pas négliger l'inventaire applicatif
- 4) Définition des priorités et des moyens
- 5) Faire des choix de matériels adaptés
- 6) Crash Test
- 7) Adapter le PRA aux changements
- 8) Apprendre de ses erreurs
- 9) Ne pas oublier la règlementation
- 10) Ne pas limiter le PRA à la DSI