LIVRE BLANC

CRiP

Club des Responsables
d'Infrastructure et de Production

Club de la Continuité d'Activité

L'OBSERVATOIRE des Directeurs d'Infrastructures et de Production

PRA

Définitions, Concepts,
Bonnes Pratiques & Enquête



LUC VRIGNAUD
FRANÇOIS TETE

Janvier 2011

CRiP
Infrastructure
& Production

Club des Responsables
d'Infrastructure et de Production



Club de la Continuité d'Activité

Table des matières

Avant-propos : le groupe de travail PRA

Éditorial de Luc Vrignaud (CRIP), pilote du GT PRA

Éditorial de François Tête (CCA), copilote du GT PRA

Les participants

1. Continuité, PRA, ... et compagnie : introduction

2. Architecture et cohérence applicative
    - 2.1 Introduction
    - 2.2 Architecture
    - 2.3 Bonnes pratiques
    - 2.4 En conclusion

3. Déclenchement du PRA et gestion de crise
    - 3.1 Introduction
    - 3.2 Résumé du chapitre
    - 3.3 La genèse : 'Le PRA naquit de l'incident majeur'
    - 3.4 La gestion de crise : Une organisation et un processus
    - 3.5 Les critères de déclenchement
        - 3.5.a Un objectif de temps
        - 3.5.b Un objectif de service
    - 3.6 Des outils pour établir ses priorités
    - 3.7 Une organisation, des équipes au service du PRA
    - 3.8 Communication Ciblée de crise
    - 3.9 Retour à une situation normale
    - 3.10 Quelques leçons à tirer

4. Validation probante du PRA
    - 4.1 Introduction
    - 4.2 Résumé du chapitre
    - 4.3 Définitions
    - 4.4 Quelques critères pour qualifier un exercice probant
    - 4.5 Écueils et bonnes pratiques

5. Maintien en Condition Opérationnelle du PRA
    - 5.1 Introduction
    - 5.2 Résumé du chapitre
    - 5.3 Principes du MCO
    - 5.4 MCO d'un PRA à froid
    - 5.5 MCO d'un PRA à chaud
    - 5.6 MCO d'un PRA en haute Disponibilité
    - 5.7 Enjeux et gouvernance
    - 5.8 Écueils et bonnes pratiques

6. Contrat de service et PRA
    - 6.1 Introduction
    - 6.2 Résumé du chapitre
    - 6.3 Points à prendre en compte en amont de la rédaction du contrat de service

6.3.1 Cas général, que le contrat soit interne ou externe :
6.3.2 Zoom sur l'externalisation du PRA
6.3.3 Périmètre de l'externalisation du PRA
6.4 La caractérisation des niveaux de service
6.4.1 La contractualisation des niveaux de service du MCO du PRA
6.4.2 La contractualisation des niveaux de services applicables aux opérations de tests du PRA
6.4.3 La contractualisation des niveaux de services en cas de déclenchement du PRA
6.5 Pilotage du contrat de service
6.6 Écueils et bonnes pratiques

7. Le vocabulaire PRA dans ce Livre Blanc

Conclusion

Annexes

A propos du CCA

A propos du CRIP

Table des figures :

Figure 1 : le plan de continuité d'entreprise
Figure 2 : le plan de continuité d'activité
Figure 3 : les différentes solutions de secours
Figure 4 : les coûts : indisponibilité/reprise d'activité
Figure 5 : niveaux de maturité d'un PRA
Figure 6 : PCA et gestion de crise
Figure 7 : architecture de secours à froid
Figure 8 : architecture de secours à chaud
Figure 9 : architecture de secours en haute disponibilité
Figure 10 : le processus de gestion de crise
Figure 11 : la pyramide d'escalade
Figure 12 : schéma simplifié du processus opérationnel de gestion de crise
Figure 13 : RPO et RTO
Figure 14 : le RTO par type de secours : secours à froid
Figure 15 : le RTO par type de secours : secours à chaud
Figure 16 : le RTO par type de secours : secours en haute disponibilité
Figure 17 : le BIA
Figure 18 : classification des processus
Figure 19 : matrice technique d'impact

Avant-Propos

le groupe de travail PRA

«La veille d'un incident, le ROI d'un système de sécurité est nul, le lendemain il est infini ...»
Dennis Hoffman de RSA

Le groupe de travail PRA rassemble des membres du CRiP et des adhérents du Club de la Continuité d'Activité (CCA). Il fonctionne comme un observatoire des plans de reprise d'activité, avec une dimension avant tout opérationnelle ; une approche qui se veut complémentaire des démarches d'études prospectives proposées par d'autres groupes de travail du CRiP.

Le paradoxe et la difficulté qui caractérisent le domaine des PRA restent entiers : le retour sur investissement (ROI) et la réduction des coûts pèsent d'un côté ; les obligations réglementaires et la sécurité tirent de l'autre. Tout est illustré dans la petite citation de Dennis Hoffman.

La difficulté pour le groupe de travail PRA a consisté à ne pas proposer le nième rapport sur la nécessité d'un PRA/PCA, sur les obligations réglementaires et légales, sur la maturité des technologies, etc., mais à appréhender certains sujets plus spécifiques et concrets, dans un objectif d'amélioration de nos pratiques :

- Définitions et types d'architectures,
- Gestion de la cohérence applicative,
- Déclenchement du PRA et Gestion de crise,
- Valeur probante d'un PRA,
- Maintien en Condition Opérationnelle,
- Négociation d'un contrat d'outsourcing du PRA,
- Les concepts et le vocabulaire.

L'objectif de ce livre blanc est bien de partager des retours d'expériences, des schémas, des abaques, du vocabulaire... transposables au domaine d'activité de chacun.

Parallèlement à cette approche, le groupe a lancé un questionnaire auprès de ses membres pour estimer approximativement la maturité des grands comptes français en matière de PRA, tant en termes de stratégie qu'en termes d'innovation.

Bonne lecture à tous

FRANÇOIS TETE & LUC VRIGNAUD

Edito rial

Bonjour à tous,

Après plusieurs mois de participation collégiale à son élaboration, nous vous livrons enfin le livre blanc sur les plans de reprise d'activités.
Nous avons voulu offrir au lecteur un panorama de l'existant sur les PRA. Cependant depuis le lancement du groupe de travail, nous assistons à une mutation des stratégies selon plusieurs axes :

- L'évolution des technologies dans les offres des fournisseurs (par exemple les nouvelles solutions de haute disponibilité chez les fournisseurs de baies de stockage, la généralisation de la sauvegarde sur disques et l'emprise croissante de la déduplication, les nouveaux usages de la virtualisation dans une optique de résilience, etc.).
- Un accroissement de la contrainte déjà exercée par les régulateurs dans les domaines de la reprise et de la continuité d'activité (audits internes, audits par commissaires aux comptes, directive Solvency II, directive Bâle 2, ...)
- Le constat d'une difficulté grandissante à maintenir en condition opérationnelle des infrastructures de secours complexes non-utilisées.
- L'apparition d'une nouvelle offre : le cloud computing.

Au cours de nos échanges, nous avons tous senti que ces nouvelles orientations émergeaient d'un besoin de service grandissant, lui-même issu de l'interconnexion de nos partenariats, de l'intensification de nos échanges internationaux, d'une complexification globale du fonctionnement des entreprises dans un environnement mondialisé.

Cela m'a rappelé les propos échangés lors d'une table ronde du dernier salon itiForums en juin 2010 : « La nouvelle problématique des risques : quelles conséquences pour la continuité d'activité ? ».

Si je devais résumer la teneur des débats tenus ce jour-là, je titrerais « L'effet papillon : bête noire de la gestion du risque ? ».
En deux mots : dans les dix dernières années, se sont multipliés des phénomènes extrêmes et peu probables (attentats du 11 septembre 2001, ouragan Katrina, crise mondiale de 2008, volcan islandais Eyjafjöll, phénomènes climatiques extrêmes, ...) qui ont impacté toutes les entreprises à diverses échelles.

On est passé de la gestion du risque à la gestion de l'incertitude ; avec un vieux constat : tout est interconnecté et interdépendant.

Ces événements nous rappellent donc qu'il est judicieux de concevoir la continuité d'activité en cherchant en premier lieu à déterminer ce qui est critique – des processus et des hommes ; et ceci indépendamment de causes pouvant subvenir.

Le PRA, au fil de cette évolution, passe du statut d'assurance risques au statut de process opérationnel indispensable à la continuité d'activités de l'entreprise.

Bonne lecture à tous

LUC VRIGNAUD,
Leader du Groupe de travail PRA
MACIF



Editorial

Bonjour à tous,

La notion de secours informatique suite à un sinistre est née en France, suite aux événements de Mai 68. Les dirigeants de trois grandes sociétés industrielles françaises prirent alors conscience du risque de blocage qui menaçait toute entreprise. Ils décidèrent en conséquence de créer un centre informatique de secours mutualisé, qui vit le jour dans les années 1970 : le GT2I. Il faut rendre ici hommage à son créateur Joël Moreau.

Devenues conscientes du risque, les directions informatiques se mirent à développer des plans de secours informatique. On parlait alors essentiellement de sinistre physique : incendie, inondation, ... Le secours consistait à réaliser des sauvegardes quotidiennes sur bandes magnétiques. Externaliser plusieurs centaines de bandes engendrait un gros travail logistique, et la faible fiabilité des supports magnétique posait de nombreux problèmes. Les moyens de secours informatiques étaient en général mutualisés et fournis par des sociétés spécialisées.

Les métiers de l'entreprise étaient rarement consultés pour déterminer leurs besoins quant à la disponibilité des applications sur lesquelles reposait leur activité. Les informaticiens décidaient à leur place. Les métiers participaient tout de même aux exercices de secours, et donnaient leur avis sur les conditions de reprise d'activité.

Que de chemin parcouru depuis. D'autres types de sinistres ont être pris en compte : ils touchaient les locaux de l'entreprise, puis les hommes. Les plans de continuité d'activité de l'entreprise (PCA) se sont développés. Le plan de secours informatique devenu plan de reprise d'activité informatique (PRA) a été intégré dans ces PCA.

Les conditions de reprise d'activité déterminées par les métiers et validées par la direction générale ont nécessité des solutions de secours de plus en plus sophistiquées. La technologie, ayant considérablement évolué, a facilité ces évolutions.

Certains thèmes de maturité différente restent à couvrir au sein des entreprises :

- Le maintien en condition opérationnelle des PRA
- La validation probante des PRA afin d'être sûr qu'ils fonctionneront le jour où se produira réellement un sinistre
- La reprise d'activité partielle par domaine applicatif
- La prise en compte de la continuité d'activité dans la conception d'applications
- La présence indispensable d'hommes clefs pour assurer la reprise d'activité dans le délai prévu

Ce livre blanc vous donnera des pistes. Le bonheur est dans le PRA ...

FRANÇOIS TETE,
Président d'honneur et
Secrétaire Général
CLUB DE LA
CONTINUITÉ D'ACTIVITÉ



LES PARTICIPANTS

Les pilotes du groupe de travail :

LUC	VRIGNAUD	MACIF
FRANÇOIS	TETE	DEVOTEAM

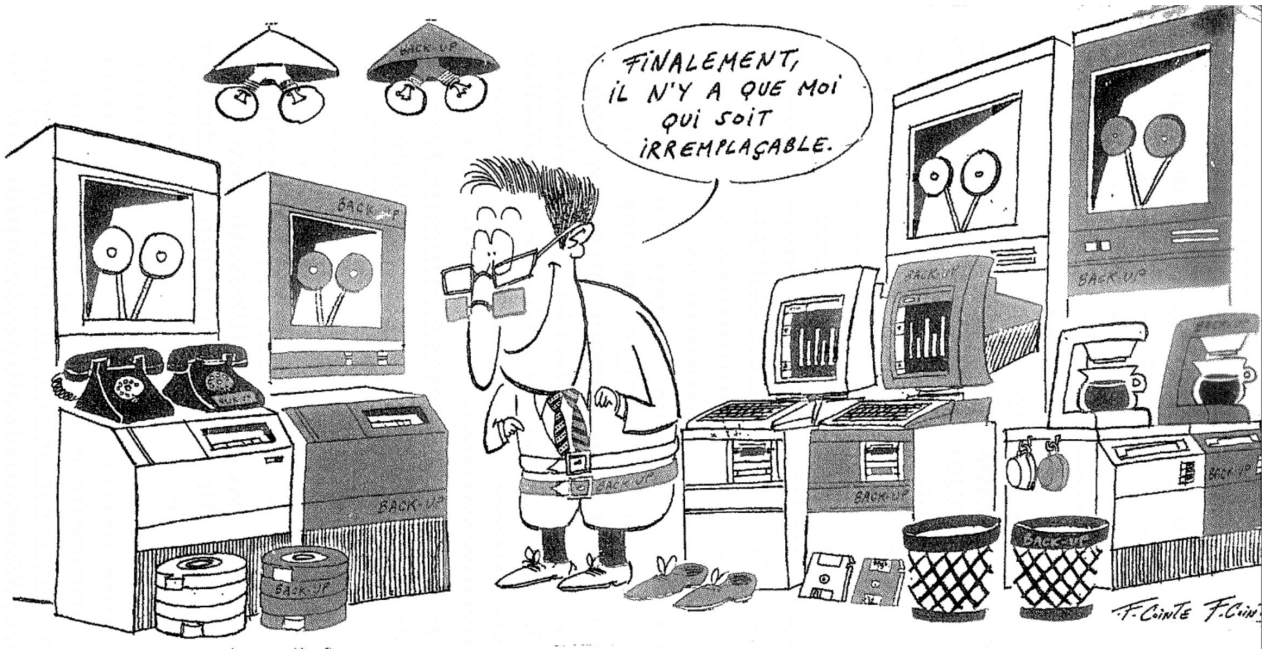
Nous remercions particulièrement pour leur participation active et assidue :

THIERRY	BECAULT	CNP ASSURANCES
SOLEIMAN	BELLI	AIR FRANCE
RENAUD	BONNET	CRiP
FLORIAN	CARRIERE	SOLUCOM
ALAIN	CESAR	EDF
ÉRIC	TOMAN	GDF / SUEZ
GERARD	VILLERS	AEROPORT DE PARIS

Nous remercions pour leurs contributions :

LUDOVIC	BEY	INA
GERARD	FOURNET	CREDIT IMMOBILIER DE FRANCE
THIERRY	HARENG	SOLUCOM
DIDIER	PLAT	CNAV
GUY	PRUD'HOMME	GROUPE CASINO
JOSE ANTONIO	RODRIGES	POLE-EMPLOI
THIERRY	SELTZ	PSA PEUGEOT CITROËN
FRÉDÉRIC	SEVESTRE	CARREFOUR
MARIE-JOSE	VANBAELINGHEM	MINISTERE EDUCATION NATIONALE
CHRISTIAN	VALLY	ARMEE DE TERRE
PATRICIA	VIOLETTE	THALES

Merci à tous



Avec l'aimable autorisation de F Cointe.
http://www.fcointe.com/

1 CONTINUITÉ, PRA, ... ET COMPAGNIE : INTRODUCTION

« Le PRA : L'assurance de l'inutile ? »

La Continuité d'Activités s'intègre dans la stratégie globale de l'entreprise, et sert des objectifs de natures différentes :

- Garantir la continuité de l'activité de l'entreprise
- Assurer la conformité réglementaire (Bâle II, Solvency II, etc.)
- Réduire les coûts de la gestion des risques
- Améliorer la sécurité, la protection de ses données
- Démontrer la pérennité de l'entreprise sur les marchés
- Devenir un partenaire plus attractif de par son niveau de résilience

Les grandes orientations concernant la continuité d'activité sont généralement décrites dans un document de stratégie d'entreprise (politique de continuité), qui se voit décliné en plans de continuité d'activités (PCA), et dont le maillage dépend de la taille de l'entreprise (plans applicables aux périmètres entreprise, direction, départements, filiales, etc.) et des types de sinistres pris en compte.

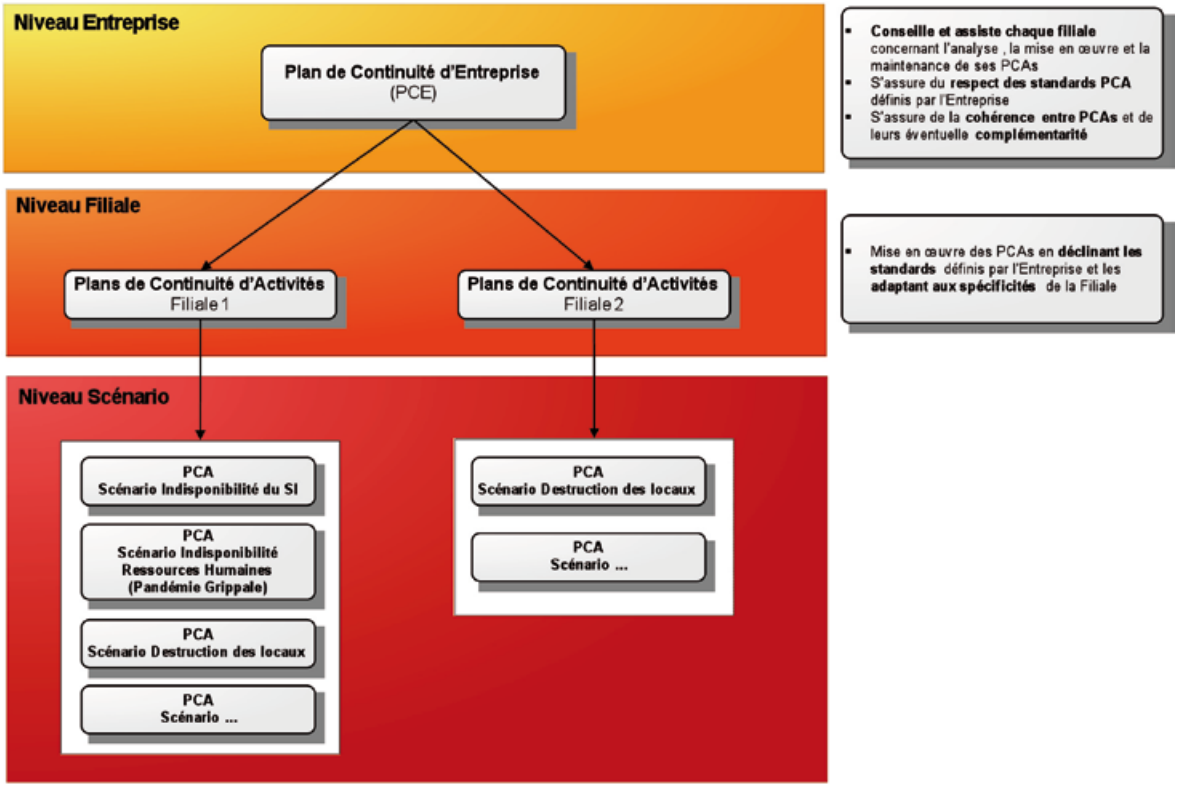


Figure 1 : le plan de continuité d'entreprise

Le PCA résulte le plus souvent d'une analyse d'impacts des risques majeurs capables d'altérer la continuité d'activité des métiers de l'entreprise. Ces risques peuvent être de divers types : destruction de donnés, perte par sinistre du site de production, déni de service, incident d'opérateur télécom, perte d'énergie électrique, vandalisme numérique et bien d'autres.

Le Plan de Continuité d'Activités se décline généralement en deux niveaux

• Un PCI (plan de continuité des infrastructures) qui dépend :

- des caractéristiques des solutions matérielles mises en œuvre (avec ou sans redondance),
- de l'organisation du Maintien en Condition Opérationnelle, de la disponibilité d'astreintes (volet RH – voir Libre Blanc du CCA – Plan de Continuité d'Activités et gestion de crise : guide pratique à l'attention des DRH, 2010, CCA[1]),
- d'un éventuel **PCA métiers** (PCM).

• Une organisation qui s'appuie sur des dispositifs d'exception :

- Une **organisation de crise** générale de l'entreprise, intégrant des sous-volets de gestion de crise par sous-systèmes : dont le Système d'Information.
- Un **PCA Métiers** (PCM) : des palliatifs métiers pour maintenir l'activité pendant la remise en état.
- Un **PRA informatique** : des solutions matérielles et organisationnelles pour reconstruire rapidement la partie du système d'information vitale pour l'entreprise.

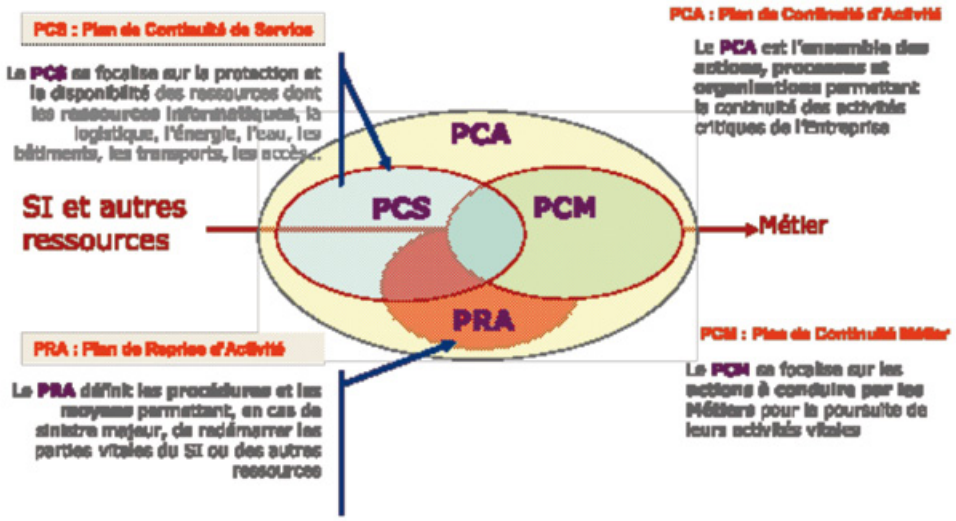


Figure 2 : le plan de continuité d'activité

Le présent livre blanc se focalise sur le PRA du SI et les moyens associés en termes de processus, mais n'abordera pas les multiples aspects des technologies disponibles éligibles au PRA.

Si le nombre d'architectures existantes croît d'année en année (architectures physiques, virtuelles, dématérialisées, architecture simple sans secours, avec sauvegarde locale, en PRA à froid, en PRA à chaud, en haute disponibilité, en tolérance de pannes, ...) celles-ci peuvent se caractériser plus simplement par leur niveau de service.

1. Téléchargeable sur le site du CCA http://www.clubpca.eu/

Dans la suite du présent livre blanc nous avons choisi de nous limiter à la typologie suivante :

Type de secours	Reprise des données	Reprise des traitements	Solution de secours
Haute disponibilité	A la dernière transaction	Sans interruption si l'application est conçue pour cela, sinon quelques minutes	Clustering et mirroring sur un environnement dédié
A chaud	De quelques minutes à quelques heures	Inférieur à 4 heures	Réplication cohérente des données entre site de production et site de secours, environnement de secours dédié
A froid	De 12 à 36 heures suivant l'heure du sinistre	De deux à cinq jours	Sauvegardes sur médias mis hors site, environnement de secours mutualisé ou dédié

Nous nous sommes attachés à préciser dans chaque chapitre les particularités de chaque type de PRA au regard des charges de MCO (maintien en condition opérationnelle) associées, du niveau de maturité requis en termes de MCO, des règles d'outsourcing ou encore des facilités de validation (test et exercice) du PRA.

Haute disponibilité

Pour la haute disponibilité, les équipements (serveurs et baies de stockage affectés à une application) du site de production et du site de secours coopèrent en permanence pour assurer aux utilisateurs un service continu.

Le dispositif maintient la cohérence des traitements et des données sur les baies de stockage entre le site primaire et le site de secours.

Les données placées sur les baies de stockage sont répliquées dans les deux sens pour qu'il n'y ait pas d'interruption de service.

Le dispositif de haute disponibilité impose une architecture technique et applicative spécifique, prise en compte dès la conception, et dans laquelle des serveurs sont dédiés au secours et actifs en permanence, ou passifs mais automatiquement activés dès la détection de l'incident (ex : modèle maitre/esclave avec heartbeat).

Parfois, la puissance disponible sur le deuxième site est moindre que celle installée sur le site principal. Dans cette situation, il y a possibilité de dégradation des temps de réponse en cas d'indisponibilité d'un des deux sites, puisque le site resté actif prend en charge l'ensemble de l'activité et risque alors de se retrouver alors surchargé.

Remarque : *la haute disponibilité n'inclut pas la tolérance de panne. Le basculement en mode secours dans un dispositif de haute disponibilité peut engendrer une rupture temporaire de service (sans perte de données) alors que dans un modèle de tolérance de panne il n'existe ni perte de données, ni coupure du service (et ceci grâce à des architectures matérielles spécifiques, avec des technologies du type partage de mémoire, de contexte, et autres).*

Secours à chaud

Le secours à chaud s'appuie sur une recopie des données « en continu » du site de production vers le site de secours (en mode synchrone ou asynchrone).

Les systèmes d'exploitation et les logiciels applicatifs sont identiques sur les deux sites mais les montées de version se font selon un contrat de service. La réplication des données des applications est gérée, par des moyens spécifiques.

Les serveurs de secours n'entrent en activité qu'en cas de situation de secours réel ou de test. En dehors de ces périodes, ils sont dormants et n'ont pas accès aux données répliquées.

Secours à froid

Le secours à froid fonctionne par transfert des systèmes d'exploitation, des logiciels et des données des applications vers un site de secours. Ce transfert est réalisé par sauvegarde puis restauration à partir de supports de sauvegarde externalisés (bandes le plus souvent).

La configuration de secours n'est activée qu'en cas de secours réel ou de test. En dehors de ces périodes, les serveurs et baies de stockage sont dormants ou utilisés à d'autres usages.

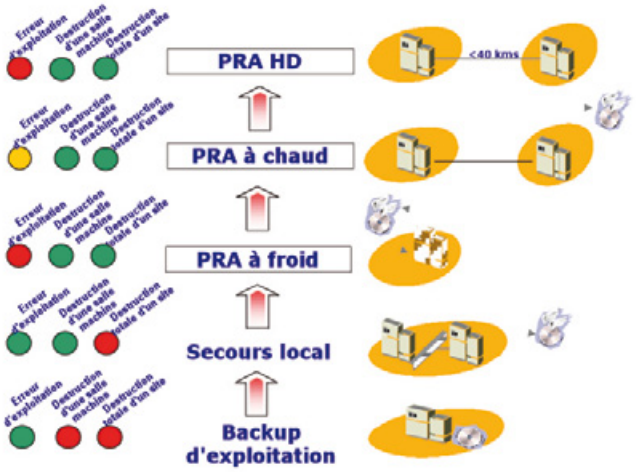


Figure 3 : les différentes solutions de secours

Ne pas confondre haute disponibilité et PRA

Un PRA peut recourir à de nombreuses solutions techniques pour répondre aux objectifs précédemment énoncés par la maîtrise d'ouvrage : solution en mode actif/passif, solution de répartition de charge (load-balancing), solution de réplication synchrone ou asynchrone, solution de reconstruction de serveurs, solution de virtualisation de serveurs, solution de sauvegarde des transactions, boot-on-SAN, solution de restauration des sauvegardes.

NB : *Il ne faut donc pas confondre haute disponibilité … et PRA ! La disponibilité répond à une exigence de continuité de service. Le PRA couvre les aspects de reprise d'activités après incident et/ou sinistre.*

Il n'existe donc pas une solution, mais des solutions de PRA au regard des prérequis de la maitrise d'ouvrage.

Il faut aussi rester conscient que le souhait d'une haute disponibilité de bout en bout reste souvent difficile à réaliser et à maintenir.

De plus, la continuité a un coût qui doit toujours répondre aux enjeux et risques qu'elle couvre.

Le choix d'une solution de continuité d'activités par l'entreprise est fonction d'une part du temps accepté d'indisponibilité d'un service et d'autre part des coûts associés à cette indisponibilité (criticité de l'application

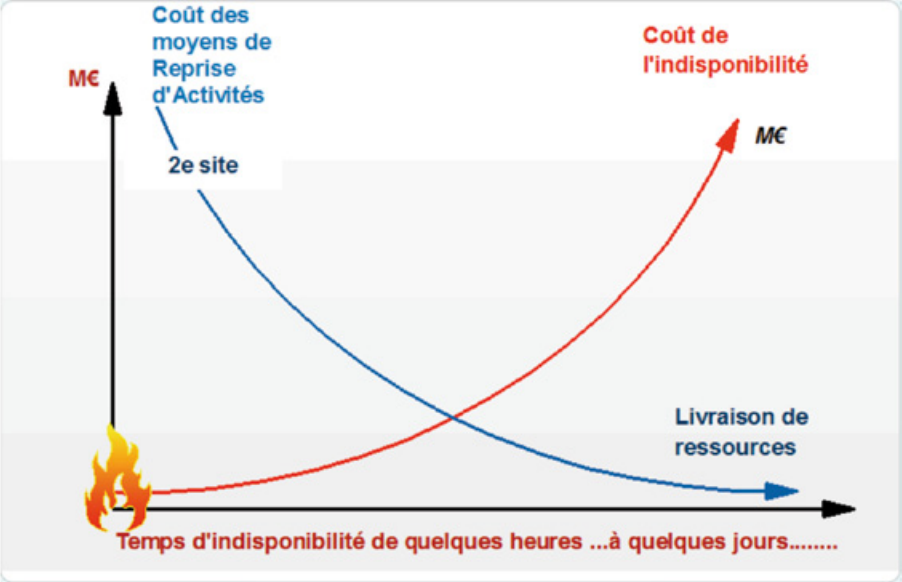


Figure 4 : les coûts : indisponibilité/reprise d'activité

Maturité des répondants

Exploitation du questionnaire
1er trimestre 2010

Un panel de 20 grandes entreprises

Taille des entreprises en nombre de collaborateurs :

- 1 000 :	17 %
1 000 à 10 000 :	25 %
+10 000 :	58 %

Nombre de datacenters :

0 à 2 :	27 %
3 à 4 :	45 %
+4 :	27 %

Distance moyenne entre datacenters :

- 2 km :	8 %
2 à 10 km :	31 %
+10 à 100 km :	31 %
+100 km :	30 %

Volumétrie du stockage SAN utile au PRA rapportée à la volumétrie SAN totale :

0 à 20 % :	12 %
+20 à 40 % :	25 %
+40 à 60 % :	38 %
+60 à 80 % :	25 %

Volumétrie SAN globale :

1 à 10 To :	0 %
+10 à 100 To :	25 %
+100 à 500 To :	50 %
+500 To :	25 %

Plan PRA :

Disponible dans 90 % des cas et testé au moins 1 fois par an
(maximum 3 fois par an)

Plan PCA :

Disponible dans 60 % des cas et testé en moyenne 1 fois par an
(maximum 2 fois par an)

Niveau de service après déclenchement du PRA :

Iso-production :	25 %
Fonctionnement en mode dégradé, à 80 % du nominal :	60 %
Autres (selon engagement) :	15 %

Déclenchement d'un plan PRA sur les 3 dernières années :

Non:	75 %
Oui:	25 % (causes: incidents sur infrastructure et problèmes électriques)

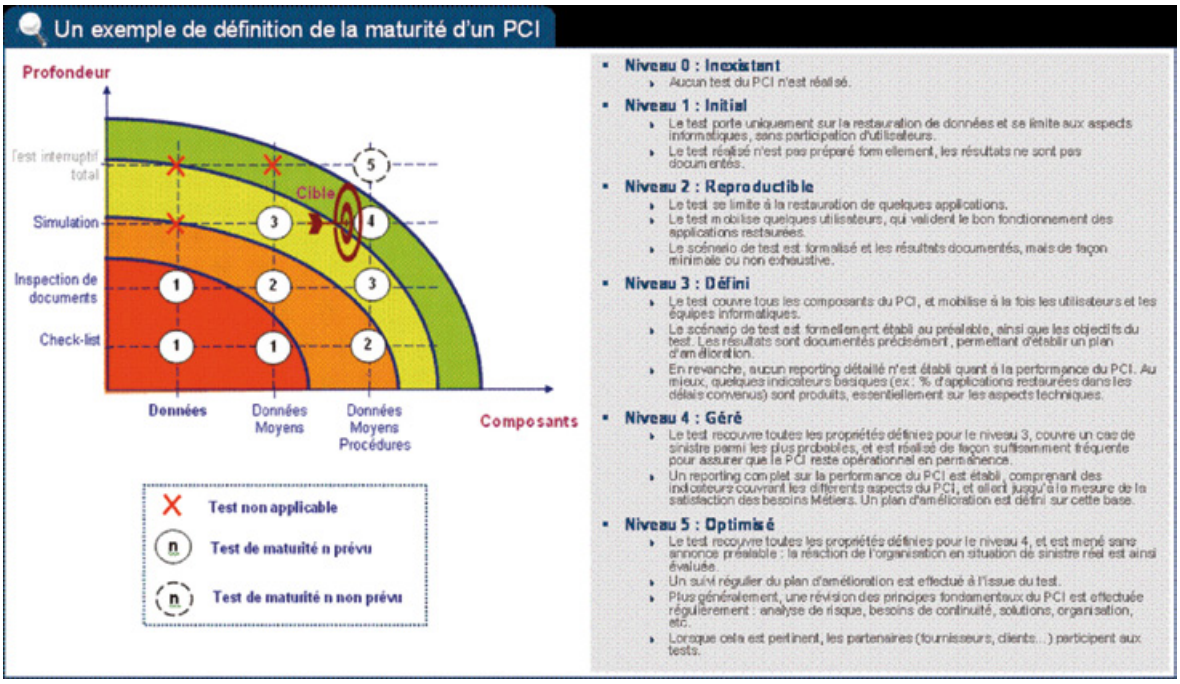


Figure 5 : niveaux de maturité d'un PRA

Suite à l'exploitation des questionnaires, nous avons déterminé que les répondants se situaient à un niveau de maturité compris entre 3 et 4.

→ Le volume maximal de perte de données admissible par les métiers, volume spécifié sous la forme d'une Perte Maximale de Données Tolérable (PMDT) ou d'une Perte de Données Maximale Admissible (PDMA). PMDT et PDMA se verront traduits en une réponse technique le « Recovery Point Objective » (RPO) lié à la stratégie de sauvegarde, et qui précise la durée maximale durant laquelle des données ont été perdues en cas de sinistre.

→ Le niveau tolérable de dégradation du service en cas de fonctionnement en mode secours (exprimé par exemple en pourcentage du SI secouru, ou en pourcentage de perte de capacité de traitement). En contrepoint, une autre valeur indique la durée acceptable de fonctionnement en mode dégradé (de quelques minutes à plusieurs jours).

→ L'existence de points de cohérence entre les applications qui communiquent entre-elles, et ce afin de faciliter la resynchronisation des flux entre applications au moment de la reprise (voir infra).

Une négociation sera souvent nécessaire à l'issue d'une première expression du besoin métier pour arbitrer entre le niveau de service attendu du SI et les limites du budget. Elle permet de repositionner le niveau relatif de couverture du plan de continuité Métiers (PCM) par rapport au PRA.

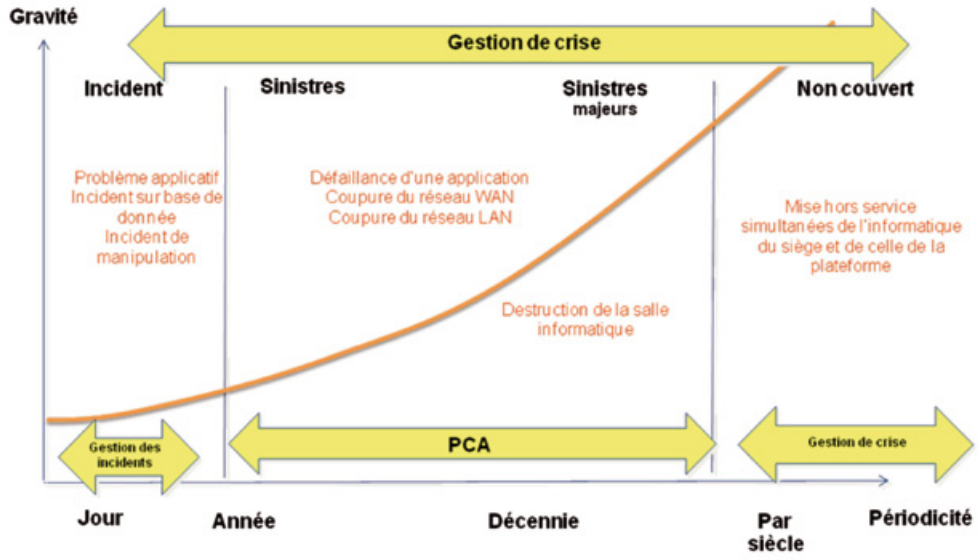


Figure 6 : PCA et gestion de crise

2 ARCHITECTURE ET COHÉRENCE APPLICATIVE

«La cohérence est comme le chaos : toute relative»
Luc Vrignaud

2.1 Introduction

Du besoin de continuité à la conception de l'architecture

La mise en place d'un PCA, et celle du PRA qui en découle, constitue d'abord une décision stratégique pour une entreprise, même si parfois des règlements externes le lui imposent (par exemple la Loi de Sécurité Financière LSF, les directives du Comité de la réglementation bancaire et financière CRBF). Une fois la décision de mettre en place un PRA prise, les choix stratégiques résident dans les solutions à retenir.

Les choix organisationnels et d'architecture découlent d'une analyse des impacts (financiers, sur l'image de marque de l'entreprise, réglementaires, conséquences d'une perte de productivité) relatifs à une rupture d'activité (partielle ou totale) touchant les processus critiques de l'entreprise, et des réponses qu'on choisit de leur donner.

Un premier niveau d'étude permet généralement de préciser le périmètre des processus ou activités à secourir.

Le besoin des métiers en termes de continuité d'activités doit être spécifié comme tout autre besoin. Certains critères ou notions, très techniques, peuvent paraitre évidents du côté des fournisseurs de ressources (le service informatique ou sa composante production), mais être inconnus coté client. Il y a donc lieu d'aider les métiers sur ces aspects.

On peut ainsi définir avec les métiers

→ Les risques contre lesquels chaque métier veut se prémunir (perte du datacenter, perte d'un immeuble, arrêt de production, perte d'intégrité des données, mouvement social, etc.) la réponse n'est pas obligatoirement la même pour chaque risque. La garantie 100 % tout risque n'existant pas, il convient de hiérarchiser les types de risques et de préciser les risques résiduels acceptables, c'est-à-dire non-couverts par le PRA. Les limites de la couverture assurée par le PRA devront être connues de la direction générale qui doit les valider.

→ Pour chaque processus métier (y compris les fonctions support comme l'informatique ou la facturation), les applications majeures ou critiques et les flux d'échanges indispensables associés.

→ Il existe au moment du sinistre un fort risque de perte de données, d'indisponibilité, en découle un impact sur l'activité, l'image, etc... Chaque métier évalue ces éléments pour classer les applications par criticité.

→ La durée maximale acceptable d'arrêt des applications informatiques pour chacun des métiers. Cette durée est spécifiée sous la forme d'un Délai Maximal d'Interruption Admissible (DMIA) qui se voit ensuite traduit en une réponse technique le « Recovery Time Objective » (RTO) qui précise le temps maximum que doit prendre la remise en fonction.

Traduire le besoin en solution avec le métier

Un sinistre informatique provoque un saut dans l'espace et dans le temps. Saut dans l'espace : la reprise aura lieu à un autre endroit. Saut dans le temps : il y aura eu une interruption, la reprise aura lieu à une heure différente.

La reprise d'activités se fera en fonction du type de secours (à froid, à chaud, haute disponibilité) dans un délai de quelques minutes à quelques jours.

Suite au sinistre, les traitements en cours se sont arrêtés brutalement. A la reprise d'activité, on doit éviter de perdre des flux reçus et de renvoyer des flux qui engendreraient des doublons (commandes, virements, ordres, ...).

Les différentes solutions seront comparées sur la base des besoins exprimés. Il sera nécessaire de revenir vers le métier pour préciser certains points :

- Peut-on revenir en arrière et rejouer des traitements ?
- Peut-on se référer à des points de synchronisation ?
- La reprise applicative peut-elle être automatisée ? L'automatisation technique de la reprise d'activités n'est pas envisageable, du fait des milliers de cas possibles dépendant du moment du sinistre. Par contre il est indispensable d'automatiser les procédures, sous forme de listes de tâches ou descriptifs, pour reprendre l'activité dans un temps court.

La problématique de la cohérence applicative dépend du type de solution de secours (à froid, à chaud, en haute disponibilité) et de la conception de l'application.

2.2 Architecture

Secours à froid

Le secours à froid constitue la plus simple des solutions de reprise d'activités, mais aussi celle à laquelle recourir lorsque tout a échoué. D'ailleurs, une solution de PRA de type haute disponibilité ou à chaud doit toujours être accompagnée d'un secours à froid.

Dans cette configuration, le site de production et le site de secours sont indépendants. Le site de secours reproduit à l'identique tout ou partie de l'architecture du site à secourir. Les données sont restituées sur le site de secours par des sauvegardes de recours suite au sinistre.

Les sauvegardes de recours sont des sauvegardes exhaustives, cohérentes et externalisées nécessaires au secours. Elles doivent être prises, idéalement, à un point de synchronisation dit « point propre ». La reprise d'activités se fait à partir de ce point d'ancrage. Le plan de continuité métiers (PCM) doit prévoir la reprise des traitements, en relation étroite avec l'informatique.

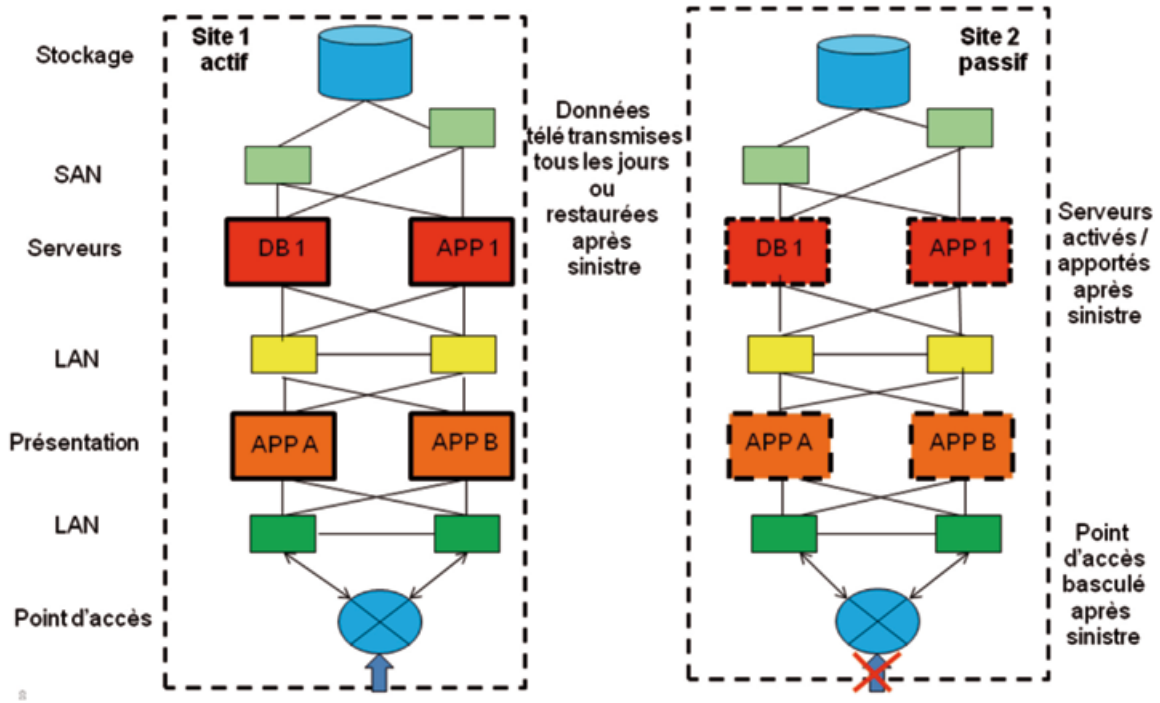


Figure 7 : architecture de secours à froid

Les données restaurées sur le site de secours sont intègres puisqu'issues de la prise de sauvegardes de recours. Les traitements effectués entre la dernière sauvegarde et le moment de l'incident sont rejoués, soit manuellement, soit à partir des logs.

Le PCM doit contrôler la cohérence du point de reprise et supprimer les doublons dans les traitements refaits. En effet les métiers possèdent une plus grande connaissance pratique de leurs données que les équipes informatiques, ce qui les qualifie pour avoir la main sur ces opérations. Les programmes doivent être prévus pour être rejoués.

Ce cas idéal présuppose l'existence d'un point de synchronisation souvent problématique à définir. Les traitements transactionnels et batch associés fonctionnent en général en permanence. Il est de ce fait difficile d'avoir un point unique de synchronisation des sauvegardes. Plusieurs techniques peuvent être utilisées pour assurer cependant la cohérence applicative :

- Des techniques de type « boite noire aviation » pour garder une trace des principales actions effectuées entre le point de sauvegarde et le sinistre.

- Des techniques pour l'application des « logs » des bases de données, si ils ont été externalisés.

Attention aux interactions en cascade entre systèmes multi-sites et / ou multipartenaires.

Le plan de continuité métiers, en association avec le service informatique doit déterminer, suite au sinistre, les modalités de la reprise d'activités.

L'étude préalable peut amener à renoncer à la saisie des donnés perdues, voire admettre un délai de régénération des données perdues conformément à la convention de service négociée avec le client, sur la base de l'analyse de risques.

Vu le nombre de cas envisageables, la diversité des situations et des architectures, l'automatisation de la reprise d'activités n'est pas possible techniquement. Des procédures manuelles de reprise et de contrôle restent absolument nécessaires.

Secours à chaud

Le site de production et le site de secours sont interconnectés et d'architecture identique pour la partie secourue. Les données sont répliquées sur le site de secours.

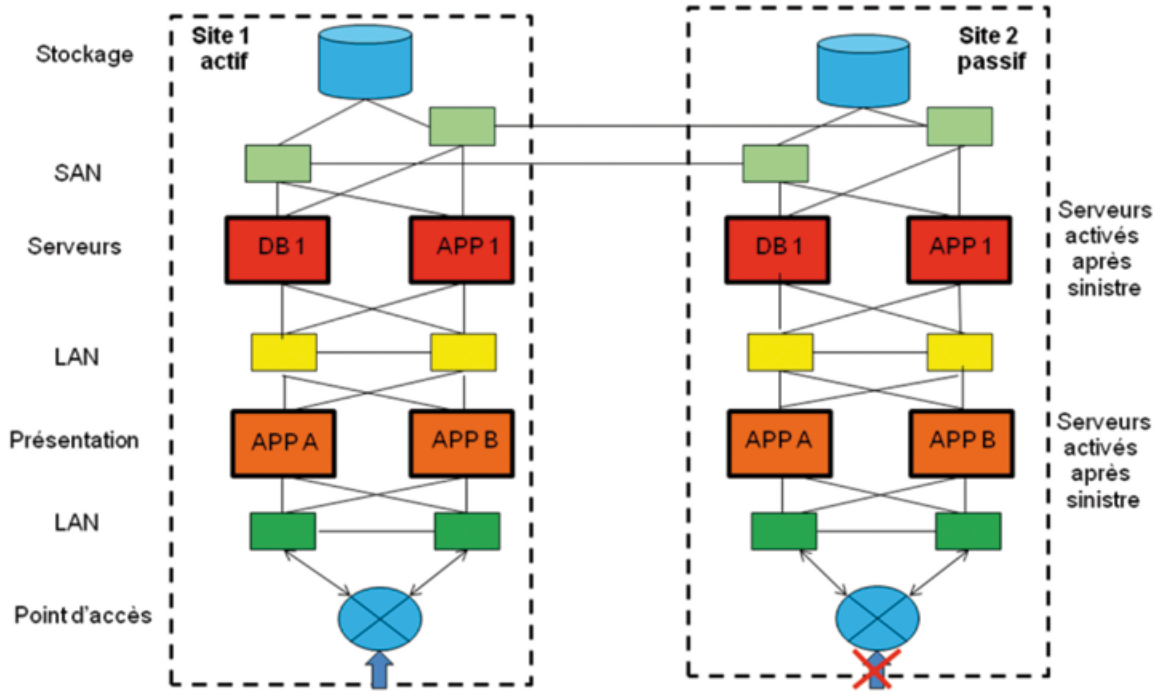


Figure 8 : architecture de secours à chaud

La cinématique du déroulement de la reprise d'activités se déroule comme suit, après la survenance du sinistre :

- Coupure de la réplication entre les deux sites.
- Lancement des procédures de sauvegarde totale des données sur le site de secours (mesure conservatoire et optionnelle pour pallier une perte totale des disques et des sauvegardes de production). Attention à la durée de la sauvegarde.
- Lancement des procédures les plus appropriées à la reprise par domaine applicatif :
  - Activation de l'infrastructure de secours et contrôle de l'intégrité technique de cette infrastructure.
  - Exécution des procédures de reprise des données et contrôle de l'intégrité fonctionnelle.
  - Exécution des procédures de reprise d'activités des traitements par domaine applicatif.
  - Les traitements et les données sont resynchronisés.

Redémarrage des traitements sur le domaine applicatif de priorité la plus élevée à la moins élevée, selon les procédures de reprise appropriée (ouverture progressive des flux par domaine applicatif).

- Le site de secours devient site de production pour toutes les activités vitales de l'entreprise. Il est équipé à l'identique de tous les éléments secourus du site principal (robotiques, stockage, outillage, réseau, sécurité).

Haute disponibilité

Le site de production et le site de secours sont interconnectés, d'architecture identique, et fonctionnent comme un site de production unique. Les données sont obligatoirement identiques en permanence sur les deux sites.

La haute disponibilité implique l'automatisation du basculement à la dernière transaction avant sinistre. En général, la production se trouve répartie sur les deux sites (fonctionnement en mode dual-site). Mais l'exigence de certaines applications vis-à-vis des performances (temps de propagation des données), implique que la production se fasse parfois sur un seul site.

Si les performances sont acceptables on préférera mettre la réplication des données en mode synchrone. Actuellement la distance intersites pour ce mode de fonctionnement ne saurait excéder une cinquantaine de km.

La haute disponibilité repose souvent sur une architecture renforcée au niveau de chacune des couches suivantes :

- Serveurs (physiques ou virtuels) : ils sont redondés et distants.
- Stockage de données : les baies sont distantes et répliquées.
- Réseau : il est totalement redondé, y compris sur les deux sites.
- Ressources/environnement (électricité, climatisation) : ils doivent être redondés

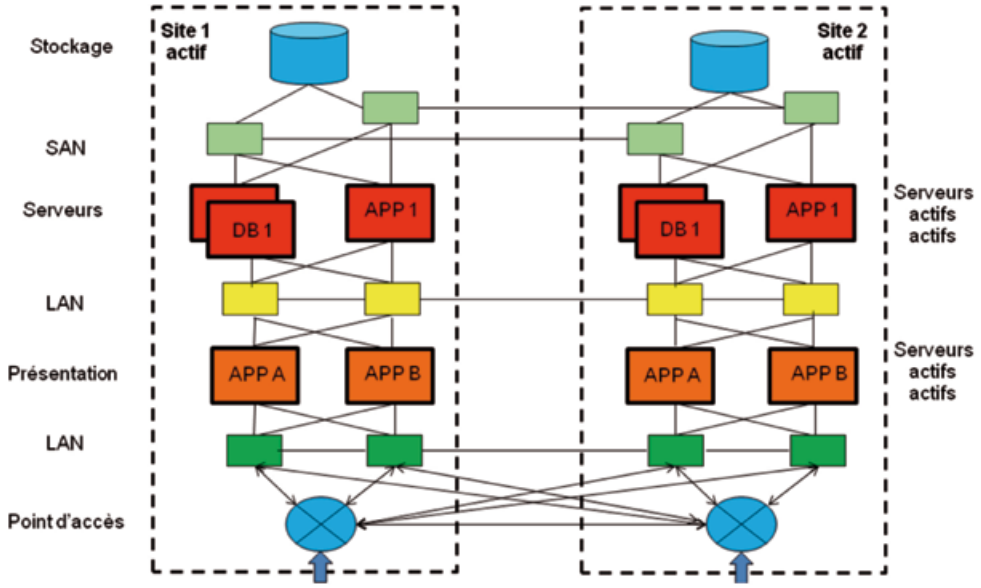


Figure 9 : architecture de secours en haute disponibilité

Les techniques de haute disponibilité peuvent se présenter sous différentes échelles, de la simple redondance locale des serveurs avec éventuellement redondance des données, à la mise en place de clusters distants avec baies de stockages en réplication. Cette dernière formule présente tout son intérêt pour faire face au risque de sinistre d'une salle.

Le plus souvent on utilise deux sites distants. Selon les attentes, les contraintes de maintien en condition opérationnelle on orientera son choix vers :

1. Déclarer un site comme principal et l'autre de secours (la production ne fonctionne effectivement que sur le site principal).

2. Avoir les deux sites actifs simultanément (la production est répartie sur les deux sites).

Les deux sites doivent-ils être de puissance identique ? Pas forcément, mais comme nous allons le voir une différence de capacité de traitement entre les deux sites posera toujours des problèmes en cas de sinistre.

- Cas 1 : les deux sites sont de puissance identique, alors le site de secours reprend en totalité l'activité du site principal.

- Cas 2 : les deux sites ne sont pas de puissance identique, alors le site survivant ne peut pas assurer l'ensemble des traitements cumulés. Il faut donc prévoir soit un délestage (fonctionnement dégradé) ; soit des moyens pour augmenter rapidement la puissance.
(Il est possible de négocier des clés d'activation de puissance (Power on Demand) en cas de PRA [ex : Capacity on Demand sur z Series chez IBM])

Dans les deux cas, si les systèmes et applications sont prévus pour, le basculement est automatique et rapide (de quelques secondes à quelques minutes). Par contre, selon la conception de l'application, le basculement peut nécessiter la réouverture des sessions de travail.

Coté données, des procédures de reprise doivent être prévues avec les métiers pour prendre en compte:

- La vérification et la reprise des transactions manuelles en cours au moment du basculement.

- La vérification et la reprise des batch en cours au moment du basculement.

En cas d'échec, la restauration des données s'imposera. La reprise à froid à partir des sauvegardes, même dans ce type d'architecture, reste un ultime secours.

Tableau comparatif entre la haute disponibilité intersites (deux sites distincts), inter-salles (deux salles au sein du même bâtiment), inter-bâtiments (deux bâtiments sur un même site).

Le choix pourra se faire en fonction des possibilités de réalisation et du niveau de couverture recherché pour chaque risque.

Haute disponibilité	Avantages / Inconvénients		
	Performances	**Facilité de MCO**	**Disponibilité**
Inter-salles	**+ + +** Bonnes (Réplication synchrone)	**+ +** Facilité par la proximité	**-** Risques dus à l'environnement partagé (énergie, climatisation, réseau, accès, localisation perte du bâtiment, ...)
Inter-bâtiments	**+ + +** Bonnes (Réplication synchrone)	**+ +** Facilité par la proximité	**+** L'environnement commun est réduit. Selon l'architecture des réseaux des ressources, le risque peut aussi être réduit
Intersites < 50 km	**+ + +** Bonnes (Réplication synchrone) (NB : perte de temps en traitement batch)	**-** Plus délicat du fait de l'éloignement	**+ +** L'indépendance des sites augmente avec la distance
Intersites >50 km	**+** Dégradation selon distance (Réplication asynchrone)	**-** Difficultés du fait de l'éloignement → Nécessite du personnel comptent sur site	**+ + +** Meilleure indépendance des sites vis-à-vis de sinistres régionaux

Retour à une situation normale (commune aux trois types de PRA)

Le retour à une situation normale peut être rapide (de l'ordre de la semaine) ou prendre plusieurs mois et se fait comme suit :

- Préparation d'un site de production nominal à la reprise (réparation/construction, recette).
- Resynchronisation/restauration des données.
- Fonctionnement normal.

2.3 Bonnes pratiques

Découper le SI en plaques « secourables » homogènes

Les SI modernes ne fonctionnent plus en silos : il est illusoire de chercher un point de synchronisation global pour le PRA. La question est donc « comment découper le SI en plaques « secourables » homogènes » ?

Il n'y a quasiment plus aujourd'hui d'application ou même de chaîne applicative fonctionnant en « stand-alone » : les échanges multilatéraux sont très nombreux, rarement documentés exhaustivement (en tous cas, leur criticité reste rarement définie) et concrètement, cela s'est traduit ces dernières années par la multiplication des projets « EAI / bus applicatifs » qui viennent d'ailleurs simplifier le secours, s'ils le prévoient dès le début.

Du coup, il est quasiment impossible de définir un point de synchronisation « global » quotidien pour toutes les applications, ce qui conduirait à arrêter toutes les bases en même temps pendant X heures, le temps de les sauvegarder … et encore moins s'il faut définir plusieurs de ces points par jour, en fonction de la durée d'interruption la plus exigeante.

En conséquence : il faut impérativement découper le SI en plaques présentant des échanges de flux minimum, et si possible regroupant des applications avec des besoins (durée maximale d'interruption admissible DMIA / PDMA) proches.

Utiliser des solutions techniques facilitant la synchronisation des sauvegardes / jeux de données répliqués du PRA

Pour limiter la fenêtre nécessaire à la synchronisation, il est désormais possible de s'appuyer sur les outils de snapshot ou équivalent. On passe de quelques heures à quelques secondes d'indisponibilité de la base de données. On est sûr d'en posséder une version cohérente (au sens du SGBD). Il est donc beaucoup plus facile de trouver un point de cohérence fonctionnelle.

En utilisant en plus les outils de journalisation de la plupart des applications / SGBD, on se limite à la réplication synchrone de volumes limités de données.

La plupart des outils de SGBD savent désormais gérer la notion de « groupes cohérents » : cela demande néanmoins un travail de conception en amont (définition des dépendances entre bases), puis d'implémentation technique, en allant jusqu'aux tests.

Dans le cas particulier des architectures orientées services (SOA) : même s'il est toujours possible de mettre en place des clusters au niveau des SGBD et des serveurs d'application (Websphere, Tomcat), il n'y a pas de solution idéale pour secourir les « queues managers ». Il faut impérativement intégrer la dimension secours dès l'étude d'architecture, et prévoir les mécanismes de resynchronisation des files d'attente, qui aujourd'hui ne sont pas automatiques.

A noter le cas particulier de la corruption de données : *plus on met en place des mécanismes visant une faible perte de données, plus on augmente les risques en cas de corruption. Le secours se retrouve corrompu quasi-instantanément en cas de problème et du coup, il faut impérativement mettre en place des mécanismes complémentaires pour « remonter dans le temps » de façon toujours synchrone : par exemple, en conservant un historique des snapshots synchronisés sur 24h (ce type d'opération présente un impact significatif sur les besoins de stockage).*

Ne pas oublier que les Métiers sont toujours indispensables lors de la validation de la cohérence fonctionnelle du PRA

Malgré tous les efforts fournis au niveau technique par les équipes de la DSI, seuls les métiers sont in fine en mesure de confirmer la validité fonctionnelle et l'exhaustivité des données restaurées : les derniers contrôles doivent donc revenir aux métiers (par exemple : par un rapprochement de balances gestion / comptables dans le cas de reprise de données financières).

De plus, sauf exception, toutes les applications ne sont pas secourues avec les mêmes exigences : il y a donc forcément des besoins de resynchronisation « manuelle ».

Et enfin, entre les plaques secourables définies plus haut, il faut forcément assurer une resynchronisation : en rejouant des fichiers, en saisissant des données manuellement, ou par d'autres procédés du même type.

Impliquer les Métiers dès la conception de l'architecture pour préparer la validation des PRA

Comme nous avons à faire à des ensembles d'applications vitales, il n'est pas acceptable pour la maîtrise d'ouvrage de prendre des risques inconsidérés pour effectuer un test.

Une architecture de type PRA à froid est généralement isolée du réseau de production principal, il est alors possible d'effectuer des tests sur un réseau de secours indépendant. La difficulté réside généralement dans la mise en œuvre des flux hors périmètre PRA. Ce test reste alors partiel.

Un PRA à chaud se fait généralement sur des machines du réseau de production.
Le test le plus pertinent consiste à basculer les utilisateurs nominaux sur les applications en PRA. Mais la difficulté réside dans la fenêtre de basculement à choisir pour éviter un arrêt de service (par exemple basculement de nuit). L'architecture doit intégrer des mécanismes qui garantissent qu'aucune perte de données n'aura lieu lors d'un basculement programmé.

Un PRA haute disponibilité sans perte de données peut se tester par des basculements intersites. On évitera par mesure de précaution les périodes d'activité les plus chargées. L'architecture physique des sites, la distance entre sites, le type de connexion (fibre noire) doivent être conçu pour cela.

Parmi les points à prendre en compte, relevons aussi

→ L'application testée forme-t-elle un ensemble cohérent ?

- Problématique de cohérence des sauvegardes ou des copies de données entre elles (diverses technologies s'avèrent parfois nécessaires, ou il existe plusieurs serveurs à coordonner et de nombreux intervenants).

- Problématique du moment de l'interruption. Par exemple, si celle-ci met fin de manière anticipée à un traitement batch, il sera nécessaire de repartir avec des données dans l'état où elles se trouvaient au début de ce batch.

→ Les procédures de redémarrage doivent être prévues avec des sauvegardes /copies « durcies » indépendantes du moment du sinistre.

→ Inclure cette conception d'exploitation des sauvegardes et des attentes en termes de RTO et RPO dans la réflexion sur le choix de l'architecture. Selon la criticité les solutions sont variées (coût) mais la base de réflexion reste valable.

→ Consulter les documentations des constructeurs décrivant les processus de duplication et copie des données, les engagements des infogérants/hébergeurs, etc.

→ Gestion des flux et historisation des messages/fichiers.

→ S'entrainer à faire des tests (voir infra).

2.4 En conclusion

Comment passer du chaos à l'ordre ? Voilà qui pourrait résumer la vocation d'un chapitre sur la gestion de la cohérence applicative. En ces temps de complexité grandissante des SI, quelle est la solution optimale pour assurer un PRA ?

Pas de réponse définitive, même si nous le déplorons, mais pour clore ce chapitre nous vous proposons quelques pistes de réflexion complémentaires.

2.4.a Mettre en place une gestion du PRA par "groupes d'applications" (pour les reprises : rejeu, élimination des doublons, etc.)

Une telle démarche s'avère judicieuse dans un environnement où les groupes d'applications sont bien compris et maîtrisés par les métiers.

De plus, dans certains cas le métier possède des contrats de service définissant les échanges avec d'autres groupes d'applications ou métiers (les scénarios de reprise sont alors intégrés au niveau fonctionnel, ou bien la reprise concerne des blocs fonctionnels plutôt que des blocs techniques).
Cette gestion du PRA doit être prise en compte et formalisée pour chaque application, voire déplacée vers un outil ou une application spécialisée (ce qui dépend de la taille du groupe d'applications, de la complexité du service, de la connaissance fonctionnelle, etc.)

2.4.b Créer des "points stables"

Pour toutes les applications interdépendantes, cette procédure consiste à prendre :

- une même image des applications et de leurs données à des moments choisis,

- ou des images synchronisées (groupe de cohérence ou consistency group).

Mais créer des points stables s'avère une procédure complexe et contraignante.

Procédure Complexe : elle demande une définition rigoureuse des différents éléments concernés et de leurs interdépendances lors de sa conception et de sa mise en place, et risque de n'être valable que pour des périmètres limités.

Procédure Contraignante : elle impose le respect d'un horaire de prise d'images à l'ensemble fonctionnel qui a été défini (avec probablement la nécessité d'un micro-figement coordonné), elle peut limiter les évolutions futures (chaque évolution induit de nouveaux échanges, donc des changements de périmètre, de nouvelles interactions à intégrer dans l'annuaire des points stables, etc.)

Si ces calendriers de figement sont contraignants (figements temporaires) on en limitera le nombre, ce qui s'avèrera préjudiciable à une faible perte de données.
Mais l'idée est intéressante, surtout si on la rapproche de la précédente dans un plan de groupes d'applications et de points stables par groupes d'applications.

2.4.c Revoir l'urbanisation du SI

Il s'agit d'instituer ou d'améliorer le zonage des échanges inter-applicatifs pour faciliter les reprises intra-zone (chacun chez soi) et interzones (ouverture progressive vers l'extérieur). On peut envisager pour une telle pratique la mise en place d'outils

de gestion spécialisés dans chaque zone et des ''points de passage'' auditables (monitoring des Firewalls + traitement des logs par exemple) complétés par des outils globaux de gestion des flux et des reprises.

Encore une piste prometteuse mais non universelle et qui suppose de longs mois de conception et probablement des années de mise en place (pour les grands groupes multi-datacenters).

2.4.d S'en remettre aux constructeurs (? ...)

Une autre solution consiste à s'appuyer sur les développements technologiques et logiciels de nos fournisseurs (de stockage essentiellement), si ces technologies apportent une solution fiable, universelle et globale. La réponse est évidente avec ce dont nous disposons en 2010.

Explications : ***Il existe des réponses (partielles)***, par la création de groupes de cohérence associés à des procédures de réplication journalisée, ou au travers de boitiers de type RecoverPoint par exemple. Mais rien d'universel qui prenne l'image de l'ensemble d'un SI et la transfère dans un endroit sûr, prête pour relancer toute l'activité de l'entreprise.

Heureusement pour ce type de scénario quelques exclusions sont assez faciles à déterminer :

- les applications peu sensibles,
- celles dont les données évoluent peu ou rarement,
- et les applications sécurisées par une solution de pleine haute-disponibilité. Celles-ci devront cependant se coordonner avec les arrêts éventuels de leurs partenaires pour la création de points stables.

Les limites : l'extension du périmètre géré (et réputé cohérent) se trouve limitée par les contraintes de volumétrie, de débits réseaux, ou – une nouvelle fois – de coordination d'applications trop nombreuses.

Et pour l'heure, le constat reste que la technologie répond très bien aux besoins de cohérence application par application mais ne prend que partiellement en compte les contraintes de cohérence entre applications. De plus, pour atteindre à une réelle cohérence fonctionnelle cette technologie doit être intégrée dès la conception de l'architecture afin d'en tirer le meilleur parti. Cela peut poser des problèmes de compatibilité ou d'évolutions ultérieures.

2.4.e Un mix de ces quatre pistes

Bien évidemment, lorsque le SI est hétérogène avec un fort historique, on va s'inspirer des quatre approches, les panacher pour arriver à LA solution.

3 DÉCLENCHEMENT DU PRA ET GESTION DE CRISE

« Là où il y a danger, croît aussi ce qui sauve »
Hölderlin

3.1 Introduction

Pour importants qu'ils soient, les aspects techniques du PRA n'en constituent qu'une partie. Le jour où survient un accident grave ou un sinistre, il faut décider, et décider vite, de la mise en œuvre – ou pas – des moyens techniques préalablement définis, puis gérer la situation de crise jusqu'à sa résolution. Il s'agit donc bien dans ce chapitre d'envisager l'organisation préalable à mettre en place.

En effet, choisir de déclencher le PRA ne va pas de soi. L'accident n'est peut-être pas si grave. Et même grave, ne saurait-on y remédier plus rapidement, avec une moindre perte de données, qu'en recourant au PRA ?

Dans cette situation, qui donc, prendra la décision de déclencher les opérations de secours ? En s'appuyant sur quels critères pertinents, définis auparavant par qui ? N'oublions pas que dans le monde des plans de reprise informatiques, comme dans celui de l'Assurance, la difficulté consiste toujours à bien prévoir les risques, et à pondérer leur probabilité d'occurrence selon la gravité de leurs éventuels impacts.

Qui sera ensuite chargé de l'application des différentes parties de ce plan, pas seulement au sein du service informatique, mais aussi du côté des métiers et de la direction générale ?

Pour répondre de façon efficace à ces questions le jour du sinistre, un travail en amont s'impose : qualification des process critiques, hiérarchisation des priorités, établissement d'un organigramme clair pour les prises de décision, gestion prévisionnelle des ressources humaines, préparation des communications ... autant de tâches à effectuer avant pour ne pas aggraver les conséquences pendant.

Cet ensemble de garde-fou ne garantit pas que le jour venu tout se déroulera bien, mais il fournit un cadre au sein duquel agir. Or, dans une situation critique, par définition stressante, pouvoir s'appuyer sur des procédures claires et complètes constitue un bon moyen d'atténuer le choc.

3.2 Résumé du chapitre

Ce chapitre porte essentiellement sur des points d'organisation. Un PRA suppose de mettre en place une architecture physique pour la reprise, comme nous l'avons vu, mais aussi une architecture 'humaine' sous la forme d'une organisation et de processus pour traiter au mieux la difficile conduite des opérations en situation de crise.

Nous explorerons ici les différentes composantes de cette organisation, en partant des retours du terrain. Ceux-ci nous montrent que de nombreuses entreprises ont mis au point un processus de gestion de crise structuré pour décider de l'activation des PRA et les conduire à bien.

Ce processus couvre trois domaines essentiels :

1 - Diagnostics, décisions, actions

2 - Organisation

3 - Communication

Il répond ainsi aux questions : qui, quand, quoi, où, comment.

Ce chapitre présente d'abord :

- le principe de l'escalade qui conduit à transformer l'incident en incident majeur, moment à partir duquel se pose la question de déclencher le PRA.
- il donne à voir comment dans l'organisation de crise se structurent les responsabilités, et qui décide du déclenchement du PRA.
- Il couvre la question des critères de déclenchement du PRA par type d'incidents, et celle des outils capables de lier ces incidents à l'activité de l'entreprise.
- Les deux dernières parties portent sur le partage des tâches entre équipes durant la crise, et sur les stratégies de communication à mettre en place.

NB : *Ce chapitre traite de la partie Informatique du PRA et ne couvrira pas les aspects métiers (PCM).*

3.3 La genèse : "Le PRA naquit de l'incident majeur"

La gestion des incidents

La gestion des incidents est un processus critique qui vise à détecter les incidents le plus tôt possible, puis à cibler le support technique approprié pour les résoudre dans les délais les plus brefs.

Les objectifs de la gestion des incidents se résument comment suit :

- Résoudre les causes d'interruptions de service le plus rapidement possible, en réduisant autant que possible leur impact négatif sur l'activité de l'entreprise (des solutions de contournement sont envisageables).
- S'assurer du maintien des niveaux de qualité de service et de disponibilité.
- S'assurer que les correctifs idoines ont été appliqués sur l'ensemble du SI pour éviter la reproduction des incidents connus.
- Disposer d'un «recueil» (Base de données, fiches, procédures) regroupant ces correctifs pour gagner en réactivité si l'incident se reproduit.

Procédure d'incident majeur

La procédure d'incident majeur concerne les incidents critiques qui menacent la capacité à maintenir l'activité ou le fonctionnement efficace de l'entreprise.

Bien que ces incidents continuent de suivre le cycle de vie normal de la gestion d'incidents, la procédure d'incident majeur décrit les niveaux de coordination, d'escalade, de communication et de ressources qu'exigent ces événements de haute priorité et de caractère exceptionnel.

La procédure de gestion de crise vise à fournir un cadre pour la prise en charge de ce type d'incidents.

ITIL et les PRA : Pour plus d'information voir article complémentaire en Annexe.

3.4 La gestion de crise : Une organisation et un processus

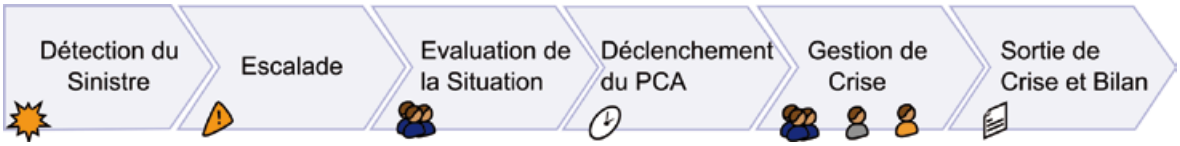


Figure 10 : le processus de gestion de crise

3.4.a Organisation

Pour répondre à l'apparition d'un incident majeur ou critique (sinistre), une Cellule Technique Opérationnelle (CTO), constituée de collaborateurs appartenant à une ou des cellules technique (N2-N3), prend en charge l'établissement du diagnostic et tente de rétablir le service aux utilisateurs au plus vite.

Il arrive cependant que le délai de résolution s'allonge. L'expérience montre en effet que les personnes en charge de l'incident ont souvent une approche optimiste du temps de résolution nécessaire.

Alors se pose la question : à partir de quel moment faut-il basculer vers le PRA en arrêtant ou non la résolution de l'incident ? Qui prend la décision ?
Le niveau de validation dépend de la solution (différent entre un PRA en haute disponibilité versus un PRA à froid) mais en général la CCD (cellule de crise décisionnelle) porte cette responsabilité. Cette dernière prend en charge la coordination, le suivi et la communication durant toute la durée de la crise.

La CCO se compose d'opérationnels métiers, elle a pour fonction de coordonner les opérations, de piloter le CTO, d'organiser les plans d'actions, de collecter et d'analyser les options à soumettre à la CCD, puis de faire exécuter ces décisions. Cette CCO reste mobilisée durant toute la durée de la crise

Il est souhaitable que la CCD soit composé de personnels autorisés à prendre des décisions plus importantes, et valide en dernier recours le déclenchement du PRA et la communication qui s'ensuit.

Selon la criticité du métier, il peut être opportun d'avoir une astreinte managériale par domaine (cadre de permanence).

Un exemple de formalisation de crise :

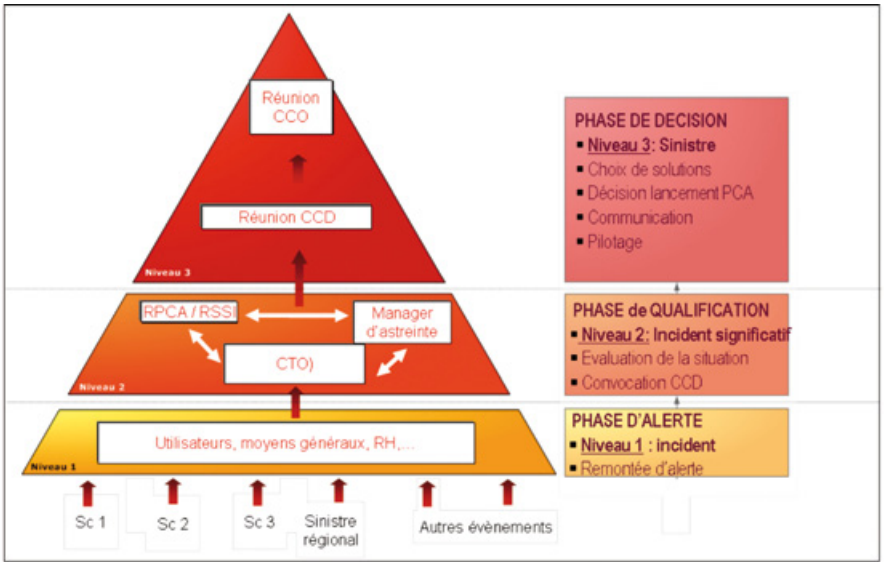


Figure 11 : la pyramide d'escalade

3.4.b Processus

Pour illustrer l'interaction des entités susnommées dans le circuit de prise de décisions, nous vous proposons un schéma simplifié du processus opérationnel :

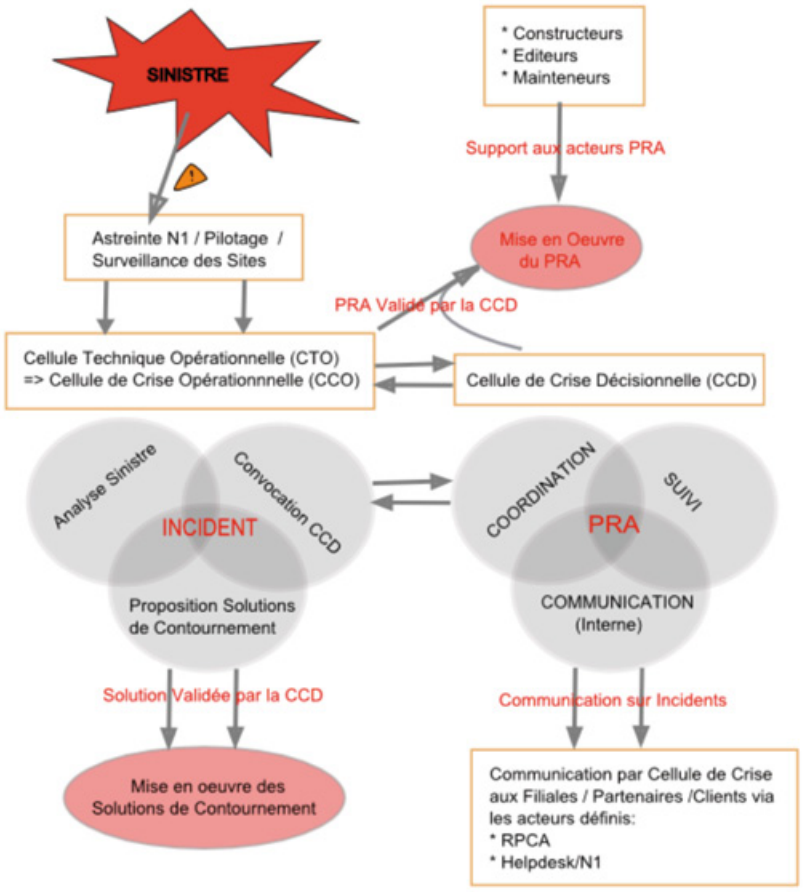


Figure 12 : schéma simplifié du processus opérationnel de gestion de crise

NB : *il n'est pas utile que les différentes cellules soient physiquement présentes (conf call ou autre).*

Il est possible d'avoir des arbres de décisions à disposition de la CCD pour diminuer le délai de prise de décision et justifier l'orientation prise.
L'organisation de ces cellules doit aussi faire l'objet d'exercice. La difficulté étant souvent d'avoir la présence de certains cadres décisionnaires.

3.5 Les critères de déclenchement

Les critères de prise de décision varient en fonction de la nature du PRA (à froid, à chaud, en haute disponibilité) et dépendent généralement de deux facteurs-clé :

- Le respect des objectifs de temps
- La capacité à restaurer le niveau de service convenable

La prise de décision est toujours difficile surtout lorsque le délai nécessaire à la Production pour restaurer le service est mal connu. Vaut-il mieux partir tout de suite sur un PRA, avec des pertes de données et de disponibilité connues et en partie liées à la nature du PRA en place (PDMA) ou temporiser parce qu'un contournement serait éventuellement possible ?

Un PRA en haute-disponibilité, dans lequel les pertes de données approchent de zéro, rend plus simple cette prise de décision qu'un PRA à chaud ou à froid, dans lesquels les impacts en perte de données existent, et sont parfois très lourds. D'ailleurs, dans le cas d'un PRA en haute disponibilité, la prise de décision perd de son importance puisqu'il existe des procédures d'automatisation de la bascule ou d'intervention ponctuelle d'un opérateur selon une procédure prédéterminée.

3.5.a Un objectif de temps

Un PRA doit satisfaire à deux exigences définies par la Maîtrise d'ouvrage (MOA): le délai maximal d'interruption Admissible (DMIA) et la perte de données maximale admissible (PDMA).

En complément de quoi, la maîtrise d'œuvre (MOE) fixe le délai de reprise visé (RTO : Recovery Time Objective) et le point de reprise informatique visé (RPO : Recovery Point Objective).

Attention à bien déterminer quand démarre le chronomètre du DMIA :

- Constat de l'incident par l'utilisateur, ou
- Constat avéré par la CTO, ou
- Décision de la CCD.

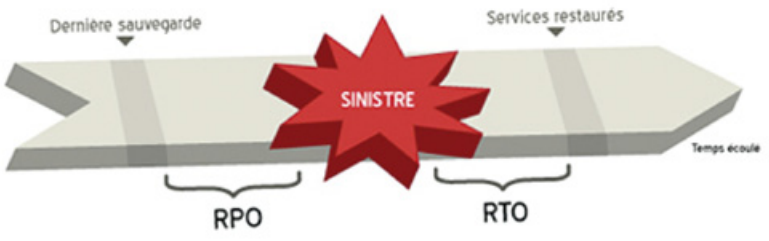


Figure 13 : RPO et RTO

La fin du RTO est décidée par la CCD suite à constat des métiers ayant validé la reprise fonctionnelle des applications.

NB : *Ces paramètres – RTO et RPO – serviront d'éléments de base pour prendre la décision de basculer.*

Il est conseillé de se mettre d'accord avec les métiers sur la durée de prise de décisions.

NB : *Dans les schémas suivant les pavés bleu, orange et jaune de la zone RTO illustrent le différentiel temporel du démarrage RTO selon les règles définies par l'entreprise.*

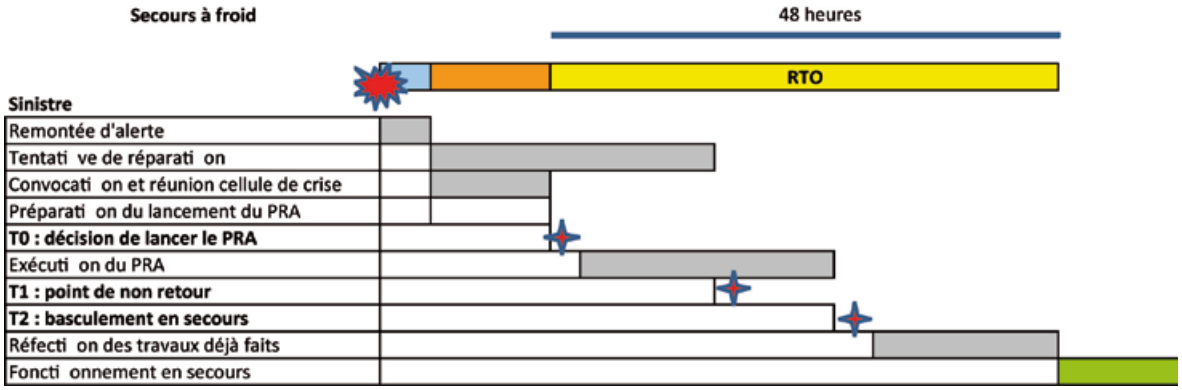


Figure 14 : le RTO par type de secours : secours à froid

NB : *la réfection des travaux déjà faits consiste à appliquer l'ensemble des traitements intervenus entre la dernière sauvegarde de recours utilisée et le moment du sinistre.*

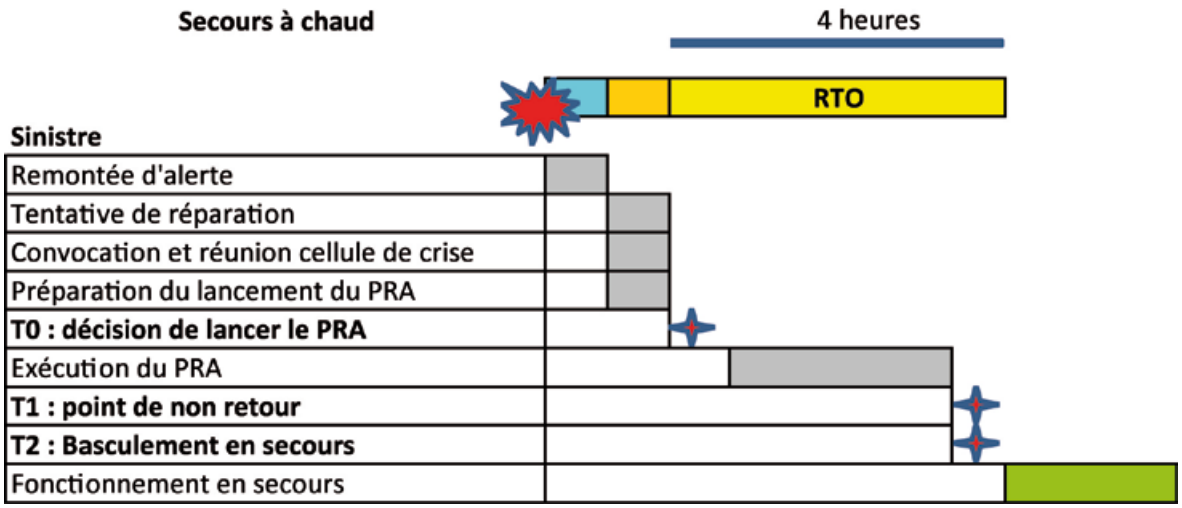


Figure 15 : le RTO par type de secours : secours à chaud

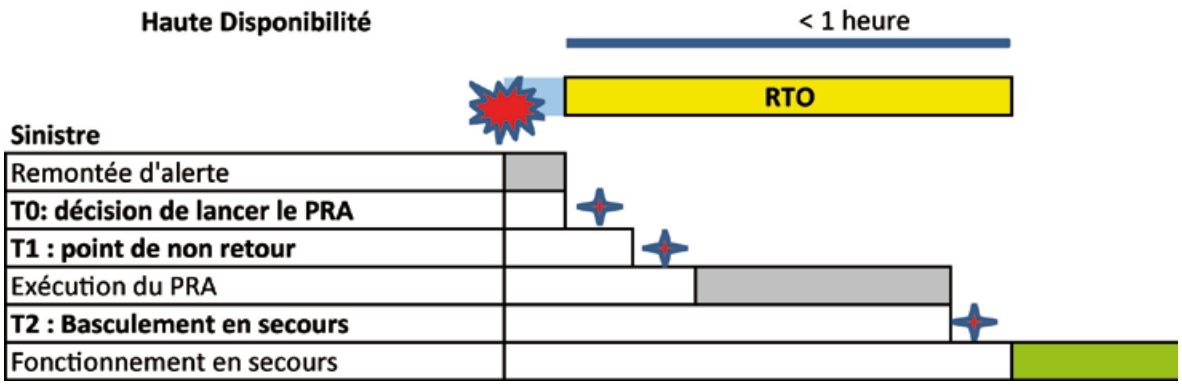


Figure 16 : le RTO par type de secours : secours en haute disponibilité

Le point de non-retour est le point à partir duquel il ne faut plus retourner en arrière (même en cas de retour à la normale sur le site primaire) mais continuer impérativement la bascule engagée. En effet, le risque associé au retour à l'état initial devient progressivement plus important que celui associé à la continuation de la procédure de PRA en cours.

Il faut alors toujours aller vers un état connu, fiable et stable en utilisant le PRA testé.

Exemple de critères et escalade par type de sinistre physique ou logique

Sinistres physiques

Type de sinistre physique	Critères	Escalade
Problème électrique	Si certitude de coupure de l'alimentation électrique supérieure à 12 heures ouvrées	Passage de niveau 1 en niveau 2 : (voir tableau supra) Alerte du responsable d'astreinte
	Coupure électrique généralisée – touchant les salles informatiques quelle que soit la durée estimée de redémarrage.	
Incendie	Si non maîtrise en 5mn d'un incendie proche ou à l'intérieur du bâtiment Informatique	
Dégagement intempestif de CO^2/ gaz inertes	Dans tous les cas	
Dégâts des eaux	Si le matériel d'une salle informatique a été touché	
Intrusion dans le bâtiment	Si intrusion non maîtrisée dans l'enceinte du bâtiment informatique	
Evacuation forcée du personnel	Dans tous les cas	
Vandalisme	Si impact sur le fonctionnement du SI (téléphonie, réseau, serveurs, ...)	
Coupure de l'accès télécoms dans les locaux d'arrivée télécoms	Si durée probable d'interruption supérieure à 4 heures ouvrées	
Climatisation de la salle informatique	Si température supérieure à 25° dans locaux informatiques et si certitude de défaillance de la climatisation supérieure à 4 heures	
Blocage d'accès au bâtiment informatique	Dans tous les cas	

Sinistres logiciels en heures ouvrables

Type d'incident ou panne logicielle	Critères	Réaction
Incident ou panne qualifié de priorité 1) impactant uniquement l'informatique	Si le transactionnel ne peut pas être lancé en consultation ET si certitude d'arrêt supérieur à 4 heures ou si après 2 heures d'analyse/ intervention de la maintenance, le redémarrage en 2 heures n'est pas certain	Passage de niveau 1 en niveau 2 : Alerte du responsable d'astreinte DSI
Obligation d'arrêter les moyens informatiques	Si certitude d'arrêt supérieur à 4 heures	

Sinistres logiciels en heures ouvrables

Type d'incident ou panne logicielle	Critères	Réaction
Incident ou panne qualifié de Priorité 1 (résolution en moins de 4 heures) impactant uniquement l'informatique	S'il n'est pas possible de terminer le plan de production ou Si le transactionnel ne peut pas être lancé en consultation ET si certitude d'arrêt supérieur à 4 heures ou si après 2 heures d'analyse/ intervention de la maintenance, le redémarrage en moins de 2 heures n'est pas certain	Passage de niveau 1 en niveau 2 : Alerte du responsable d'astreinte DSI
Obligation d'arrêter les moyens informatiques	Si certitude d'arrêt supérieur à 4 heures	

NB : *les chiffres en gras correspondent à des paramètres spécifiques qui varient pour chaque entreprise*

3.5.b Un objectif de service

Si l'entreprise est tournée vers la satisfaction client, sa solution de continuité d'activités le sera aussi. Ainsi, l'entreprise recherchera les solutions qui lui assurent de continuer à satisfaire ses engagements pour chacun des risques auxquels elle aura choisi de se préparer.

Pour définir la nature de ces engagements et les spécifier clairement :

- Chaque direction métier doit identifier ses processus métiers, et désigner les plus critiques.
- Chaque direction métier fixera ses propres objectifs opérationnels en cas de sinistre, tels que répondre aux clients moins de 24 heures après l'accident, honorer les commandes avec au plus un jour de retard, etc.
- Les services support (au premier rang desquels ceux attachés aux systèmes d'information) évaluent leurs propres contributions à ces processus métiers, et les objectifs opérationnels en cas de sinistre correspondants.

L'examen détaillé des contrats de service est abordé dans le chapitre 6.

3.6 Des outils pour établir ses priorités

La Matrice BIA (Business Impact Analysis/Analyse d'Impact Métiers)

La matrice d'Analyse d'Impact Métiers est la pierre angulaire sur laquelle bâtir la stratégie associée à un PRA. Elle consiste à identifier les processus, les systèmes, les fonctions, les missions critiques pour l'entreprise.
Cette analyse doit adresser un objectif majeur : minimiser l'impact d'un incident en termes financiers directs ou indirects, éviter la détérioration de l'image de marque de l'entreprise, assurer le respect de ses obligations réglementaires (Solvency, Bâle II), garantir sa pérennité sur les marchés boursiers, assurer le respect de ses obligations contractuelles avec ses clients, limiter la perte de productivité.

Elle s'inscrit dans une démarche qui comporte trois phases :

- Etude de risques (Probabilité / Impact)
- Analyse des Impacts Métiers
- Besoins de reprise

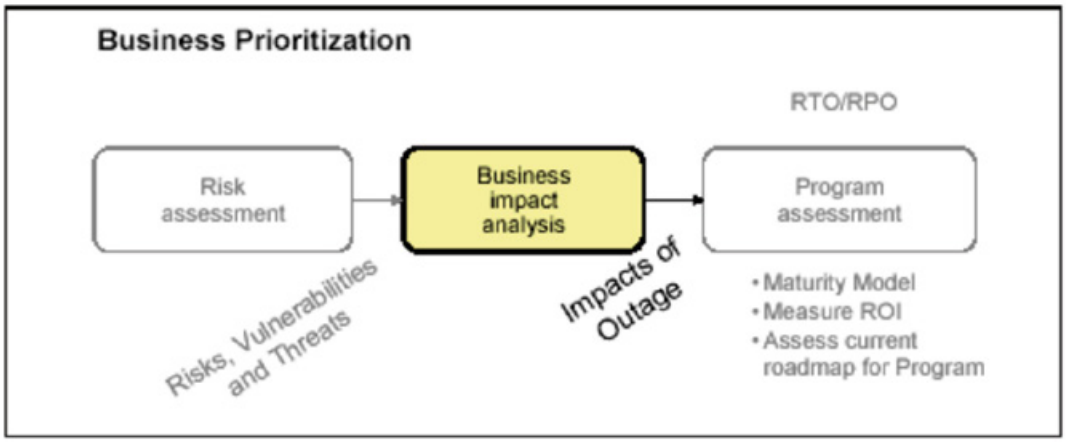


Figure 17 : le BIA

Cette opération se base sur différentes approches mais pourrait idéalement inclure les items suivant :

- un découpage des missions, des fonctions, des process de l'entreprise
- une description des processus, listant les processus entrants et sortants et leurs interactions avec les processus tiers
- une description des temps maximaux d'interruption admissibles (DMIA) avant impact sur le métier avec les objectifs de reprise (RTO) correspondant
- une évaluation des impacts financiers et opérationnels découlant de l'interruption
- une description des ressources techniques et humaines nécessaires pour supporter ces processus
- une description des impacts juridiques possibles
- une description des incidents passés et de leurs impacts

Avant d'atteindre une maturité suffisante dans la description complète de la matrice d'Analyse d'Impact Métiers, une approche plus simple peut suffire ; à condition qu'elle inclue les DMIA souhaités par les métiers et validés par la DG.

La DSI peut proposer aux métiers trois niveaux de reprise d'activités :

- Un niveau « or » correspondant au secours « haute disponibilité »
- Un niveau « argent » correspondant au secours « à chaud »
- Un niveau « bronze » correspondant au secours à froid

Les RTO / RPO correspondants à ces trois solutions sont proposés aux métiers avec leurs coûts associés.



Figure 18 : classification des processus

Il existe d'autres types de matrices, comme la matrice technique d'impacts métiers utilisée plutôt par les opérationnels au sein des DSI :

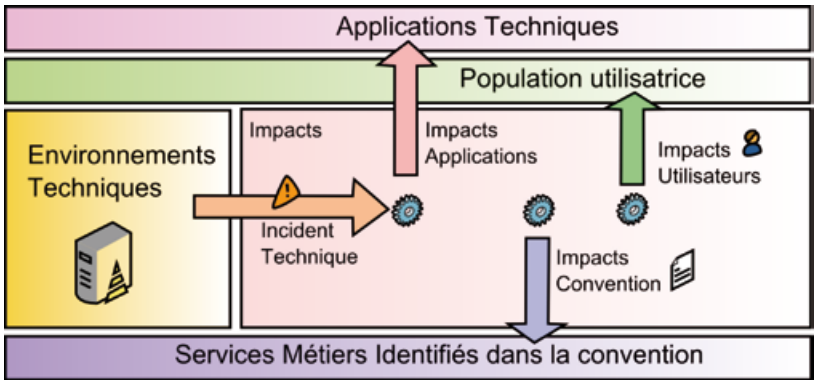


Figure 19 : matrice technique d'impact

Elle permet de mesurer rapidement l'impact d'un incident technique (panne d'un serveur, perte d'un rack, dysfonctionnement d'une baie de stockage, ...) sur une population particulière, sur un applicatif, sur la convention de service.

3.7 Une organisation, des équipes au service du PRA

Le niveau de service demandé dans le cadre du PRA détermine l'organisation de crise retenue. Tout est question d'engagement.

Dans le cadre d'un PRA à froid, l'impact de la décision de déclenchement est fort (arrêt de processus, perte de données, ...). Cependant, le délai de reconstruction étant de l'ordre de plusieurs jours, on dispose d'assez de temps pour consacrer plusieurs heures à la prise de décision, et donc le temps de consulter divers experts.

Dans le cadre d'un PRA à chaud, la prise de décision s'effectue dans un délai de 30 minutes pour une durée maximum d'interruption de 4 heures. Raison pour laquelle les organisations qui disposent de ce type de PRA établissent généralement des astreintes 24 h/24 et 7 j/7 ; astreintes opérationnelles, mais aussi décisionnelles appelées « Permanences managériales ».

A noter : Pour bien décider, il faut disposer des éléments d'appréciation adéquats. Les outils de supervision, de pilotage, ... jouent un rôle essentiel dans l'alimentation en informations de cette chaine de décision, et ce avant toute analyse humaine plus poussée.

Pour les entreprises qui disposent de PRA en haute disponibilité, la prise de décision est souvent réduite voire automatique. Cette situation résulte du faible impact du basculement en haute disponibilité en termes de DMIA et de PDMA.

NB : *Dans le cas des bascules automatiques, il faudra s'assurer de disposer d'indicateurs d'états en conséquence (alarme sur bascule).*

La bonne organisation à mettre en place pour le déclenchement d'un PRA peut se composer de :

- Une équipe en charge du PRA qui travaille avec les équipes de production présentes sur site au moment de la survenue du sinistre.
- Des astreintes au niveau décisionnel comme opérationnel.
- Un accord avec la DRH concernant les conditions de travail en situation de crise : heures supplémentaires, dérogation à la durée légale quotidienne de travail, travail le dimanche ou la nuit (voir livre CCA).

Ce qui nous emmène à rappeler que ce sujet devrait être couvert dans le cadre du volet Ressources Humaines du PCA/PRA selon 3 axes :

- Faire connaître : établir un dispositif et des démarches RH spécifiques s'appliquant en cas d'incident majeur impactant l'entreprise.
- Savoir Faire : formation et organisation des équipes exploitant le SI en heures non-ouvrables.
- Faire Adhérer : définir les règles du jeu applicables dans le cadre d'une situation exceptionnelle (astreintes, rémunération, compensations).

Il s'agit de trouver un équilibre entre la stratégie de continuité, les besoins métiers et les ressources disponibles dans la situation de crise.

3.8 Communication Ciblée de crise

Pour éviter qu'une communication défectueuse ne laisse le client interne ou externe dans un flou potentiellement ravageur il faut anticiper en ayant établi à l'avance des règles de communication interne et externe.
La communication dans ce type de situation s'avère primordiale : pour éviter le sentiment de ne pas être tenu au courant, éviter les spéculations, dégonfler les rumeurs, il est nécessaire de communiquer fréquemment, régulièrement et clairement.

NB : *Un devoir de réserve doit être systématiquement rappelé aux collaborateurs.*

Communication Interne

Il est nécessaire d'avoir prévu à l'avance une communication interne destinée à l'ensemble des employés de l'entreprise, qu'ils soient directement impliqués ou non. Les informations à communiquer sont validées par la CCD.

Ces informations sont transmises par le DRH ou ses délégués. Les moyens à utiliser : messagerie, intranet, alertes SMS, courriers, cascades téléphoniques. Certaines entreprises disposent aussi d'un site internet de crise (Accès sécurisé) hébergé chez un tiers.

Pour pallier une défaillance de la messagerie interne, il peut être nécessaire de disposer d'une messagerie de crise externe.

Les SMS sont à privilégier.

Les messages d'alertes comportent usuellement les éléments suivants :

Historique Incident :
Niveau de criticité: Fort/Moyen/Faible
Niveau de vigilance (attaque sécurité) :
Site Impacté :
Impact Métiers :
Impact Utilisateur:
Cartographie de l'impact:
Processus Incident Déclenché :
Heure du déclenchement :
Délai de rétablissement estimé :
Fréquence de communication :

Communication avec les partenaires et externes (médias, ...)

L'exercice de communication reste délicat car souvent lié à des aspects contractuels de fourniture de service. Il faut en général accepter en toute transparence (et toute confiance) d'alerter sur la nature de l'incident (sa gravité, ses impacts, ...), tout en rassurant le partenaire sur un événement qu'il ne peut évaluer et qui touche son activité.

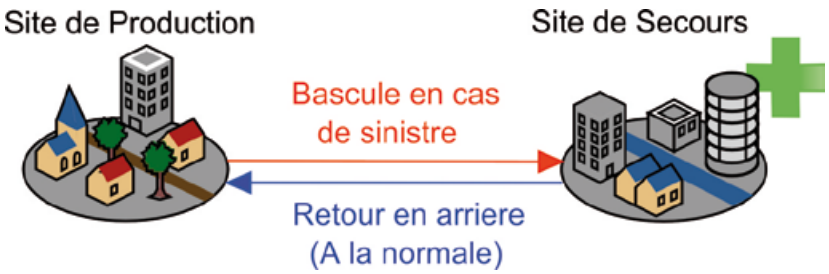
L'élément clé des échanges reste le suivi des opérations en conformité avec le délai de reprise estimé et négocié.

Ce volet, souvent sensible, ressort de la responsabilité d'une cellule de communication entreprise dédiée sous la responsabilité de la CCD.

A retenir pour une communication efficace :

- Alerter sans alarmer
- Communiquer régulièrement
- Informer de façon claire et transparente

3.9 Retour à une situation normale



Une fois le PRA activé et la bascule vers les moyens de secours effectuée, il reste à parcourir l'autre moitié du chemin, souvent la plus délicate, car la moins testée.

La décision de revenir à une situation normale est prise par la CCD sur avis de la CCO.

Le retour arrière n'est pas toujours décrit dans le PRA car il dépend de la nature du sinistre :

- Retour envisageable sur le site de production après quelques jours ou quelques semaines, par exemple à l'issue du temps de réhabilitation du site suite à un dégât des eaux. On considère généralement qu'il est acceptable de ne plus disposer de PRA pendant cette phase. Mais il faut alors muscler les sécurités et veiller particulièrement à la mise hors-site des sauvegardes.

- Retour impossible sur le site de production, par exemple destruction totale du site dans un incendie. Il est alors nécessaire de revoir l'implantation des applications sur d'autres datacenters existants (réserve d'espace) et ceci dans un délai raisonnable afin de restaurer le niveau de service en cas de nouveau sinistre majeur.

Avant de retourner en situation normale, il faut s'assurer d'avoir un système de sauvegarde externalisée.

Nous avons vu que dans un PRA les ruptures de disponibilité et les pertes de données dépendent du niveau de service choisi : à froid, à chaud, en haute-disponibilité. Cependant, le retour en arrière étant une opération programmée, et non pas provoquée par un incident, on essaiera d'en réduire les effets au maximum, en se fixant une durée d'interruption minimale et connue, et une perte de données nulle.

Comme pour la bascule en PRA, le retour en production normale doit aussi faire l'objet de tests.

3.10 Quelques leçons à tirer

La principale difficulté en situation de crise consiste souvent à conserver les bons réflexes :

1) suivre les procédures définies,
2) canaliser les énergies : éviter les nouvelles idées intempestives, se méfier du stress, vérifier que les équipes se reposent, ...
3) séparer clairement les opérationnels des décisionnaires : avoir un relais entre les deux,
4) effectuer des points d'avancement réguliers (suivre une main-courante),
5) communiquer, communiquer et communiquer, différemment selon les cibles et clairement.

Maturité des membres du CRiP

Exploitation du questionnaire

Qui prend la décision de basculer en PRA ?

CCD : 67%
DSI : 22%
DG : 11%

En Synthèse: le manque de formalisation est souvent mise en avant : tant au niveau des processus, de la communication que sur l'organisation RH.

Disposez-vous d'un diagramme d'escalade clairement établi et diffusé ?

OUI : 62%
NON : 38%

Quelle matrice d'aide à la décision utilisez-vous ?

Critères définis dans le PCA : 25%
Convention de service : 35%
Décision métier : 40%

Disposez-vous d'une communication préétablie :

Oui : 60% (communication interne)
Non : 40%

Dans le cas d'un déclenchement de PRA de nuit avec rappel de salariés : quelle organisation, quel aménagement RH, ... avez-vous mis en place ?

Dispositif exceptionnel prévu par les RH : 50%
Régulation post-incident : 50%

4 VALIDATION PROBANTE DU PRA

« Les tuiles qui protègent de la pluie
ont toutes été posées par beau temps »
Proverbe chinois

4.1 Introduction

Lorsqu'un sinistre se produit, la cellule de crise décisionnelle se pose toujours la même question : le PRA est-il opérationnel ? Assurera-t-il la reprise de l'activité dans le délai prévu ?

Les tests et exercices constituent le seul moyen d'apporter une réponse crédible à ces questions. On peut même affirmer qu'un PRA non testé régulièrement est un PRA qui n'existe pas. Dans cette logique, quelle suite de tests et d'exercices probants faut-il définir et réaliser afin d'acquérir la quasi-certitude qu'au moment voulu le PRA fonctionnera ?

4.2 Résumé du chapitre

Après avoir défini tests et exercices, ainsi que leurs buts respectifs, ce chapitre dégage un certain nombre de critères pour qualifier une validation probante. Ces critères sont indépendants du type de secours (à froid, à chaud ou en haute disponibilité).

4.3 Définitions

Test et exercice (définitions issues du Livre Blanc du Club de la Continuité d'Activité : Lexique structuré de la continuité d'activité) :

Il est nécessaire de faire une distinction entre test et exercice :

- **Le test** est destiné à apprécier la validité d'une modification (innovation, mise à niveau, correction, ...) et produit un résultat binaire (réussi ou non réussi). Le test a un caractère exploratoire qui peut conduire à un échec.

- **L'exercice constitue un entrainement**, et correspond à l'entretien d'un savoir-faire, à la répétition d'une mise en situation matérialisée par un scénario de sinistre. Il sert à maintenir le niveau de compétence de l'ensemble des participants, et à préparer les utilisateurs finaux.

Type d'exercice

L'organisation d'un test ou exercice résulte souvent d'un compromis entre le risque pris lors de sa réalisation et le caractère probant que l'on en attend. En conséquence, une grande majorité des tests présentent un périmètre plus réduit que celui d'une crise réelle, par exemple ils ne débutent pas de façon inopinée, mais sont préparés à l'avance et planifiés.
Pour les plans de secours à froid et à chaud (comme nous le verrons plus bas, la haute-disponibilité constitue un exemple à part), l'exercice sera simulé ou réel, préparé ou impromptu. Un plan de validation complet du PRA doit prendre en compte ces quatre types d'exercices.

Les exercices de type préparés et simulés sont évidemment les premiers à pratiquer de par leur faible caractère perturbateur.

	Exercice simulé	Exercice réel
Préparé	La date de l'exercice est connue de tous les participants. Il n'y a pas d'arrêt de la production.	La date de l'exercice est connue de tous les participants. La production est arrêtée, le secours prend le relais (Périmètre en fonction des décideurs).
Inopiné	La date de l'exercice est inconnue de tous les participants. Le fonctionnement en mode secours est validé, mais il n'y a pas d'arrêt de la production.	La date de l'exercice est inconnue de tous les participants. La production est arrêtée, le secours prend le relais (Périmètre en fonction des décideurs).

Les exercices de type préparés et réels vérifient que le fonctionnement sur le site de secours s'effectue dans des conditions acceptables.

Les exercices de type simulés et inopinés vérifient la réactivité des participants dans des conditions proches des conditions réelles, mais sans faire courir de risque au bon fonctionnement de la production.

Exercice hors-production et exercice en production

Le risque lié à l'exécution d'un exercice hors-production ou en production diffère évidement, mais ces deux types de simulations ne relèvent pas du même niveau d'exigence.

- Les exercices hors–production offrent plus de souplesse dans les tests et l'entrainement des populations concernées. Ils contribuent à rendre les gens moins frileux à l'idée de faire le grand saut de l'exercice en production. Cependant ils ne préparent pas avec le maximum d'efficacité les équipes à réagir à une situation de crise réelle.

- Les exercices en production : sont idéaux (de par leur nature) car effectués en situation réelle. Ils nécessitent cependant une préparation plus délicate : bascule en heures non-ouvrables (le soir, la nuit ou le week-end), et un retour-arrière vers la production normale sans perte de données.

***NB** : Le passage d'un mode d'exercice à l'autre dépend de la maturité du PRA, du niveau de compétence atteint par les équipes, de la confiance dans les processus mis en place, mais aussi de la volonté de répondre à des contraintes opérationnelles fortes.*

On note ainsi que certaines entreprises du CRiP, par exemple celles qui se trouvent fortement soumises à des régulations bancaires, ou encore des services publics, exécutent souvent des exercices de PRA en conditions réelles. La durée de l'exercice varie alors selon le mode de bascule (ex : bascule technique le week-end et fonctionnement réel en mode PRA durant la semaine ; bascule en HD ; ...).

Dans ce cas, la réalisation et la validation de l'ensemble des cahiers de tests techniques et fonctionnels sur le site de secours constituent un préalable au GO/NOGO pour l'exécution du test du PRA en production. L'activité métier peut ensuite s'exécuter dans ce nouvel environnement devenu similaire à l'environnement de production.

La phase de retour arrière, pour revenir sur le site de production primaire, est toujours critique car elle oblige à respecter deux étapes préliminaires :

1° qualifier les données enregistrées sur le site de secours pour s'assurer de la cohérence entre les deux sites.

2° resynchroniser les données sans perte pour les métiers (mise à jour des données commerciales, des annuaires, des messageries, ...).

Fréquence annuelle des exercices

Il n'existe pas de règles établies, cependant, comme le dit bien la formule : si rien n'est obligatoire, il est fortement conseillé de ... Les retours d'expériences du CRiP montrent qu'un PRA à froid nécessite au minimum un exercice par an. Quand au secours à chaud, il impliquerait idéalement deux exercices par an.

La haute disponibilité demanderait des tests plus fréquents (selon les organisations, les montées de version applicatives permettent aussi de tester la bascule). Il est envisageable de fonctionner 50% du temps sur chaque environnement (moins pairs et impairs par ex).

Durée des exercices

Les exercices se déroulent généralement sur une durée courte, de l'ordre d'une journée à une semaine.

Il est souhaitable de tester les PRA sur plus une période plus longue. En effet, certains incidents ne se produiront qu'au-delà des premières 24 heures. Un exemple : sur le site de secours, ont été installées des licences logicielles provisoires, uniquement pour faire des tests. Suite à la bascule sur le site de secours, et en l'absence de régularisation rapide de ces licences, les applications cessent de fonctionner au bout de quelques jours.

Selon Gartner, 60 % des entreprises ne prévoient pas de plan de continuité d'activités au-delà de sept jours (Janvier 2008. Source : 359 professionnels de la gestion des risques et de la sécurité informatique aux Etats-Unis, en Grande Bretagne, et au Canada.)

4.4 Quelques critères pour qualifier un exercice probant

Remarque

- Probant : en français, fait référence à une preuve. L'anglais ne possède pas d'équivalent. On parle dans cette langue de confiance et d'acquisition d'assurance.

- Les éléments de validation et de qualification de l'exercice doivent impérativement être mis par écrit avant le début de l'exercice, ce qui permettra que la validation s'effectue selon des critères connus. Les métiers doivent valider ces critères avant l'exercice.

Pour évaluer la valeur probante des exercices de PRA nous proposons une liste non exhaustive de critères éligibles. Ces critères visent un double but : parfaire le PRA suite à un exercice ; évaluer la maturité du PRA avant son déclenchement.

1. Le périmètre du PRA s'est-il avéré adéquat aux besoins négociés avec les métiers à partir de leurs exigences : applications secourues, processus de gestion de crise, nombre de personnes impliquées ?

2. Le scénario de sinistre pris en compte était-il réaliste et validé par la direction des risques ou son équivalent ?

3. Les conditions de reprise d'activités observées (RTO, RPO) ont-elles été conformes aux conditions attendues par les métiers (DMIA, PMDT) ?

4. L'entrainement des décideurs et des opérationnels :
   - L'implication des responsables (et de leurs remplaçants) pour décider du déclenchement a-t-elle été satisfaisante ?
   - L'implication des hommes clés opérationnels a-t-elle été satisfaisante ?
   - Les hommes clés opérationnels sont-ils en nombre suffisant pour assurer le bon déroulement du PRA à tout moment ?

5. Les dernières mises à jour du PRA ont-elles été testées ?

6. Les exercices ont-ils été rejoués par une autre équipe ? En effet, les procédures écrites doivent toutes être ré-exécutables par des personnes ne les ayant pas écrites.

7. Les conditions de stress des participants étaient-elles suffisantes ?

8. Les exercices ont-ils révélé des erreurs ? Dans le cas contraire, on se demandera si l'observation a été suffisamment fine. Ou on considérera avoir réussi un exercice probant. Ces erreurs doivent être diagnostiquées, faire l'objet d'un plan d'actions correctives, et ce plan doit faire lui-même l'objet d'un rapport d'exécution.

9. Les conditions d'arrêt simulant le sinistre comportaient-elles assez d'éléments aléatoires pour éviter que l'exercice ne se déroule dans des conditions trop 'propres' et donc peu réalistes ? Pourra-t-on éventuellement reprendre l'activité avec une perte de données ?

10. Des exercices inopinés avec une préparation limitée ont-ils été réalisés ?

11. Le test/exercice a-t-il été contrôlé par des observateurs internes ou externes indépendants ?

12. La durée de l'exercice a-t-elle été suffisante pour caractériser un scénario de sinistre réaliste ? Un jour ne suffit peut être pas ?

NB : *Ces critères ne sont pas des conditions nécessaires et suffisantes pour qualifier de probant un exercice. Pour ce faire, il doit atteindre les objectifs préalablement établis par une entité de l'entreprise (Risques, Métiers…) différente de la DSI. Il doit aussi faire l'objet d'un compte rendu validé et signé par les parties prenantes.*

Rappel : *Les correctifs apportés suite aux incidents doivent faire l'objet d'un procès-verbal de mise en place annexés au compte rendu.*

NB : *le risque pris lors de la réalisation d'un exercice de PRA ne doit pas être supérieur au risque que l'on cherche à couvrir !*

Cependant, l'exercice inopiné est celui qui se rapproche le plus des conditions réelles, et par conséquent le plus probant.

4.5 Écueils et bonnes pratiques

Quelques leçons à tirer :

- De l'importance des procédures : bien écrites, bien à jour, bien testées, bien contrôlées. Ce qui n'est pas écrit n'existe pas ! Ce qui n'est pas à jour ne sert à rien !
- De l'importance du pilotage : coordonner les actions, consolider les informations, démarches primordiales afin d'éviter les initiatives individuelles intempestives et pour permettre que les arbitrages nécessaires soient rendus conformément aux procédures.

Quelques écueils à éviter :

- Éviter les bruits de fond : pas de correctifs juste avant l'exercice réel, partir d'une situation stabilisée.

- Le Maintien en Condition Opérationnelle est un travail permanent, il ne s'effectue pas uniquement les jours d'exercice (des tests techniques préalables doivent être effectués pour assurer la réussite de l'exercice).

- Veiller à ne pas fatiguer excessivement les équipes, prévoir des remplaçants.

Maturité des membres du CRiP

Exploitation du questionnaire

Le SI est-il testé partiellement ou totalement au cours de vos exercices ?

Production complète :	53 %
Production partielle :	47 %

Quel est le périmètre des tests ?

Par brique d'infrastructure :	50 %
Par applicatifs métiers :	50 %

Ce qui a été testé est-il reproductible par d'autres personnes ?

Oui :	60 %
Non :	20 %
Ne sait pas :	20 %

Les tests / exercices sont-ils contrôlés par des observateurs internes ou externes indépendants ?

Oui :	80 %
Non :	20 %

Les conditions de reprise d'activités (RTO, RPO) sont-elles mesurées ?

RTO mesuré :	48 %
RPO mesuré	26 %
Ne sait pas :	26 %

Faites-vous des exercices inopinés ou seulement à un moment propice ?

Moment propice :	80 %
Inopiné :	16 %

Quel est le niveau de préparation des tests ?

Préparé :	79 %
Inopiné :	16 %
Ne sait pas :	5 %

Raisons pour lesquelles il n'y a pas de tests inopinés ?

Manque maturité :	21 %
Trop lourd :	21 %
Impératif de production :	14 %
Veto de la Direction Générale :	7 %
Pas de tests suffisant :	7 %
Test de gestion de crise inopiné uniquement :	7 %
Pas de demande :	7 %
Ne sait pas :	7 %

5 MAINTIEN EN CONDITION OPÉRATIONNELLE DU PRA

« Ce qui n'est pas écrit n'existe pas !
Ce qui n'est pas à jour ne sert à rien ! »
Confucius

5.1 Introduction

Si l'exercice de PRA permet de valider les procédures, les process, et les types d'architectures techniques de reprise, la plus grande difficulté dans le temps reste de maintenir le PRA à jour !

Deux solutions complémentaires pour garantir ce bon entretien : la fréquence élevée des exercices (voir statistiques dans les chapitres précédents) et le maintien continuel en condition opérationnelle (MCO).

Tous les opérationnels partagent une même préconisation : il faut traiter le Maintien en Condition Opérationnelle des PRA à la même fréquence que les livraisons en production. Une contrainte de plus diront certains ... mais la gestion du risque (encore une fois) est mère de sureté

Selon les types de PRA, la méthode change.

5.2 Résumé du chapitre

Nous considérerons d'abord ici les bonnes pratiques générales du Maintien en Condition Opérationnelle, en insistant particulièrement sur la dimension dynamique qui doit caractériser cette opération. Nous déclinerons ensuite les spécificités propres au MCO des trois architectures de PRA de référence que nous avons déjà définies. Nous rappelons ensuite que ce MCO participe à la gouvernance globale du SI, et que s'il existe des bonnes pratiques, il existe aussi des écueils.

5.3 Principes du MCO

Le PRA ne doit pas rester figé dans le temps. Il suit et prend en compte tous les changements qui concernent le SI : les patchs, les livraisons applicatives, les évolutions de l'infrastructure, les changements de personnes et de fonctions dans l'entreprise, les évolutions des conditions de reprise d'activités ... Toute évolution dans l'entreprise sera l'occasion de se demander comment doit évoluer le PRA pour s'y adapter.

L'étape préalable consiste à définir le contenu du Maintien en Condition Opérationnelle du PRA et les moyens de contrôler sa bonne exécution :

- Mise à jour des applications et des flux d'échanges associés.
- Tenue à jour des procédures de gestion de crise majeure.

- Tenue à jour des procédures techniques : de restauration, de synchronisation des données et de bascule des échanges.

- Maintien des compétences nécessaires à la bonne conduite du PRA : acteurs des cellules de crise, personnels soumis aux astreintes opérationnelles, personnels soumis aux astreintes de la maîtrise d'ouvrage.

- Déterminer les types de changements à gérer et la méthode applicable à chaque type de changement: évolution des équipements et des OS, des échanges, ...

- Inclure les corrections des erreurs mises en évidence au cours des exercices précédents.

Le Maintien en Condition Opérationnelle du PRA doit être traité de la même façon que celui de la Production. Ainsi toute analyse d'impacts en production (voir cellule de mise en production du type CAB - Change Advisory Board - ou autre) suite à modifications (livraisons, incidents, ...) devra prendre en compte le PRA. On devra s'assurer du déploiement à l'identique des modifications et évolutions sur tous les sites informatiques hébergeant le PRA, internes comme externes, pour maintenir la cohérence des architectures.

Lors de nouveaux déploiements, la question du test unitaire de compatibilité entre sites reste à définir : test technique unitaire ou test de plus grande ampleur impliquant les métiers (exercices).

Une attention particulière sera portée aux environnements multipartenaires de par les dépendances et incidences qu'ils induisent dans le PRA.

Il faut bien garder à l'esprit que toute période de transition, toute modification ou évolution non-encore propagée globalement, met le PRA en état d'instabilité. Durant une phase de modification, il existe, selon la stratégie employée (mise à jour synchrone /asynchrone), le besoin de définir un délai de validation. Durant ce délai, toute bascule en PRA devient critique, car l'état du site secondaire génèrera des incidents corrigés par le MCO sur le site primaire.

Pendant cette période d'instabilité :
- tout exercice durant la période d'instabilité est à proscrire.
- si un sinistre a lieu, il faut mettre à niveau le second site avant toute autre opération.

La CTO/CCO devra impérativement fournir à la CCD un état du site de bascule avant déclenchement du PRA.

La suite du chapitre décrit le Maintien en Condition Opérationnelle par type de solution de secours.

5.4 MCO d'un PRA à froid

Dans une architecture de type PRA à froid, le secours se trouve généralement isolée du réseau de production. Il n'est pas nécessaire dans ce cas d'appliquer les changements intervenus sur l'environnement de production de manière synchrone sur l'environnement de PRA. Une erreur dans la gestion des changements n'impacte pas la Production.

Dans cette situation, il est souvent admis d'écraser ce qui était installé sur le site de secours selon deux stratégies majeures et complémentaires :

- Vision image (ghost, RDP, PVS, NIM, ...)

- Vision applicative (sauvegarde complète applicative,...).

La question clé reste de s'assurer de la disponibilité technique et opérationnelle de l'infrastructure du site distant, par exemple par une surveillance minimale des serveurs, clusters, dispositifs de stockage présents sur ce site.

Une des difficultés du modèle du PRA à froid consiste à maintenir sur le site de secours un volant de ressources disponibles ou mobilisables compatibles en termes de plateforme et de capacités (RAM, CPU, stockage) avec les exigences de la production. A défaut, il faut prévoir des procédures de commandes accélérées d'équipements avec les fournisseurs (Attention au délai d'approvisionnement).

Ces ressources de secours peuvent être chez un prestataire spécialisé (site mutualisé). Mise à disposition, maintien à niveau, périodes de tests, sont alors définies par contrat.

Si l'on dispose de deux sites, une répartition judicieuse entre ressources de production et "autres" (développement, intégration, etc..) peut également satisfaire les besoins de secours, avec des ressources connues, mises à jour, mobilisables et surtout non dormantes, ce qui diminue d'autant le coût d'infrastructure du secours à froid.

Dans tous les cas cela suppose de disposer d'une cartographie complète et à jour des ressources, y compris des ressources dormantes.

5.5 MCO d'un PRA à chaud

Un PRA à chaud fonctionne généralement avec des machines installées sur le même réseau que celui de la production.

En général les deux environnements (production et secours) sont parfaitement symétriques d'un point de vue machines et données (réplication). En revanche, il faut se poser la question de la continuité des sauvegardes : après la reprise en PRA, combien de temps l'application peut-elle se passer de sauvegarde ? Faut-il reprendre aussi le catalogue des sauvegardes ou redémarrer à zéro après la reprise ? Quel est le niveau de sécurité de l'infrastructure de sauvegarde/restauration après bascule sur l'environnement de secours ?

Pour conserver le niveau de service du PRA, il est nécessaire de synchroniser les poses de versions applicatives entre les deux environnements (délai de pose inférieur à 4 heures).

Pour cela il faut s'assurer que lors de la réplication des données, les environnements soient totalement compatibles (ex. structures de bases de données).

Il arrive que l'on fasse les montées de version d'abord sur l'environnement de PRA, puis qu'on bascule les utilisateurs nominaux sur les applications de cet environnement afin d'effectuer ensuite les mises à jour sur l'environnement de production. L'architecture doit alors prévoir des mécanismes qui garantissent une perte de données nulle.

Avantage : *le PRA est testé régulièrement. Le temps d'indisponibilité pour les utilisateurs est faible.*

Le MCO d'un PRA à chaud requiert une gestion des changements plus rigoureuse que celle d'un PRA à froid. Il faudra s'assurer par tests unitaires de la bonne installation des évolutions sur le site secondaire. Attention aux écarts non testés !

5.6 MCO d'un PRA en haute Disponibilité

Plus simple ou moins simple ? Un système en haute disponibilité facilite la vie des utilisateurs ; et celle des administrateurs ?

Le Maintien en Condition Opérationnelle se montre souvent plus sensible dans ce cas que dans les deux précédents, car il n'est jamais conseillé d'avoir des versions de composants (firmware, correctifs, applications, ...) différentes concourant à un service en haute disponibilité !

Selon les architectures ce type de solution serait même plus sensible aux corruptions de données.

Si le MCO est facilité pour les poses de versions applicatives, certaines opérations nécessitent toutefois l'arrêt complet du système (exemple : changement de version de base Oracle, d'hyperviseur, et autres composants critiques).

Normalement ce processus n'implique aucune interruption pour les métiers, mais l'expérience montre qu'il est parfois nécessaire de stopper les deux sites pour effectuer la mise à jour de certains composants.

NB : *il faut s'assurer que les constructeurs offrent des solutions de mise à niveau rétro-compatibles.*

5.7 Enjeux et gouvernance

Plus on peut prouver que son PRA est à jour, plus on peut prouver la fréquence et la réussite de ses exercices, et plus il est simple de basculer.

La crédibilité du process opérationnel du PRA constitue un facteur de qualité recherché par les auditeurs. Pour preuve : une question revient souvent lors d'une gestion de crise suite à sinistre : « quelle est la maturité opérationnelle du PRA que nous allons déclencher ? »

La rotation infinie (et maitrisé) du PDCA (Plan-Do-Check-Act) est bien connu de tous et doit rester un élément de solution à ce MCO.

Alors quelle organisation pour assurer ce processus ?

Acteurs :
Le MCO du PRA est de même nature que le MCO de la production, il devrait donc être assuré par les mêmes équipes.

Pilotage :
Chaque entreprise possède ses propres structures de pilotage mais au travers de notre questionnaire nous observons qu'elles restent la plupart du temps noyées dans la Production.

Le MCO est l'affaire de tous ! Cependant le pilotage du Maintien en Condition Opérationnelle du PRA est indispensable.

Le pilotage du MCO du PRA est confié au responsable du plan de reprise d'activités. Il coordonne l'ensemble des acteurs intervenant sur le MCO : exploitants, responsables d'applications, responsable métiers, gestionnaires de risques. Il contrôle le travail de ces acteurs et valide le caractère opérationnel de cette maintenance par des tests et des exercices.

Un comité de maintien en condition opérationnelle statue sur les budgets à mettre en œuvre pour assurer la mise à niveau du PRA lors de la prise en compte de nouveaux risques ou lors de modifications des conditions de reprise demandées par les métiers.

NB : *Suite aux exercices, il est souhaitable de qualifier le caractère opérationnel du PRA d'un domaine applicatif ou d'une application.*

5.8 Écueils et bonnes pratiques

Ecueils :

- Penser que le Maintien en Condition Opérationnelle du PRA sera effectué lors de la période préparatoire de l'exercice, ou pire : durant l'exercice.

Bonnes pratiques :

- Le Maintien en Condition Opérationnelle est l'affaire de tous.
- Tout changement en production doit faire l'objet d'une analyse d'impact sur le PRA (Voir Process de gestion des Changements et son CAB).
- Une réorganisation, si minime soit-elle, peut impacter de façon critique le Maintien en Condition Opérationnelle du PRA : penser à revoir les process.
- Avoir une politique 'antistatique' ;-) (pas d'adresses IP en dur, des points de reprise dans les jobs, éviter d'être dépendant d'un seul opérateur sur une quelconque configuration,...).
- Le Maintien en Condition Opérationnelle doit être contraint par l'existence de points de validation au même titre que toutes les modifications en production.
- Ne pas oublier la mise à jour des habilitations, des certificats, des licences.
- S'assurer que les procédures techniques sont bien partagées et connues des nouveaux entrants (faire la chasse aux bouts de ficelle nés de l'habitude et qui disparaissent avec le départ des personnes).
- Faire un exercice en grandeur réelle pour prouver que l'activité métiers fonctionne sur l'environnement de PRA.

En conclusion : *tout est interconnecté et interdépendant avec le PRA.*

Maturité des membres du CRiP

Exploitation du questionnaire

1- Quelle organisation pour le MCO ?

Qui a la responsabilité du MCO du PRA ?

DSI :	35 %
RPRA :	35 %
Autres :	17 %
Ne sait pas :	13 %

Quelle est l'organisation des équipes responsables du PRA ?

Equipe dédiée PRA :	48 %
Noyé à la Production :	35 %
Autres :	17 %

Quels outils sont utilisés pour le MCO du PRA ?

Intranet Documentaire:	30 %
Excel/Word :	17 %
Progiciel :	17 %
Microsoft Project :	9 %

2- Comment le MCO est-il géré ?

Quel est le Périmètre du MCO ?

Production vitale :	61 %
Production totale :	26 %
Autres :	13 %

Quel est le délai de mise à jour du site de secours :

Immédiat :	30 %
Dépend du service :	22 %
Dépend de la disponibilité :	9 %

Comment est effectué le contrôle des mises à jour et de la cohérence ?

Humain :	43 %
Logiciel :	22 %
Humain et logiciel :	13 %
Autres :	22 %

Y-a-t-il Blocage possible de la mise en production si défaut de PRA ?

Oui : 48 % Non : 26 %

6 CONTRAT DE SERVICE ET PRA

« On ne devrait externaliser ou contractualiser que ce que l'on maitrise ; sinon, on l'apprend rapidement à ses dépens »
L'expérience

6.1 Introduction

Dans quelle mesure la notion de contrat de service s'applique-t-elle aux PRA ? En cas de problème, qui assume quelles responsabilités ? Peut-on aller jusqu'à un engagement de résultats ?

La rédaction de ce chapitre diffère des précédents par sa construction : interrogative, multi-paragraphes, car la contractualisation reste souvent un exercice difficile.

Difficile car sensible: dans sa description, dans les attendus, dans son mode de pilotage, ... dans l'engagement juridique associé.

Nous avons donc choisi d'aborder le sujet sous l'axe des Questions/Points de vigilance qui permettra d'appréhender plus sereinement le sujet.

6.2 Résumé du chapitre

Les contrats de service de PRA se concluent soit au sein d'une entreprise, entre les différentes directions métiers et la DSI, soit avec une société de services externe, dans le cadre de l'outsourcing/externalisation du PRA.

Dans cette situation, plusieurs questions se posent :

- Quels sont les objectifs et le périmètre du PRA ?
- Que doit-on déléguer à un prestataire de services ?
- Quels engagements doit-on obtenir pour assurer le maintien en condition opérationnelle du PRA ?
- Quels engagements faut-il contractualiser pour la phase de déclenchement du PRA puis pour le support de l'infrastructure de secours durant toute la période de fonctionnement en mode secours ?
- Quel regard porter sur l'outsourcing du PRA ? Une pratique encore rare, comme le prouvent les réponses à notre enquête qui se trouvent en fin de ce chapitre.

6.3 Points à prendre en compte en amont de la rédaction du contrat de service

Nos amis juristes interviennent souvent lors de cette difficile rédaction pour nous rappeler qu'en matière contractuelle, on doit clairement spécifier ce que l'on attend ;

et c'est bien là que réside toute la difficulté : ne rien oublier. Nous vous proposons quelques axes de réflexions avant rédaction.

6.3.a Cas général, que le contrat soit interne ou externe

- Une nécessité : adapter le niveau de service (et donc le coût) du PRA aux enjeux métiers réels (cf. BIA).

- On n'externalise que ce qu'on maîtrise, cela vaut aussi pour le PRA.

- Un PRA implique la reprise d'un ensemble de services à un niveau déterminé pour les activités vitales de l'entreprise. Peut-on obtenir un engagement de résultats qualifié ? L'expérience montre que la chose est rare, mais pas inexistante, et que la question doit-être posée. Dans tous les cas, il faut définir précisément ce qui tient aux engagements de moyens et aux engagements de résultats. Attention, ces engagements sont à préciser aussi bien lors d'une négociation en interne entre l'équipe IT et les métiers, que dans le cas d'une négociation avec un prestataire externe.

- Une bonne pratique universelle : négocier des pénalités en cas de non-respect des engagements liés aux différentes composantes du PRA.

- Il faut formaliser des processus d'alerte et de gestion de crise, que le PRA fonctionne en interne ou en externe en y incluant le prestataire.

6.3.b Zoom sur l'externalisation du PRA

- A priori, quasiment tous les éléments techniques du PRA sont éligibles à l'externalisation : l'hébergement, les infrastructures, les serveurs de secours, les procédures, les opérations de reprise d'activités, le maintien opérationnel du site de secours.

- A contrario, tous les aspects « décisionnels » (organisation de crise) doivent être conservés en interne.

- Il faut se poser la question du coût de revient d'un PRA Interne et d'un PRA externalisé.

- Les modalités de mutualisation des moyens partagés chez le prestataire de services sont-elles bien définies et contractualisées ? (par exemple taux de mutualisation, règles de priorité des workloads en cas de sinistre, etc.)

- Il faut maintenant compter sur une nouvelle offre, à considérer pour des besoins peu élevés : les « cloud recovery services » ou PRA dans le Cloud.

6.3.c Périmètre de l'externalisation du PRA

- L'externalisation d'une solution de haute-disponibilité impliquant un dual-site de production n'est possible que dans le cadre de l'outsourcing du pilotage total de la production. Sans quoi le partage des responsabilités et le maintien en condition opérationnelle peut rapidement devenir inextricable. En effet, une solution haute-disponibilité fonctionne souvent comme un système unique réparti sur deux sites, on ne délègue pas plus la gestion de la moitié d'une telle architecture qu'on ne déléguerait celle d'un demi-serveur ...

- L'externalisation du secours à chaud ou à froid est envisageable en ce qui concerne le maintien en condition opérationnelle et la reprise d'activités. Le pilotage de la production sur le site de secours, suite à accident ou sinistre, ne peut pas être délégué et doit rester de la responsabilité de l'entreprise.

- Le client idéal pour un PRA externalisé ? Les SI les moins exigeants, ceux qui ne disposent pas de moyens préexistants, voire ceux qui n'ont pas encore mis en place de PRA. Il existe un certain nombre d'avantages dans cette situation :
  - Le prestaire apporte l'expertise technique.
  - La souplesse du dimensionnement, qui relève de la responsabilité du prestataire.
  - L'absence de gestion des infrastructures pour l'entreprise.
  - Un aiguillon externe pour avancer : en effet, externaliser un PRA constitue un bon moyen de se forcer à avancer en interne sur la définition de celui-ci si la chose n'a pas encore été faite.

6.4 La caractérisation des niveaux de service

De nombreuses directions (informatiques ou générales) se sont lancées dans une démarche de contractualisation interne et/ou externe des services. Ceci prend la forme de SLA (Service Level Agreement) et d'OLA (Operationnal Level Agreement), basés sur des notions de KPI (Key Performance Indicator). Ces démarches doivent inclure désormais un chapitre sur les PRA.

Dans ce cas, les critères de déclenchement du PRA sont associés à des notions de niveaux de service (complémentairement au BIA) couverts sous des descriptifs du type Or/Argent/Bronze ou autres.

Contenu d'un contrat SLA voire OLA :

Le plus souvent, il dépend de l'organisation de l'activité de l'entreprise. Qu'il s'agisse d'un contrat interne ou externe de PRA, celui-ci doit prendre en compte les particularités de fonctionnement des processus métiers de l'entreprise : les exigences diffèrent totalement si elle fonctionne 7 jours sur 7 et 24 heures sur 24 ou 5 jours par semaine, de 8 h à 18 h.

Trois blocs caractérisent l'établissement d'un tel contrat :

1. les modalités de gestion du maintien en condition opérationnelle du PRA,
2. les modalités de gestion et de conduite des tests,
3. les modalités de gestion du service en cas d'accident ou de sinistre.

6.4.a La contractualisation des niveaux de service du MCO du PRA

Elle précise l'ensemble des points suivants :

- La surveillance des serveurs et applications du PRA, par exemple à quelle fréquence sont-elles surveillées ?
- Les conditions de mise à niveau des infrastructures et des applicatifs sur le site de secours pour préserver la cohérence avec le site principal (par exemple les mises à jour sur le site PRA ne devront pas intervenir plus de quatre heures après celles appliquées sur le site principal).
- Les modalités de contrôle à l'implémentation de ces mises à niveau.

- Les mesures à prendre en cas d'écart constaté entre site principal et site de secours.
- La gestion d'incidents, accompagnée éventuellement de pénalités, et la remontée d'incidents survenus sur le site de secours.
- Les habilitations et astreintes des personnels impliquées dans le PRA et leur gestion dans le temps.
- Les responsables de la tenue à jour des procédures opérationnelles (exploitant, SI, métiers, permanence managériale).
- La définition des arrêts programmés pour maintenance du site de secours
- La gestion des dérogations de disponibilité du PRA, par exemple sous la forme d'un délai de consignation (durée prévue d'une intervention de maintenance sur le site de secours qui le rend indisponible) associé à un délai de restitution (en cas d'urgence, en combien de temps le site de secours peut-il être restauré dans un état utilisable dans le cadre du PRA, par exemple en revenant à un état antérieur à l'opération de maintenance).

Dans tous les cas, l'interruption de disponibilité du site de secours ne pourra pas excéder son délai de mise à disposition tel que défini contractuellement.
En résumé, il peut exister des opérations de maintenance de longue durée sur le site de secours, qui se traduisent par son indisponibilité, du moment qu'il est possible de remettre rapidement ce site en service en cas d'urgence.

6.4.b La contractualisation des niveaux de services applicables aux opérations de tests du PRA

Elle devra préciser les points suivants :

- Nature et fréquence des exercices de PRA, pénalités applicables en cas de non-respect de ce calendrier.
- Les exercices de PRA programmés se feront sans perte de données (exercices réels).
- En cas d'exercice de PRA inopiné, une perte de données inférieure à x mn sera tolérable.
- Définition de la préparation de l'exercice de PRA (revues des procédures, évaluation des risques et actions visant à les réduire, organisation des ressources,...)
- La réalisation et vérification de la « bascule aller puis retour» vers le site de secours selon la procédure adaptée au contexte.

6.4.c La contractualisation des niveaux de services en cas de déclenchement du PRA

- Plages de déclenchement. En concordance avec les horaires d'activité de l'entreprise, par exemple : le PRA du site peut être déclenché 24h/24 et 7j/7, mais aussi seulement les jours ouvrés, etc.
- Le délai de restitution du service est inférieur à x heures. Ce point doit aussi prendre en compte les plages ouvrées de l'entreprise : si le sinistre a lieu un lundi matin, le redémarrage devra intervenir l'après-midi. Si le sinistre a lieu en fin de journée, le redémarrage pourra intervenir dans la matinée suivante.

- Délai de restitution des données et de reprise des flux perdus durant le sinistre (attention, certaines formes de récupération sont de type SI et concernent des données brutes, d'autres sont de type métiers et demandent une réorganisation des données au sein des applications.)
- Les indicateurs de performances des processus en mode PRA doivent être les mêmes qu'en production normale après la période de bascule de 4 h.
- Préciser la fourniture des services associés au fonctionnement en mode secours avec l'accompagnement de proximité des acteurs participants.
- La remise en conformité du site de repli après exercice.
- Conditions du retour à une situation normale (par exemple effacement sécurisé des données sensibles sur le site de secours).
- la réalisation du bilan des opérations et la définition, avec l'ensemble des acteurs, d'un plan d'actions correctives ou d'amélioration.
- Le délai maximum de fonctionnement en mode PRA et les conditions de sortie à échéance.
- L'externalisation éventuelle des sauvegardes sur le site de secours, voire la gestion des opérations de production sur ce site, si elles sont prises en charge par l'équipe du prestataire externe.

6.5 Pilotage du contrat de service

Le contrat étant signé, reste à piloter la relation client/fournisseur sur la base d'un certain nombre d'axes :

- Comment piloter les évolutions contractuelles : juridiques, tiers, ...
- Quels indicateurs pouvez/devez-vous définir pour suivre le "caractère opérationnel" de l'infrastructure ?
- Avez-vous défini des indicateurs de suivi de la prestation ?
- Quelles sont les modalités juridiques intégrées dans le contrat ?
- Avez-vous défini des pénalités contractuelles en cas de non-conformité de la prestation ?
- Quid de clauses sur la rupture du contrat (délais de rupture, modalités de passation vers un autre prestataire, transmission d'informations) ?

Comble de malchance : vous venez de basculer en réel sur un site de PRA externalisé, qui lui aussi subit un incident (malheureuse expérience effectivement vécue par un membre du CRiP) : existe-il des clauses contractuelles en cas de sinistre sur le site de secours ? Comment cela est-il géré ?

6.6 Écueils et bonnes pratiques

Bonnes pratiques :

- Il faut adapter le niveau de service (et donc le coût) du contrat de service PRA aux enjeux métiers (cf. BIA)
- On n'externalise que ce que l'on maitrise.

Ecueils à éviter :

- Ne pas prévoir le secours du site de secours

Maturité des membres du CRiP

Exploitation du questionnaire

La contractualisation du PRA (interne ou externe) est devenue un standard

- 90% des répondants ont formalisé les engagements associés, en allant parfois jusqu'à un engagement de résultat (10% des cas)
- Toutefois, seuls 30% ont défini des pénalités en cas de non-respect de ces engagements

Les tests du PRA constituent le principal indicateur de performance du PRA

- Dans 90% des cas, le délai de reprise lors du test est le principal (voire unique) indicateur
- Test annuel systématique, mais 30% font plus d'un test par an (jusqu'à 4 !)
- 40% des tests proches d'une situation réelle / 35% des tests limités à une bascule unitaire
- Indicateurs « avancés » définis dans seulement 20% des cas (ex : taux de succès des sauvegardes PRA en interne, taux de mutualisation des moyens en externe)

L'externalisation du PRA : une pratique encore peu développée…

- 10% des répondants seulement s'appuient sur un prestataire de secours, la plupart s'appuyant plutôt sur leur infogérant actuel (PRA = extension de la production)

… malgré des apports variés et des freins assez limités

- Objectifs : solution complémentaire (45% des cas), réduction des coûts (30%), apport d'expertise technique (15%), etc.
- Freins : coût, sécurité des données, etc.

7 LE VOCABULAIRE PRA DANS CE LIVRE BLANC

« Ce qui se conçoit bien, s'énonce clairement
et les mots pour le dire arrivent aisément »
Boileau

→ Boot on SAN

Technologie permettant à un serveur connecté sur une baie SAN d'initialiser son système d'exploitation à distance.
Cette fonctionnalité permet, dans le cadre d'un dual-site disposant d'une réplication synchrone ou asynchrone des baies, de pouvoir redémarrer un serveur secondaire distant sur l'image parfaite du serveur primaire (accès non concurrent). Cette solution rentre dans les PRA à chaud.

Attention cette solution reste "fragile" car en cas de corruption de données sur les disques primaires, le site de secours devient automatiquement inopérant.

→ Clustering / Cluster = « Grappe »

Solution d'agrégation de serveurs (en grappe) permettant de mutualiser/répartir la fourniture d'un service sur des nœuds indépendant. Cette technique permet d'augmenter la disponibilité, et d'assurer la montée en charge.
Il existe des solutions de cluster matériels, logiciels (ex : Veritas Cluster Server) ou applicatif (ex : Oracle RAC)

→ Cellule de Crise Décisionnelle (CCD)
Cellule de Crise Opérationnelle (CCO)

Source : AFNOR
Elle est composée des responsables de chaque Direction utilisatrice concernée par le PCA. Elle comprend également des membres de la Direction Générale, de la Direction des Services Généraux, de la Direction des Ressources Humaines, de la Direction de la Communication, de la Direction Informatique et des responsables PCA. Son rôle est de se réunir en cas d'incident grave pour décider de déclencher ou non le PCA. Ses membres doivent être assujettis à des astreintes (service de garde) ou au moins être disponibles à tout moment et en tout lieu.

Commentaires CCA :
Il n'y a pas lieu de distinguer comité et cellule de crise, si ce n'est que le comité serait une réunion éventuellement élargie des membres de la cellule de crise.
Par contre, selon la taille de l'entreprise concernée, on peut distinguer cellule de crise décisionnelle (CCD) et cellule de crise opérationnelle (CCO) pour l'activation des PCA et la mise en œuvre des initiatives décidées par la CCD. Dans ce schéma-là, la CCD peut prendre des décisions stratégiques (ex : communiquer ou pas) et tactiques (choix de la modalité de mise en œuvre).

→ Cellule Technique Opérationnelle (CTO)

Elle est appelée pour évaluer la gravité de la situation suite à la survenance d'un incident qualifié de grave. Le résultat de son analyse décidera de la convocation de la CCD.

→ Délai Maximal d'Interruption Admissible (DMIA)

Source : Livre blanc lexique structuré de la continuité d'activité
Délai Maximal d'Interruption Admissible des activités après lequel l'entreprise s'expose à des pertes financières, d'image, à une désorganisation et à des manquements contractuels. Délai après lequel les systèmes, applications, ou les activités doivent être rétablis après une interruption (ex : 2 heures ; un jour ouvrable).

→ Domaine applicatif / Groupe d'application

Il s'agit d'un ensemble d'applications étroitement liées entre elles, du fait des flux qu'elles échangent et de leurs interactions. Suite à sinistre, elles doivent reprendre leurs traitements de façon synchronisée pour fournir les services attendus par les métiers. Un exemple : le traitement de la paye et le paiement des salaires, qui sont usuellement deux applications séparées pour éviter les fraudes.

→ Dual site

Le dual site regroupe deux sites de production se secourant réciproquement en cas de sinistre. Il est possible de répartir sa production sur les deux sites. Ils fonctionnent souvent en haute disponibilité.

→ Plan de continuité Informatique (PCI)

Partie strictement informatique du PRA.

→ Plan de Continuité d'Activités (PCA)

Source : Livre blanc lexique structuré de la continuité d'activité
Définit et identifie l'ensemble des moyens (organisation, procédures et matériels) requis pour se tenir prêt à faire face à un sinistre ou à une avarie majeure. Ces moyens doivent permettre d'assurer la continuité de service et le retour en mode normal dans les meilleurs délais possibles.

Le Plan de Continuité peut être conçu à différents niveaux. Par exemple, au niveau d'une filiale ou d'un métier ou répondant à un scénario particulier (ex : pandémie grippale, incendie de locaux, etc.) : on parle alors de différents PCA. L'ensemble de ces Plans de Continuité constitue le Plan de Continuité d'Entreprise (PCE).

→ Plan de Continuité Service (PCS)

Le Plan de Continuité de Service exprime les obligations réciproques des parties signataires, décrit l'organisation et les définit pour remplir les engagements de la DIT de continuité de service.

→ PCM : PCA Métiers : Plan de Continuité Métiers

Une sous-partie du PCA qui organise la continuité d'activités des métiers en relation avec l'ensemble du PCA dont la partie informatique. Il décrit un ensemble de procédures de fonctionnement métiers, par exemple en mode dégradé. Il décrit les contrôles fonctionnels que doivent effectuer les métiers à la reprise d'activités.

→ PCE : Plan de Continuité d'Entreprise

Le plan de continuité d'entreprise PCE est composé :
- de mesures de prévention, pour diminuer la probabilité d'occurrence d'une défaillance,
- de mesures de détection et de réaction, en ayant de bon réflexe,
- de plans de secours, pour diminuer les conséquences du sinistre

Un plan de secours se décompose en différents plans :
- un plan de gestion et de communication de crise,
- un PRA (plan de reprise d'activités) des moyens techniques (informatique, réseaux, autocom, téléphonie), pouvant nécessiter un site de secours, des plans de reconstruction de l'infrastructure, ...
- un PCA (plan de continuité d'activités) par métiers de l'entreprise, pouvant nécessiter un site de repli hébergeant les collaborateurs critiques des activités prioritaires,
- un plan de fonctionnement en secours,
- un plan de retour à une situation normale.

L'équivalent traduit en vision Anglo-Saxonne :
BCM= BIA + MCBS/RP + BCP
Business Continuity Management = Business Impact Analysis and Risk Analysis + identification of Mission Critical Business Services that must be recovered in an event of a failure and Remediation Plan +Business Continuity Plan

BCP= EM+CM+CP+DRP+BRP
Business Continuity Plan = Emergency Management + Crisis Management + Contingency Plans + Disaster Recovery Plans + Business Resumption Plans

→ Perte de Donnée Maximale Tolérable PDMT / PMDT / PDMA

Source : AFNOR (Perte de Données Maximale Admissible - PDMA)
Pour une application quelle est la perte acceptable au niveau des données (liée aux sauvegardes) pour que celle-ci soit d'un niveau acceptable pour les services utilisateurs. Selon les besoins exprimés, le degré de fraîcheur des données correspond à la perte des données considérées comme acceptable entre l'arrêt de l'activité et sa reprise. Par exemple, au démarrage après sinistre, les données peuvent dater de la veille au soir, du matin ou de la minute du sinistre.

→ Plan de Reprise d'Activités PRA

Le PRA est un des plans constitutifs du PCA qui couvre le secours des moyens informatiques et télécoms, l'ensemble des procédures et des dispositions prévues pour garantir à l'entreprise la reprise des applications et des données critiques suite à un sinistre informatique. Il garantit la reprise des systèmes désignés comme critiques dans le temps minimum fixé par le RPO.

→ Réplication asynchrone

Modèle de réplication dans lequel la synchronisation permanente des données n'est pas exigée. La réplication à distance est réalisée sans attendre l'accusé de réception sur le site émetteur. Il n'y a pas de contrainte de distance entre le site émetteur et le site récepteur, puisqu'il n y a pas d'impact sur le site émetteur.

→ Réplication synchrone

Modèle de réplication dans lequel les données sont en permanence strictement identiques sur les différents sites. La réplication à distance est réalisée lorsque l'accusé de réception d'écriture sur le site distant est revenu sur l'émetteur. Les limites de la physique font qu'il n'est pas possible de réaliser de réplication synchrone sur une distance supérieure à 70 km, surtout en raison des conséquences sur la durée des gros traitements batch. Attention, au niveau de réplication en mode synchrone : donnée, transaction.

→ Résilience

Source : AFNOR
Capacité d'une organisation à résister à un incident, à un accident, à une crise dans des environnements adverses, puis à revenir à un état normal.

Source : Joint Forum 2006
La capacité d'un acteur de l'industrie financière, d'une autorité financière ou d'un système financier à absorber l'impact d'une perturbation opérationnelle majeure et à poursuivre les opérations ou les services critiques.

Commentaire CCA :
Une nuance peut être apportée en français entre :

- Résilience : Qualité de celui qui se rétablit vite
- Robustesse : Qualité de ce qui reçoit des coups sans trop en souffrir

En anglais Robustness n'est pas employé.
Un bon PCA concoure à la robustesse ; un bon PRA à la résilience.

→ Retour à une situation normale

Source : AFNOR
Capacité d'une entreprise, après un choc extrême, à accepter et traiter de nouvelles opérations, à un rythme au moins égal à celui qui précède la catastrophe.

Commentaires CCA :
Lorsqu'il s'agit de retrouver une production ou un rythme pour les exploitations définis de manière contractuelle, on peut parler d'un retour à une situation nominale. D'une manière générale, le fait d'avoir vécu une crise apporte des renseignements permettant d'améliorer la situation antérieure. Il est préférable de parler d'un retour à une situation normale plutôt que d'un retour à la normale.
Le retour à la production nominale est un objectif de court terme et la prise en compte des enseignements de la crise (faiblesses, vulnérabilités qu'elle a révélées) est un objectif de moyen ou long terme.

→ RTO : Recovery Time Objective

Le RTO définit le délai de reprise informatique à partir duquel les services sont restaurés.
Il s'agit de la traduction informatique de l'expression du besoin métiers.
Par exemple : quatre heures, une journée.
Attention à bien déterminer le point de départ du chronomètre : décision de la CCD ou moment de survenance du sinistre.

→ RPO : Recovery Point Objective

Le RPO définit le point temporel stable antérieur au sinistre à partir duquel la reprise d'activités a lieu.
Il s'agit de la traduction informatique de l'expression du besoin métiers.
Par exemple : date de la dernière sauvegarde cohérente. Date de la dernière transaction synchrone validée.

→ Sauvegarde de production / de recours / d'archivage

→ Sauvegarde de production
Les sauvegardes d'exploitation sont effectuées pour assurer des restaurations suite à des problèmes d'exploitation : travaux à refaire, crash du serveur. Elles n'ont pas besoin d'être mises hors du site de production. Elles doivent être au contraire faciles d'accès pour réparer des incidents de production. Le nombre de versions et leur période de rétention sont définis par la MOA.

→ Sauvegarde de recours suite à un sinistre informatique
Les sauvegardes de recours sont effectuées pour assurer :
- la reprise d'activités sur le site de secours
- le fonctionnement en production sur le site de secours pendant plusieurs mois si nécessaire

Elles doivent être :
- effectuées à un point d'ancrage des restaurations
- mises hors du site de production, le plus tôt possible après leur création
- opérationnelles quoi qu'il arrive
- exhaustive (données, logiciels, documentation)
- contrôlées

→ Sauvegarde d'archivage :
Les sauvegardes d'archivage sont effectuées pour répondre à des demandes ponctuelles d'information en général pour des besoins réglementaires.

→ Sauvegarde des transactions

Enregistrement systématique de toutes les mises à jour réalisée sur une base de données (logging) ou dispositif équivalent (attention, cette notion évolue avec la généralisation des ESB). En cas de besoin, on peut réappliquer les mises à jour sur une base de données restaurée dans un état antérieur.

→ Sinistre régional

Sinistre majeur couvrant une importante zone géographique (séisme, tempête, inondation centennale). Ces sinistres de par leur ampleur induisent des impacts sur la vie humaine, les moyens de communication, ... Les solutions de secours de type campus ou de proximité ne protègent pas contre un sinistre régional.

Conclusion

« Au bout de la patience, il y a le ciel »
Proverbe africain

L'aventure rédactionnelle de ce livre touche à sa fin et nous souhaiterions rappeler que ce document constitue une approche technique, qui n'aurait de sens sans l'existence, les attentes, les exigences, ... de continuité du métier. Pensez à leur transmettre ce document.

Il sera intéressant d'envisager dans un prochain livre blanc d'aborder la notion de Plan de Continuité d'Activités (PCA) à charge des métiers. Car c'est ce couple Métiers/DSI qui doit converger vers une approche commune dans l'écriture de La Solution raisonnable et acceptable en matière de risques et de coûts pour l'entreprise. Et ce sans oublier que le PRA, si complet soit-il, ne peut jamais couvrir tous les risques. Et ce sans oublier non plus que si puissants soient les moyens techniques actuels, la reprise d'activités ne pourra jamais être absolument garantie. Il est indispensable d'y sensibiliser la direction générale.

Il ne faut pas oublier qu'un système d'information est un écosystème en perpétuelle évolution, et que le PRA doit en être le reflet.

Alors quelque soit la cause du sinistre, il y aura en situation de crise des ajustements à apporter pour lesquels seul l'entrainement et l'agilité des hommes de l'art pourront répondre.

Gardons à l'esprit, qu'en marge de tout cela, Monsieur PRA doit rester un homme de bon sens, qui revient toujours aux fondamentaux : quelle est la priorité ? Quel est le cœur de métier, ... Je citerai en exemple ce PCA où en cas de sinistre de l'entreprise, l'activité principale est assurée par un comptable avec un carnet de chèque. 'Faites simple mais pas simpliste'.

Pour finir, après l'avènement du web 2.0, l'arrivé dans nos entreprises des collaborateurs 2.0 (génération Y), l'émergence de l'interconnexion par le cloud, on assiste maintenant à la venue du Telco 2.0, phénomène de convergence des réseaux et des services. Alors dans cette mouvance internationale, le PRA 2.0 émergera t-il ?

Annexes

Liens

- **Livre Rouge sur la continuité d'activité :**
  http://www.redbooks.ibm.com/redbooks/pdfs/sg246547.pdf

- **Livre FFIEC sur le BCP**
  http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf

Ouvrages

- **Livre blanc du Club de la Continuité d'Activité : lexique structuré de la Continuité d'Activité**
  http://www.clubpca.eu

- **Guide des bonnes pratiques de la Continuité d'Activité à l'attention des Directions des Ressources Humaines**
  http://www.clubpca.eu

Articles Complémentaires

- **ITIL et la continuité d'Activité**
  Source internet : http://www.newsitweb.info/nov06/itil_nov06.html

L'objectif principal du processus de gestion de la continuité des services est de remettre en conditions opérationnelles les infrastructures informatiques pour supporter les fonctions métiers de l'entreprise en cas de destruction partielle ou totale des équipements. Il ne s'agit pas forcément de tout reprendre (d'ailleurs ITIL propose une option de reprise qui peut paraître singulière mais qui pourtant est de toute première importance: ne rien faire). En effet, le plan de reprise intègre la notion de fonction métier vitale pour concentrer les efforts sur les fonctions les plus critiques et ignorer s'il le faut, d'autres fonctions annexes.

- **Les étapes du processus**

Quatre étapes structurent le processus de gestion de la continuité des services. Elles permettent de développer puis de déployer les méthodes et les moyens qui permettront de garantir l'accès à l'information, en respectant les contraintes d'alignement et l'équilibre entre investissements et risques à couvrir.

- **Lancement :** dès la prise de conscience au sein de la DSI et de l'entreprise, ITIL recommande de cadrer l'initiative en définissant le périmètre de couverture, les ressources et les organisations impliquées.

- **Exigences et stratégie :** c'est le travail d'analyse (impact et risques) qui doit amener l'équipe projet à définir les stratégies de reprise. Les objectifs du processus y sont définis en accord avec les exigences des directions métiers. Trois fonctions composent cette étape: analyse d'impact, analyse des risques, stratégie de continuité.

- **Implémentation :** à partir de la stratégie de continuité décidée, l'organisation projet est mise en place pour définir le planning d'implémentation et élaborer les techniques de reprise pour l'ensemble des solutions couvertes par le plan. Les activités de cette étape sont: mise en place de l'organisation, planning d'implémentation, développement des dispositifs de secours, déploiement des mesures de réduction des risques, développement des procédures de reprise et tests de reprise.

- **Gestion opérationnelle :** en mode production, le processus veille à la sensibilisation des ressources et à la formation des experts identifiés. Le processus de gestion des changements s'assure que toute modification pouvant impacter la reprise est analysée et intégrée aux solutions de secours. Les activités de cette étape sont: éducation et sensibilisation, audits, plans de tests, gestion des changements et formations.

• Les options de reprise

Six options de reprise sont proposées par le référentiel ITIL. Elles permettent d'adapter la stratégie de reprise aux contraintes et aux exigences des directions métiers.

- **Ne rien faire :** cas des solutions dont l'entreprise peut se dispenser en cas de sinistre majeur.
- **Solution de contournement manuelle :** la direction métier dispose d'un dispositif ou d'une méthode qui lui permet de continuer son activité sans l'outil informatique.
- **Partenariat réciproque :** solution de partenariat entre deux organisations de l'entreprise ou entre deux sociétés sur un dispositif de secours mutuel.
- **Reprise progressive :** aussi appelée «cold stand by», cette option propose une reprise sous 72 heures. Elle concerne les applications non critiques. L'infrastructure de secours est construite sur demande en cas de sinistre.
- **Reprise intermédiaire :** aussi appelée «warm stand by», et dédiée aux fonctions critiques, cette option se positionne sur une reprise comprise entre 24 et 72 heures. La solution de secours, de type mutualisée, est affectée à l'entreprise au moment du sinistre.
- **Reprise immédiate :** pour les fonctions vitales, il est parfois nécessaire de garantir une reprise sous des délais très courts. Ce qui suppose la mise à disposition d'un environnement de secours dédié. Cette option est parfois appelée «hot stand by» car les données y sont généralement déjà présentes au moment du déclenchement du plan de reprise.

Toutes ces options peuvent bien évidemment cohabiter pour offrir un plan de reprise adapté à chaque exigence métier. La communication, la disponibilité et les mises à jour des procédures de reprise sont capitales pour obtenir de cet investissement le retour escompté.

• Les avantages du processus

Au delà du fait que la DSI et l'entreprise n'ont pas forcément d'alternative à la mise en œuvre d'un plan de reprise, ce processus apporte la garantie que les fonctions vitales de l'entreprise continueront à pouvoir fonctionner même en cas de sinistre majeur. Dans sa démarche de gouvernance et d'alignement, le DSI dispose d'un processus clé pour l'élaboration de sa stratégie.

- **Pour les directions utilisatrices :** le processus de gestion de la continuité des services prend en compte, dès la deuxième étape de son cycle, l'impact d'un arrêt prolongé du service. Il s'agit ensuite de développer des solutions adaptées à chaque profil en fonction du risque, de l'impact et de l'exigence. La direction métier dispose donc d'un service aligné à ses besoins en matière de continuité, et sur lequel la DSI s'engage sur les résultats.
- **Pour la DSI :** le référentiel ITIL apporte les bonnes pratiques nécessaires à un dispositif auquel la DSI ne peut plus échapper. Les pressions concurrentielles sur l'entreprise entrainent obligatoirement l'exigence de continuité. La DSI peut ici capitaliser sur des pratiques largement utilisées dans de nombreuses entreprises en adaptant le référentiel à ses propres

A propos du

Le Club de la Continuité d'Activité

Association régie par la loi de 1901, dotée d'un Bureau et d'un Conseil d'Administration

- Crée en 2007, pour échanger sur la Gestion de la Continuité d'Activité (GCA)
- Réunit des entreprises et des administrations de toutes tailles, de tous secteurs, de tous pays (une centaine d'adhérents)
- Ouverte à tous praticiens concernés : Responsable de la Continuité d'Activité (entreprise, administration), Directeur des risques, Professeur, Etudiant (maitrise)

Son objet est de réunir tous les praticiens œuvrant dans le domaine de la Gestion de la Continuité d'Activité afin de :

- Partager leurs visions : retour d'expérience, bonnes pratiques
- Parfaire leurs maîtrises : solutions, réglementation, normes
- Pérenniser leurs actions : intégration de la Gestion de la Continuité d'Activité dans la stratégie de l'entreprise

Notre mode de fonctionnement

A l'initiative d'un adhérent voulant approfondir et confronter son expérience, une réunion d'échanges et de retour d'expérience est organisée (matinale de la continuité). A l'issue de cette réunion, un document « état de l'art » est produit et un groupe de travail peut être constitué pour approfondir le sujet. Ce groupe produira un livre blanc et les résultats seront présentés lors d'une matinales de la continuité.

Les matinales du CCA

- **2 octobre 2008 :** Validation probante du PRA
- **11 décembre 2008 :** Site de repli interne ou externe
- **16 septembre 2008 :** Retour d'expérience sur la pandémie grippale
- **11 décembre 2008 :** la crise économique et la continuité
- **28 avril 2009 :** le cloud computing et la continuité d'activité
- **1er décembre 2009 :** Quelles responsabilités au sein d'une organisation en matière de gestion de la continuité d'activité?
- **19 janvier 2010 :** La normalisation des PCA
- **23 mars 2010 :** Réalisation d'un exercice de gestion de crise en direct
- **1er juin 2010 :** Certification PCA : Comment faire certifier son dispositif de gestion de la continuité d'activité et par qui?
- **12 octobre 2010 :** la supply chain et la continuité d'activité
- **9 décembre 2010 :** le retour d'expérience de trois sinistres réels
- **10 février 2011 :** la présentation du livre blanc PRA, résultat du groupe de travail PRA
- **22 mars 2011 :** le manuel de la continuité d'activité destiné au DRH issu du groupe de travail PCA et RH
- **Date non planifiée :** Exercice de gestion de crise

Groupes de travail :

- Concepts & vocabulaires de la Gestion de la Continuité d'Activité
  - Elaboration d'un lexique structuré de tous les concepts en regroupant tous les vocabulaires employés aux USA, UK et France. Proposition de définition et commentaire du CCA
- Pandémie grippale → gestion des grands risques
  - Elargir aux grands risques. Le groupe convient qu'il serait judicieux de poursuivre les réflexions sur le thème des grands risques, ceux sur lesquels l'effort de compréhension des phénomènes et des enjeux nécessite une réponse globale, à la fois dans l'entreprise mais également au niveau du pays.
- Juridique
  - Regroupement des textes juridiques concernant la continuité d'activité
- PCA et RH
  - Elaboration d'un guide de bonnes pratiques de la Continuité d'Activité à l'attention des RH.
- PRA en 2010
  - Elaboration du présent livre blanc PRA
- PCA en 2010
  - Elaboration d'un livre blanc PCA
- Pré normalisation
  - Etude des normes existantes ; Proposition d'une liste de critères pour évaluer un PCA
- Risque pénal et juridique en Continuité d'Activité
  - La vocation du groupe de travail est d'appréhender la responsabilité de l'entité qui met en œuvre le plan de continuité, de sa défaillance, voire de son absence.
  - La gestion de crise (en création)
  - La continuité d'activité et la supply chain (en création)

Pour toute information, n'hésitez pas à:

Visiter notre site Internet : www.clubpca.eu

Nous adresser un mail : contact@clubpca.eu

Nous envoyer un courrier :
73 rue Anatole France, 92300 Levallois Perret

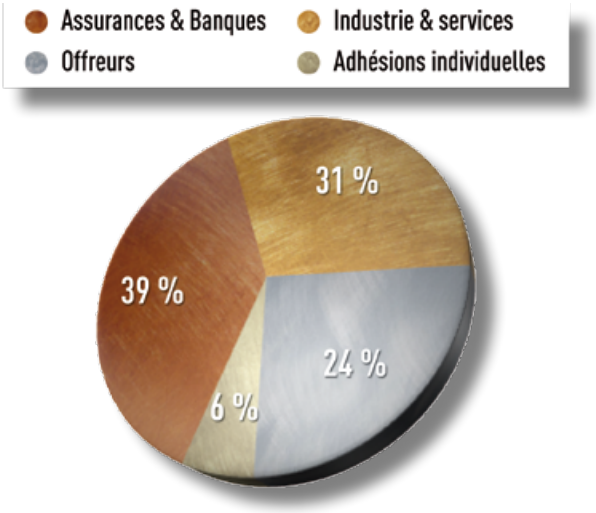
Membres du bureau du CCA (2010 – 2011)

Olivier CREHANGE, président - BPCE : olivier.crehange@bpce.fr
François TÊTE, président d'honneur - Devoteam : francois.tete@devoteam.fr
Pierre Dominique LANSARD, vice président - France Télécom : pierredominique1.lansard@orange-ftgroupe.com
Hervé MOLINA, trésorier - Groupe La Poste : herve.molina@laposte.fr

→ L'objectif du Club de la Continuité d'Activité

Le métier de Responsable PCA s'est progressivement créé, d'abord au sein des entreprises bancaires et financières; contraintes par des obligations réglementaires, et s'élargit aujourd'hui vers les autres secteurs d'activité.

Des acteurs provenant de divers horizons (Assurances & Banques, Télécommunications, Services, Conseils, Industrie) se sont alliés
afin de fonder en Octobre 2006 le CCA. Aujourd'hui le CCA compte plus de 50 sociétés adhérentes représentant 90 membres actifs.



Les objectifs de ce club sont de favoriser les retours d'expériences entre Responsables PCA, et de participer à l'évolution du métier
par la publication de documents de référence.
C'est dans cette perspective que les groupes de travail ont été formés.

> Adhérez au CCA

L'adhésion au CCA, loi 1901, est ouverte à tous
les praticiens de la Continuité d'Activité :
RPCA,
RSSI,
DSI,
Direction des Risques,
Direction de la Conformité,
Direction de la Production,
et tous les responsables ayant des missions liées
à la Continuité d'Activité.

Pour plus d'informations, veuillez consulter les documents d'adhésion sur le site www.clubpca.eu

A propos du CRiP

Le Club des Responsables d'Infrastructure et de Production

Investir dans la production

Les responsables d'infrastructure et de production viennent d'abord au CRiP pour y travailler ensemble à élaborer les contenus qui les aideront à devenir plus performants dans leur métier. Ils y viennent aussi pour se rencontrer et pour se fréquenter, mais notre club a avant tout pour vocation de créer des outils de travail et d'expertise. Le noyau dur de nos activités se renforce, mais reste le même : des conférences thématiques plus fréquentes, une production éditoriale renforcée, des groupes de travail plus nombreux. Le tout en conservant à l'égard des fournisseurs une stricte indépendance, condition impérative pour que nos échanges se déroulent avec le degré de confiance nécessaire entre nous. Cette façon de procéder nous garantit que chacun d'entre nous apportera au CRiP sans réserves l'expression de son savoir-faire tout autant que celle des questions qu'il se pose. Tant mieux. Nous sommes une communauté de travail, et ces questions reflètent la vraie vie de l'entreprise, celle qui nous intéresse.

Le credo du CRiP : Indépendance par rapport aux fournisseurs et sociétés de consulting

Philippe SERSOT
Président du CRiP
CTO CA-CIB



Partager nos expériences

J'ai trouvé très intéressante l'initiative du CRiP de réunir des Responsables de production en charge d'informatiques clientes variées dans un cercle où n'interviennent pas les fournisseurs. Cela permet de confronter ses propres idées aux retours d'expériences d'autres sociétés plus avancées sur certains sujets. Une démarche d'autant plus indispensable que nous nous trouvons, dans le métier de la production informatique, particulièrement exposés à des situations de grands changements, tels que la virtualisation dans ses multiples dimensions ou le cloud computing. J'apprécie particulièrement ce souci d'apporter, partager et recevoir tout en même temps ces indispensables retours d'expérience.

Jean-Paul AMOROS
GDF SUEZ
CTO/Directeur de la Production Informatique,
membre du Bureau Exécutif du CRiP



Le Bureau exécutif

Président :
- **Philippe SERSOT**
  CA-CIB - CTO

Vice-présidents :
- **Marc LIMODIN**
  LA BANQUE POSTALE
  Directeur des Techniques et Infrastructures
- **François STEPHAN** - THALES
  Directeur Technique
- **Eric STERN**
  ORANGE-FRANCE TELECOM
  Responsable Expertise Environnement Technique
- **Noël CAVALIERE**
  PSA PEUGEOT-CITROËN
  Responsable de l'Architecture Technique
- **Claude CORIAT** – RENAULT
  Responsable Stratégie et Politiques Techniques
- **Jean-Paul AMOROS** - GDF SUEZ
  CTO /Directeur de la Production Informatique
- **Olivier MAUPATE** - IT Director
- **Pascal PICCHIOTTINO**
  BOUYGUES TELECOM
  Responsable Département Infrastructure SI Réseau
- **Frédéric DIDIER**
  CREDIT FONCIER
  Directeur Production Informatique

Secrétaire : Michel GROSBOST

Trésorier : Gilles ALBERT
SOCIETE GENERALE
Technology Strategy Manager

Plus de 115 grandes entreprises françaises adhèrent ou sont en cours d'adhésion au CRiP :

TOTAL
MAAF
L'OREAL
GROUPAMA SI
DARVA
CREDIT AGRICOLE SA
ADP GSI
AEROPORTS DE PARIS
ERDF
GIE ALLIANZ INFORMATIQUE
EIFFAGE
AIR LIQUIDE
MINISTERE DES FINANCES
RENAULT
CCR ASSET MANAGEMENT
AREVA
LA FRANCAISE DES JEUX
SWISS LIFE
KEOLIS
AUCHAN INTERNATIONAL TECHNOLOGY
AVIVA
SOCIETE GENERALE
AXA TECH
LAFARGE
BRED
MUREX
NEXTER GROUP
NORBERT DENTRESSANGLE
BOUYGUES TELECOM
CASINO
THALES GROUP
CNES
VALLOUREC
MANPOWER FRANCE
RTE FRANCE
BIC
CHOREGIE
FRANCE TELEVISIONS
CA SITS
DISNEY
DIRECTION DES DOUANES
CREDIT IMMOBILIER DE FRANCE
DANONE
DCNS
CNP ASSURANCES
INA
CPSIAT – ARMEE DE TERRE
CREDIT FONCIER
EDF
ESSILOR INTERNATIONAL
FM LOGISTIC
LOUIS VUITTON MALLETIER
GENERALI
GDF SUEZ
SFR
SI2M (MALAKOFF MEDERIC)
VENTE PRIVEE.COM
I-BP
AIR FRANCE
MACIF
ARAMICE
MINISTERE DE L'INTERIEUR
CARREFOUR GROUPE
IMS GROUP
NATIXIS
GROUPE ADEO
OECD
ORANGE FT GROUPE
PMU
ARKEMA
RESEAU FERRE DE FRANCE
RHODIA
SAINT GOBAIN
SANOFI AVENTIS
CA SILCA
CAISSE DES DEPOTS
LA BANQUE POSTALE
GCE TECH (CAISSE EPARGNE)
CREDIT AGRICOLE CIB
CANAL +
APHP
PSA PEUGEOT-CITROEN
RATP
ALSTOM
SCOR
STIME
POLE EMPLOI
DEXIA
LA POSTE
MINISTERE DE LA DEFENSE
SNCF
GENERALE DE SANTE
VOLVO IT
SPIE
DIM
TECHNIP
ETAM
SUPERMARCHES MATCH
EULER HERMES
PRAXIS SERVIER
GROUPE PREVOIR
PIERRE FABRE
AGIRC-ARRCO
COFACE
BUREAU VERITAS
COFIDIS
CFAO
VALEO
Etc...

Le CRiP (Association Loi 1901) compte 115 grandes entreprises ou entités utilisatrices des technologies de l'information, adhérentes ou en cours d'adhésion. Il rassemble une communauté de plus de 900 membres, responsables d'infrastructure ou de production.

Le CRiP est un cercle de confiance, lieu d'échanges et d'informations entre les différents membres confrontés aux mêmes défis financiers, technologiques et organisationnels.

Objectifs

- **Etre plus performant dans les métiers de l'infrastructure et de la production**
- **Partager** nos visions et retours d'expériences
- **Echanger** et travailler sur
  - les technologies
  - les ressources humaines
  - les organisations et processus
  - les approches financières des projets
  - les relations avec les offreurs
- **Promouvoir** notre fonction au sein des entreprises
- **S'appuyer** sur les travaux du **CRiP** pour asseoir une position au sein de notre entreprise
- **Créer** un réseau de communication rapide et efficace entre dirigeants.

16 Groupes de travail sont actifs à ce jour

Le mode de fonctionnement

Actuellement, 16 groupes de travail thématiques se réunissent tout au long de l'année.
Les groupes sur les thèmes Réseaux, Mobilité & Collaboratif et Maîtrise des coûts viennent d'être créés.
Les travaux de ces groupes sont présentés à l'ensemble des membres deux fois par an lors des plénières et à l'occasion de la Convention annuelle du **CRiP** au sein d'itiForums.



STOCKAGE

Animé par
François DESSABLES
Architecte SAN Stockage
PSA PEUGEOT-CITROËN

Objectifs :
Identifier et partager les bonnes pratiques dans le domaine du stockage, établir le cadre d'usage des différentes technologies.

Thèmes :
- Virtualisation du stockage/de la sauvegarde
- Déduplication
- Sauvegarde sur disques
- Réplication
- Convergence LAN-SAN
- Architectures.

CRiP Thématique
Stockage
14 décembre 2011

Livre Blanc
Analyse et Tendance
du Stockage
(édité en novembre 2009)



MÉTIERS

Animé par
Marc LIMODIN
Directeur des Techniques
et des Infrastructures
LA BANQUE POSTALE

Objectifs :
Traiter de l'évolution des métiers de l'infrastructure et de la production, des problématiques de ressources humaines et des problématiques d'organisation.

Thèmes :
- Panorama des métiers et de leurs changements,
- Sous-traitance,
- Gestion des ressources humaines de production.

Livre Blanc
Métier
(prévu en 2011)

EFFICACITÉ ENERGETIQUE et DATACENTER



Animé par
Claude CORIAT
Responsables Stratégie
et Politiques Techniques
RENAULT



Animé par
Eric STERN
Responsable Expertise
Environnement Technique
ORANGE FT

Objectifs :
Identifier les meilleures pratiques en production pour le datacenter de demain et pour l'optimisation de la consommation des composants d'infrastructure

Thèmes :
- Optimisation énergétique
- PUE, définition d'indicateurs
- Outillages de mesure
- Bonne gestion du froid
- Green IT, design de site

Livre Blanc
Analyse et Tendance, vers
le Datacenter idéal
(édité en juin 2009 à
l'occasion d'Itiforums)

CRiP Thématique
Datacenter
10 novembre 2010

Dossier Technique Datacenters :
Efficacité Energétique et indicateurs
de performances
(édité en mars 2010)

LOW COST



Animé par
Frédéric DIDIER
Directeur Production Informatique
CREDIT FONCIER

Objectifs :
Inventorier les pratiques d'infrastructure de rupture capables de fournir des services à bas coût et les pratiques associées.

Thèmes :
- Logiciels open source,
- Bring-your-own-PC,
- Appliances,
- Différenciation des classes de service dans le datacenter,
- Utilisation de services et matériels grand public.

CRiP Thématique
Low Cost
6 avril 2011

CLOUD COMPUTING



Animé par
François STEPHAN
Directeur
IT Transformation
THALES

Objectifs :
Comprendre et analyser les technologies du cloud computing pour déterminer leurs conditions d'usage.

Thèmes :
- Définition des concepts,
- Gains attendus et constatés,
- Sécurité,
- Typologie des usages,
- Modèles privé-public-mixte,
- Retours d'expériences et roadmaps des membres du CRIP.

Livre Blanc
Analyse et Grandes Tendances du Cloud Computing
(édité en juin 2010
à l'occasion d'Itiforums)

CRiP Thématique
Cloud Computing
13 janvier 2011

z/OS



Animé par
Bruno KOCH
Directeur Délégué
Architecture Système Mainframe
GCE TECH (CAISSE EPARGNE)

Objectifs :
Gérer, optimiser et mieux maîtriser les coûts sur Mainframe, identifier les bonnes pratiques, inventorier les évolutions et optimisations possibles.

Thèmes :
- Modèles de facturations,
- Panorama de l'offre logicielle,
- Rationalisation et consolidation,
- Tendances du marché.

Maîtrise des coûts
z/OS
17 Novembre 2011

VIRTUALISATION SERVEURS & POSTES DE TRAVAIL



Animé par
Marie-Christine MOULLART
Responsable Exploitation /
Direction Infrastructures et Support
GENERALI

Objectifs :
Recenser les expériences et les solutions, analyser les enjeux, décrire la démarche projet.

Thèmes :
- Solutions, arguments en faveur de la virtualisation, bonnes pratiques, pièges et limites, impacts sur les projets les hommes et les services, les gains financiers et de niveaux de services.

Dossier Technique
Hyperviseur
(édité en Décembre 2010)

CRiP Thématique
Virtualisation Serveurs
19 mai 2010

CRiP Thématique
Virtualisation Postes de Travail
28 avril 2011

BASES DE DONNÉES



Animé par
Jean-Paul VEZARD
Ancien Responsable DBA à
la SOCIÉTÉ GÉNÉRALE

Objectifs :
Etudier les problèmes d'optimisation des SGBD.

Thèmes :
- Métrologie,
- Solutions de tolérance aux pannes,
- Méthodes de mutualisation,
- SGBD open source.

ARCHITECTURE TECHNIQUE D'ENTREPRISE



Animé par
Alain BALAGUER
Responsable Architecture

Objectifs :
Analyser les modèles de standardisation et de mise en oeuvre de modules opérationnels pour la construction du SI.

Thèmes :
- Perception de l'architecture technique d'entreprise,
- Définition du métier d'architecte technique,
- Bonnes pratiques,
- Référentiels et outils de cartographie.

PRA



Animé par
Luc VRIGNAUD
Responsable Division
Support et Sécurité
MACIF

Objectifs :
Etablir le cadre technique et opérationnel des plans de reprises d'activité.

Thèmes :
- Concepts et vocabulaire PRA,
- Architectures,
- Cohérence applicative,
- Critères de déclenchement,
- Maintien en conditions opérationnelles,
- Validité probante d'un PRA.

Livre Blanc
Plan de Reprise d'activités (PRA)
(prévu en février 2011)

En association avec CCA

CRiP Thématique
PRA
10 février 2011

CMDB



Animé par
Frédérick PAQUET
Responsable Outils et Process
THALES

Objectifs :
Rassembler et documenter les bonnes pratiques de mise en place et d'utilisation de CMDB

Thèmes :
- Périmètre et niveau de détail de la CMDB,
- Fiabiliser ses données,
- Gains attendus,
- Pièges à éviter lors de la création d'une CMDB,
- Exemples concrets de résultats de mise en place.

Livre Blanc - Comment construire et tirer bénéfice d'une CMDB ? (édité en juin 2010 à l'occasion de la Convention CRIP)

CRiP Thématique
CMDB
14 décembre 2010

ORCHESTRATION



Animé par
Hugues FONDEUX
Chargé de Mission Evolution de l'Infrastructure
PSA PEUGEOT CITROEN

Objectifs :
Etudier l'automatisation des processus d'exploitation informatique et établir les bonnes pratiques associées.

Thèmes :
- Gestion de fermes de serveurs,
- Provisioning,
- Accélération des PRA,
- Traitement automatisé d'incidents,
- Outils du marché,
- Difficultés rencontrées,
- Analyse de rentabilité.

GOUVERNANCE



Animé par
Maryse NICLI
Responsable Départements Projets,
Intégration et Correspondants Métiers
GENERALI

Objectifs :
Déterminer les conditions de mise en place de modèles de gouvernance dans l'informatique de production.

Thèmes :
- Opérations d'alignement métier,
- Gouvernance des contrats,
- Valeur ajoutée dans des environnements fortement externalisés.

Fiche Pratique Alignement Stratégique de la Production Informatique aux Métiers de l'Entreprise (éditée en mars 2010)

ANALYSE DES COÛTS DE LA PRODUCTION



Animé par
Sasun SAUGY
Chargé de Mission Infrastructure & Production
MINISTERE DES FINANCES ET DE L'ECONOMIE

Objectifs :
établir un modèle standardisé d'analyse des coûts qui prenne réellement en compte les spécificités de la Production

Thèmes :
- Inventaire des bonnes pratiques
- Analyse des modèles existants
- Méthodes de benchmarking des coûts
- Construction d'un référentiel de coûts Infrastructure et Production

RÉSEAUX, MOBILITÉ, COLLABORATIF



Animé par
Eric Cambos
Network & Telecom Manager
CREDIT AGRICOLE CIB

Objectifs :
traiter de l'ensemble des problématiques liées aux réseaux d'entreprise, en particulier la gestion de la mobilité et l'exploitation des outils de travail collaboratif

Thèmes :
- Haute disponibilité des réseaux
- Convergence SAN-LAN
- Le collaboratif
- La mobilité, les nouveaux terminaux (tablettes, smartphones, ByoPC)
- Réseaux et Cloud Computing

Les livrables du CRiP

Les Observatoires des Directeurs d'Infrastructure et de Production sont une initiative du **CRiP**. Ces observatoires regroupent l'ensemble des documents produits par les groupes de travail.

A l'usage des membres du **CRiP**,
ces documents sont de plusieurs types :
- Enquête et Analyse des tendances
- Livre Blanc : les meilleures pratiques
- Guide de rédaction d'appel d'offre
- Fiches pratiques

Les **Enquêtes et Analyses de tendances** sont issues de questionnaires renseignés par les membres du **CRiP**. L'analyse des résultats recueillis permet de mesurer et d'observer l'évolution des enjeux des CTOs et de leurs infrastructures. En outre, elle met en relief les grandes tendances liées aux principaux challenges des productions informatiques.
Dans le cadre de l'Observatoire des Directeurs d'Infrastructure et de Production, chaque groupe de travail actif apporte une contribution importante dans l'élaboration de documents de référence.
Actuellement, 16 groupes de travail **CRiP** sont actifs : DataCenter, Stockage, Could Computing, Low Cost, z/OS, Métiers, CMDB, PRA, Architecture Technique d'Entreprise, Virtualisation Serveur & Poste de Travail, Gouvernance, Bases de données, Efficacité Energétique, Orchestration, Réseaux, Mobilité & Collaboratif, et Maîtrise des Coûts.

Depuis trois ans, bon nombre de documents ont été publiés. Parmi les plus significatifs, on mentionnera :
- **Livre Blanc Enquête et Analyse des Tendances Serveurs**
- **Enquête et Analyse des Opérations informatiques**
- **Enquête et Analyse des tendances liées au Datacenter**
- **Livre Blanc Meilleures Pratiques du DataCenter**
- **Enquête et Analyse des Tendances du Stockage**
- **Enquête et Analyse des Tendances CMDB**
- **Définitions et Concepts, Enquête et Analyse des Tendances du Cloud Computing**
- **Fiche Pratique Alignement Stratégique de la Production Informatique aux Métiers de l'Entreprise**
- **Dossier Technique Datacenters : Efficacité Energétique et indicateurs de performances**
- **Dossier d'Analyse Technologique : Les Hyperviseurs serveurs x86**

Tous ces ouvrages produits ou en cours de production deviennent inéluctablement une référence importante pour les CTOs. Ils permettent de s'affranchir d'études parfois longues et coûteuses et de se « benchmarker » par rapport aux grandes tendances actuelles. Plus généralement, ils constituent des outils reconnus pour l'amélioration de la productivité.



Nicolas COURAUD
Responsable de la coordination des travaux du CRiP

ItiForums

le réseau social des professionnels de l'Infrastructure et de la Production

Une relation privilégiée avec le CRiP

Véritable associé du CRiP, ITIFORUMS est chargé de la communication, de la production et de la diffusion des documents et vidéos issus des travaux du CRiP, de l'organisation des évènements (Convention, CRiP Thématiques, CERCLE i) , du référencement fournisseurs, de la relation avec les partenaires stratégiques du CRiP, et de la relation avec les partenaires fournisseurs du CRiP (présence de porte-parole aux évènements propriétaires, voyages d'étude, etc..)

Charte d'Ethique et d'Engagement du CRiP

Le Club des Responsables d'Infrastructure et de Production est constitué sur la base de valeurs et de principes d'action et de comportement, fondés sur des rapports de confiance permanents entre ses membres.
Les membres sont les représentants des sociétés adhérentes du CRiP.

Principes d'action

· Respect de la loyauté
Les membres du **CRiP** ont pour principe la loyauté à l'égard des autres participants afin d'instaurer et de maintenir des relations de confiance durables.

· Participation active
Les sociétés adhérentes au **CRiP** et leurs représentants membres du **CRiP** s'engagent à contribuer activement à la vie du Club en apportant leur expérience et leur savoir-faire aux travaux collectifs.

Les sociétés adhérentes s'engagent
- à répondre dans un délai convenable aux différents questionnaires qui pourraient leur être envoyés
- à faire participer au moins un de leurs représentants à au moins un groupe de travail
- à favoriser la participation de leurs représentants aux plénières du **CRiP**
- à promouvoir le **CRiP** au sein de leur organisation

Les membres représentants s'engagent
- à se comporter en ambassadeur du **CRiP** et à promouvoir le **CRiP** auprès de leurs pairs et des fournisseurs
- à participer activement dans la mesure de leurs compétences, de leurs moyens, et de leurs autorisations internes aux conférences **CRiP**/ itiForums, soit en tant que membre d'un comité de programme, à travers un témoignage, une table ronde ou en aidant à la production de contenu.

Principes de comportement

· Confidentialité
Chaque membre du **CRiP** s'engage à ne pas divulguer à des tiers les informations professionnelles présentées, sauf accord explicite des membres émetteurs et du bureau exécutif du Club. Chacun des participants, membre permanent ou occasionnel, s'interdit d'utiliser directement ou indirectement, à des fins personnelles, des informations sensibles qu'il pourrait détenir dans le cadre du Club.

· Conflits d'intérêts
Chaque membre du **CRiP** se doit d'éviter toute situation de conflit entre les intérêts du Club et ses intérêts personnels ou ceux de ses proches.
Le Club est un club d'utilisateurs.
Cependant certains de ses membres peuvent appartenir à des sociétés adhérentes qui possèdent dans leurs missions une offre de service pour les autres adhérents. Il est impératif dans ce cas que les représentants membres de ces dites sociétés aient un comportement irréprochable et n'utilisent pas ce cercle de confiance pour promouvoir les offres de services de la société qui les emploie.

L'Etat de l'Art et la Traduction Opérationnelle des Services et Technologies dans la vraie vie de l'Entreprise

Des conférences Utilisateurs qui font le point sur les travaux du CRiP.
Les thèmes traités dans les sessions sont ceux des 16 groupes de travail actifs du CRiP.

Chaque session fournit à l'auditeur les clés de compréhension de la technologie, présente l'Etat de l'art et la traduction opérationnelle des technologies et services dans la vraie vie de l'Entreprise à travers des retours d'expériences utilisateurs.

CONVENTION ANNUELLE CRiP Infrastructure et Production 2011

21 & 22 Juin 2011
CNIT, Paris - La Défense

Les thèmes abordés :

- RÉSEAUX, MOBILITÉ ET COLLABORATIF
- STOCKAGE & SAUVEGARDE
- PRODUCTION ET INDUSTRIALISATION
- VIRTUALISATION SERVEURS ET POSTES DE TRAVAIL
- CLOUD COMPUTING
- LOW COST
- MAINFRAME & Z/OS
- DATA CENTER FACILITIES, GREEN IT, HÉBERGEMENT
- CONTINUITÉ D'ACTIVITÉ & PRA
- ARCHITECTURE TECHNIQUE D'ENTREPRISE
- BASES DE DONNÉES
- GOUVERNANCE, MÉTIERS, PROCESS, ITIL, CMDB

CRiP Thématiques

Les CRiP Thématiques programmées en 2011

13 janvier :	**Cloud Computing**
10 février :	**PRA**
6 avril :	**Low Cost**
28 avril :	**Virtualisation Poste de Travail**
15 septembre :	**Mobilité et Collaboratif**
13 octobre :	**Industrialisation de la production - Alignement des métiers**
17 novembre :	**Maîtrise des coûts - z/OS**
14 décembre :	**Stockage**

Le format choisi permet à l'auditeur :

- de se forger une opinion en toute indépendance à travers la restitution des travaux du **CRiP**, Club utilisateur des Responsables d'Infrastructure et de Production dont le crédo est l'indépendance vis-à-vis des fournisseurs

- de découvrir à travers des témoignages utilisateurs l'implémentation opérationnelle des technologies et solutions avec leurs composantes clés, leurs business cases, leurs bénéfices : promesses et réalités, leurs écueils et freins

- de bénéficier de l'éclairage sur les grandes tendances actuelles et le panorama de l'offre par un cabinet d'analyste de renommée internationale tel que « Forrester Research » qui est le partenaire stratégique du **CRiP**

- de rencontrer les acteurs majeurs du marché à l'occasion des pauses et du cocktail qui clôture ces sessions

Programme & inscription sur
www.itiforums.com

itiForums

Contacts

Club des Responsables d'Infrastructure et de Production
contact@crip-asso.fr
www.crip-asso.fr

Club de la Continuité d'Activité
contact@clubpca.eu
www.clubpca.eu

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation d'Alcane et du CRiP.



Infrastructure & Production

Club des Responsables
d'Infrastructure et de Production

www.crip-asso.fr

PARTAGER C C A PARFAIRE
PERENNISER

Club de la Continuité d'Activité

www.clubpca.eu

Création : fred.lameche - www.anousdejouer.fr