Fiche Pratique

CRiP Club des Responsables d'Infrastructures et de Production

En association avec le CCA PARTAGER PARFAIRE PERENNISER

PRA - PCA

Le calcul du ROI* du PRA

(*Retour sur Investissement)

Synthèse

Comme pour tout projet informatique, le ROI (Return on Investment) d'un PRA doit être calculé avant sa mise en œuvre. Ce ROI détermine le montant financier gagné ou perdu par l'entreprise par rapport aux sommes investies dans le projet. Mais comment calculer un ROI d'un PRA ?

Déterminer les coûts initiaux et récurrents du projet ne pose guère de problèmes. Les coûts récurrents doivent prendre en compte la validation périodique du PRA. En revanche, établir les gains potentiels et avérés se montre plus compliqué.

Le premier gain potentiel découle du déclenchement du PRA suite à sinistre. Dans cette situation, l'étude de BIA (Business Impact Analysis) conduite auprès des métiers préalablement au lancement du projet PRA détermine les gains à attendre. Ces gains découlent de la limitation des impacts du sinistre sur l'activité. Le calcul se base alors sur une logique de couverture des risques en liaison avec leur probabilité de survenance. LUn sinistre majeur se produit moins fréquemment que des sinistres mineurs partiels. L'investissement dans un PRA afin de faire face à un sinistre majeur se trouve aussi rentabilisé par l'utilisation de ce PRA pour réagir à des accidents moins spectaculaires, mais néanmoins potentiellement couteux, et plus fréquents.

Mais le sinistre ne constitue pas le seul horizon de ROI du PRA. La mise en place d'un PRA produit d'autres gains, même en l'absence de sinistre :

- Gain de productivité liée à l'amélioration du fonctionnement de la Production,
- Ajustements des contrats de maintenance consécutifs à la mise en place d'un fonctionnement en mode redondant plus ou moins poussé,
- Gains dus à l'utilisation ponctuelle des moyens de secours pour d'autres usages, dont la maintenance,
- Gains liés à une augmentation de parts de marché lorsque la sécurisation de l'activité de l'entreprise constitue un argument commercial,
- Réduction ou non-augmentation des primes d'assurances du fait de la réduction des risques,
- Gains liés à une meilleure maitrise des risques (calcul de fonds propres, taux des emprunts), pour le secteur Banque / Assurance.

Mai 2012

Contexte

D'après Dennis Hoffman de RSA : « La veille d'un incident, le ROI d'un système de sécurité est nul, le lendemain il est infini … ». Ce constat nous laisse sur notre faim. Peut-on affiner le calcul du ROI entre ces deux cas extrêmes ? Comment calculer ce ROI de manière réaliste ? Comment le faire évoluer dans le temps ? Doit-on justifier des investissements dans le PRA par un ROI ou par une couverture des risques ? Doit-on différencier les incidents se limitant à impacter les niveaux de services des sinistres graves ? Et dans ce dernier cas, le calcul de ROI a-t-il un sens ?

Le ROI établit le montant financier gagné ou perdu par rapport à la somme initialement investie dans un projet. En général, ce ratio s'exprime en pourcentage plutôt qu'en valeur. Il détermine le seuil de rentabilité d'un projet de PRA. Parfois, ce ROI s'exprime sous la forme d'une durée au bout de laquelle l'investissement initial se trouve remboursé par les gains réalisés.

Le débat se réduit-il à démontrer que le PRA présente la rentabilité d'une assurance (cotisation/gain lors de la survenue d'un incident) ou devons-nous ouvrir la discussion sur un autre axe, plus lisible de nos dirigeants ? C'est l'objet de notre réflexion dans ce document.

Problématique

Un calcul de ROI peut intervenir dans des projets de plusieurs types :

- Mise en place initiale d'un PRA
- Evolution d'un PRA à chaud vers un PRA Haute-Disponibilité
- Mise en place et maintien d'un PRA à l'aide d'un logiciel de gestion de PRA
- …

Le calcul doit se baser sur une comparaison entre les gains potentiels et avérés d'un côté, et les coûts d'investissements et récurrents de l'autre. Ces gains et ces coûts doivent être évalués selon différents axes d'analyse de ROI.

Il faut garder à l'esprit que pour chaque type de sinistre, les perspectives de gains associés peuvent faire varier le ROI. Aussi, en fonction du contexte, la couverture de certaines hypothèses de sinistre pourra ne pas être retenue, par exemple lorsque le montant du gain se montre trop faible, ou la probabilité d'occurrence trop minime.

Une constatation souvent avancée est que le site de secours constitue un facteur de coût. Cet argument ne tient plus dés qu'on en tire un bénéfice additionnel : réalisation d'une mutualisation, existence d'un site de production complémentaire, etc.

Certaines Directions affirment, de manière provocatrice, que pendant une interruption de service liée à un sinistre, l'entreprise n'a rien réellement perdu, mais seulement enregistré un manque à gagner temporaire. L'activité non produite durant l'interruption peut-elle vraiment, et toujours, être rattrapée le lendemain ?

Tant que l'accident n'a pas eu lieu, le PRA ne rapporte rien. Lorsque l'accident a eu lieu, il ne rapporte pas toujours quelque chose. Il faut donc prendre le problème autrement.

Analyse

Le coût annuel du secours doit être comparé au coût d'interruption du travail pour les utilisateurs connectés. Dans ce cas, le montant est directement calculable, et le gain en cas de sinistre aisément chiffrable. Celui-ci dépend directement de la criticité de l'activité qui a été déterminée par les métiers lors de l'étude de BIA (Business Impact Analysis) selon les critères habituels : pertes financières, perte d'image, pertes liées aux pénalités contractuelles, pertes de productivité.

Ces pertes sont chiffrables par les métiers.
L'approche par conventions de service (SLA ou OLA) largement déployée dans les entreprises permet aussi de fixer un type de réponse financièrement chiffrable en fonction du non respect des exigences du client.

Au-delà de son utilisation en cas de sinistre, le PRA peut apporter des gains induits avérés :

- **en matière de productivité :** Le PRA peut être vu comme une solution complémentaire contribuant au maintien du niveau de service inscrit dans le SLA, permettre une réduction des couts sur les interventions HNO grâce à la redondance, et indirectement permettre une meilleure connaissance de son SI. Il arrive souvent

qu'une démarche PRA permette d'améliorer le fonctionnement des applications par une re-urbanisation optimisée du SI.

- **en parts de marché :** l'argument du PRA est commercialement utilisable afin de rendre plus lisible le niveau de sécurité de l'entreprise (nouveaux contrats, place boursière, partenariats, …)
- **en image positive pour les investisseurs** car le PRA réduit le risque de perte de leurs actifs.

Un autre axe de mise en évidence des gains du PRA réside dans la réduction des risques. L'absence de PRA correspond à un risque maximum. Disposer d'un PRA réduit le risque, et cela se traduit par une réduction ou une non augmentation des primes d'assurances que doit payer l'entreprise.

> *NB : Dans les métiers de la Banque / Finance / Assurance, il existe des obligations réglementaires (type Bale II, Solvency II). Les directions générales ne demandent pas à leurs équipes de calculer un ROI, mais exigent que l'entreprise se place en conformité avec la réglementation. La question du ROI du PRA ne se pose donc éventuellement que pour la protection de la continuité d'activité des métiers. C'est un cas particulier.*

Prenons l'exemple d'un calcul de ROI dans le cadre du passage d'un PRA à chaud à une architecture de Haute Disponibilité. On constate alors que la Haute Disponibilité engendre d'importantes économies sur la maintenance. Lorsqu'un serveur tombe, il devient possible d'attendre quelques heures une intervention de maintenance puisque toute l'infrastructure est doublée. Ce mode de fonctionnement permet de réviser certains contrats, d'augmenter les délais d'intervention du prestataire, de sortir de conventions d'intervention 24/7 et sous quatre heures toujours couteuses, pour se replier sur des solutions moins onéreuses.

Relativisons cependant ces bénéfices, car les études du Gartner indiquent que les causes d'indisponibilité sont dues dans 60 % des cas à des à des problèmes logiciels ; dans 20 % des cas à des erreurs humaines et dans les 20 % des cas restant à des causes matérielles. La haute disponibilité ne remédierait donc qu'à 20 % des cas d'interruptions non planifiées.

La haute disponibilité dépend aussi de l'étendue du périmètre du SI. Plus il est consolidé et virtualisé, plus la haute disponibilité est facile à mettre en œuvre et donc moins onéreuse.

Pour reprendre l'exemple du domaine de la Banque/ Finance/ Assurance, les entreprises de ces secteurs d'activité sont notées, un peu comme par une agence de notation financière, en fonction de leur niveau de couverture de risques en matière de solvabilité. Si une banque n'a pas de PRA, cela impacte directement l'évaluation de sa note. Si cette note baisse, la Banque de France lui augmentera ses taux d'intérêts: Il y a donc là un argument économique clair.

Un autre exemple dans le domaine des opérateurs téléphoniques. L'état paye le service en contrepartie du respect strict des délais dans la réalisation des réquisitions légales et des obligations de portage de numéro, …

La façon la plus simple de présenter le ROI du PRA à une direction générale consiste donc à mettre en regard l'investissement (TCO (Total Cost of Ownership) équivalent à amortissement, coût récurrent, maintenance, exploitation du PRA) et une estimation du coût annuel de perte de l'activité métiers.

Selon les entreprises, on constate qu'il existe des processus à forts enjeux financiers, mais aussi des processus à fort impact sécuritaire, qui, dans certaines industries, ont la même valeur qu'une obligation réglementaire pour la Banque-Finances-Assurances.

Remarques générales

L'analyse de coût diffère selon les risques et selon les entreprises. Une corruption de données a plus de chances de se produire qu'un incendie de datacenter. Elle n'aura pas la même gravité pour une entreprise qui fait du transactionnel à flux tendu et pour une autre qui peut attendre 12 heures et rejouer ses transactions.

Les PRA ne couvrent pas tous les mêmes objectifs ; certaines entreprises veulent surtout préserver leurs données, d'autres leur activité (et/ou leur réputation). D'autres ont des obligations légales et tentent de ne pas se faire condamner. Certains encore travaillent sur des risques extrêmement lourds et savent que les coûts d'un arrêt de certaines fonctions informatiques seraient énormes du fait des accidents qui en découleraient éventuellement (énergie, contrôle aérien par exemple).

Il faut donc toujours établir une typologie de risques : ne pas se focaliser sur la seule perte de datacenter alors qu'il existe des risques plus fréquents, avec des impacts moins spectaculaires, mais tout aussi coûteux. Une solution est d'autant plus rentable qu'elle couvre des incidents moins graves et plus fréquents.

Il est important de noter que la réduction du risque engendrée par le PRA ne doit pas être ramenée qu'au seul ROI, mais que celui-ci constitue un élément non négligeable parmi une série incluant notamment la perte de données cruciales à la bonne marche de l'entreprise, sans lesquelles l'activité peut être sérieusement remise en cause ...

Un exemple de calcul de ROI

Cette démarche permet d'évaluer le niveau actuel des capacités du S.I. en termes de taux de disponibilité, les coûts liés à l'arrêt et ainsi de déterminer le coût du risque engendré (dans cet exemple, l'heure d'arrêt est estimée à 30 k€ pour une société X).

Niveau de Service	Silver	Gold	Platinium
Taux de disponibilité	99 %	99 ,5 %	99,9 %
Nb d'heures d'arrêt /an	87h22	43h41	8h46
Coût de l'heure d'arrêt	30.000 €	30.000 €	30.000 €
Coût du risque engendré	2.620.800 €	1.310.400 €	262.080 €

Cela permet de valider le modèle financier du projet et de comparer les coûts liés au projet de plan de secours avec ceux liés au risque engendré par le niveau actuel des capacités du S.I. en terme de taux de disponibilité. Et ainsi d'en mesurer ROI. Gartner Group estime à 2% la part du budget du service informatique qui doit être mobilisée pour préparer efficacement un PRA.

(*) : Restauration sur des serveurs utilisés habituellement à autre chose (pré production, ..)
(**) : Réplication de données, serveur dédié au secours non actif en attente, les applications sont à démarrer
(***) : Cluster dans le même data center avec réplication sur un data center distant
(****) : Cluster dans deux data centers distant de dix km environ.

Moyens mis en œuvre dans le plan de secours	Procédures de restauration (*)	Redondance des données (**)	Cluster local avec redondance (***)	Cluster distant avec redondance (****)
Coût du projet (investissement)	40.000 €	100.000 €	200.000 €	250.000 €
Maintenance	Faible	Moyen	Fort	Fort
Validation du PRA	Elevé	Elevé	faible	faible
Coût du risque avant projet (ex. 99,2 % à 3K€)	210.240 €	210.240 €	210.240 €	210.240 €
Pourcentage de réduction du risque	25 %	65 %	90 %	99 %
Réduction du risque	52.560 €	136.656 €	189.216 €	247.500 €

Dans cet exemple on constate que la meilleure solution financière est de type «redondance des données»

Conclusion

Comme nous l'avons vu dans ce document, l'argumentaire sur le ROI en matière de PRA (en tant que tel, donc juste envisagé dans la logique de reprise d'activité en cas d'incident) est difficilement suffisant. Il tombe court. Il faut l'enrichir, le diversifier, étendre les bénéfices du PRA au-delà de l'accident majeur.

L'approche que nous proposons vise à montrer que le PRA constitue un projet catalyseur et porteur d'améliorations au sein d'une démarche Sécurité au sens global. Ce projet génère de nombreux effets induits, qui sont eux directement chiffrables : amélioration de l'exploitation, ajustements contractuels (contrat d'intervention en 6/18 au lieu de 7/24 du fait de l'existence d'une infrastructure de Haute Disponibilité qui permet d'attendre quelques heures), maitrise des risques (calcul de fond propres), amélioration de l'image de l'entreprise, … il existe de nombreux arguments.

La question qui se pose au final est bien de savoir si cette évaluation/justification sert à montrer que l'on maitrise son budget ? Ou bien démontrer que l'alignement de certains projets IT répond aux exigences du métier dans l'expression de ses contraintes en matière légales et donc sécurité (couverture de risque). Probablement un peu des deux.

Nous cédons donc à la tentation de clore par la phrase de A. Capus : « Tout s'explique, rien ne se justifie ». La sécurité n'échappe pas à l'argumentaire. Soyez inventifs, soyez opportunistes.

Rédaction : Groupe de Travail PRA-PCA - Assistance Editoriale : Renaud Bonnet, CRiP - Création Fred.lameche - www.anousdejouer.fr

CRiP

Club des Responsables d'Infrastructures et de Production
15 rue vignon 75008 PARIS - contact@crip-asso.fr www.crip-asso.fr

Club de la Continuité d'Activité
73 rue Anatole France 92300 LEVALLOIS PERRET - contact@clubpca.eu www.clubpca.eu