



Le Plan de Continuité d'Activités (PCA)

Une étape primordiale dans la réduction des risques opérationnels

Les nouvelles normes prudentielles (Bâle 2) imposent une meilleure maîtrise des risques opérationnels. Leur prise en compte dans la mesure de la couverture en fonds propres (ratio Mc Donough) implique une identification exhaustive des facteurs de risque et des chaînes de traitement sensibles.

Les services en charge des risques opérationnels des entreprises d'investissement visent à établir les cartographies et définir les algorithmes afin d'évaluer globalement les pertes potentielles. Impliquées dans le suivi des risques, ils n'ont pas en général la responsabilité de définir les mesures permettant leur prévention. Il incombe ainsi aux opérationnels de conduire les projets visant à réduire et maîtriser ces risques. Une démarche qui doit être menée selon deux principaux axes : l'industrialisation des process dans une optique d'excellence opérationnelle et la définition d'un Plan de Continuité d'Activité (PCA).

Les auteurs

Franck Delbès, senior consultant
Philippe Prunier, manager

Pourquoi un PCA ?

Une entreprise est soumise à de nombreuses sources d'interruption de son activité intervenant à tous les niveaux de son organisation :

- systèmes d'information : défaillance du matériel informatique, erreur dans une application, corruption d'une base de données, arrêt d'un moyen de communication (réseau, télécoms), ... ;
- infrastructure : grève, accès impossible aux locaux, interruption de courant, erreur humaine, ... ;
- externes : feu, catastrophe naturelle, acte terroriste,

Les chiffres que vient de publier le Clusif (Club de la sécurité des systèmes d'information française) indiquent que les principales causes des sinistres qui affectent les systèmes d'information des entreprises françaises sont les pannes internes, les pertes de services essentiels (notamment les liaisons télécoms) et les erreurs également de garantir la constante disponibilité des services de ses partenaires et fournisseurs. Suite à un crash système chez mon courtier, quelle information m'assure-t-il sur le statut de mes ordres en attente et dans quel délai ? Les prestataires de sous-traitance informatique affichent des taux de disponibilité à 99,9... %.

Le PCA a pour objectif de prévoir les moyens techniques, contractuels, organisationnels et humains pour préparer l'entreprise à réagir face à une crise : maintenir ses prestations sans à-coups, ni rupture de charge et de façon transparente pour sa clientèle, protéger ses données stratégiques ou réglementaires et finalement son image de marque. Il est généralement décomposé en trois parties :

- le plan de secours : capacité à reprendre une activité suite à un sinistre ;
- le plan de crise : organisation et la communication pendant la crise ;
- le plan de reprise : préparation du retour à la situation normale.

Initiés pour le passage à l'an 2000 mais souvent limités au bug informatique et au week-end de bascule, ils n'ont pas toujours été maintenus. Une étude récente¹ montre que seules 44% des entreprises sont capables de réinstaller leurs collaborateurs sur un autre site suite à un incident majeur et qu'au moins 17% des entreprises ne peuvent récupérer leurs données après un sinistre.

Alors que leurs clients souhaitent des garanties sur la continuité des prestations qu'elles proposent, aujourd'hui trop peu d'entreprises d'investissement disposent d'un PCA en conditions opérationnelles. C'est un des critères de sélection dans les appels d'offres adressés par les clients institutionnels aux asset managers et la sélection des brokers. L'existence d'un PCA est appréciée des organismes de notation et des autorités de contrôle et il fait partie intégrante des conditions de service signées entre les entreprises d'investissement et leurs clients.

Un projet d'entreprise

L'élaboration d'un PCA est un projet d'entreprise et l'implication de la direction générale est importante. En effet, en plus des équipes « informatiques et sécurité » et des services généraux, la participation et l'engagement des directions opérationnelles sont indispensables. Seule une analyse orientée métier autorisera la définition des besoins et le choix de solutions techniques adéquates. Pour obtenir l'adhésion de tous les participants, la direction doit communiquer sur les attentes et les sensibiliser aux enjeux métier. Par exemple chez un courtier, comment recomposer mes positions suite à un crash système pour être en mesure de les déboucler sur le marché ? Les équipes opérationnelles doivent également être informées de la diversité des risques encourus. Ils vont au delà de l'interruption de courant ou de la panne informatique. Lors du récent incendie du Grand Hotel à Paris, tout le quartier a été bouclé plusieurs heures rendant l'accès aux locaux des entreprises du secteur impossible aux salariés ; soit d'autres événements plus rares mais bien plus tragiques : les attentats du 11 septembre, l'incendie du Crédit Lyonnais, l'explosion de l'usine AZF ou les inondations dans la baie de Somme. De même, les mesures de protection sont plus vastes qu'un extincteur, un générateur de secours ou un back up informatique (visant à sauvegarder et à restituer lorsque nécessaire les données).

Une démarche en quatre volets

Selon notre expérience, la définition et la mise en place d'un PCA se découpe en quatre volets :

- l'étude préalable qui définit le plan stratégique, fonction du niveau d'exigence attendu par la description des processus prioritaires et la sélection des risques à couvrir ;
- la conception des solutions de prévention et de secours envisageables ;
- la mise en place des mesures retenues et la définition du plan de crise et de reprise ;
- enfin, le suivi qui couvre les tests périodiques et la mise à jour régulière du plan de secours.

Dans un premier volet, les équipes opérationnelles identifient les processus métier prioritaires à partir des activités principales de l'entreprise. Les processus les plus critiques sont par exemple : pour un acteur du « buy side », la prise en compte des ordres de souscription / rachat des clients, la garantie d'assurer la meilleure gestion des actifs qui lui sont confiés et pour un asset manager le calcul et la diffusion de la valeur liquidative, ... ; côté « sell side » : le pricing, l'analyse financière, l'exécution et la confirmation des ordres, le règlement / livraison,.... Pour chaque processus sont ensuite détaillés :

- les acteurs internes et externes (fonction et responsabilités),
- les processus liés (chaîne de traitement),
- les données,
- les outils et applications informatiques,
- les flux d'information,
- les dispositions de sécurité et de protection existantes.

Le niveau actuel de couverture des polices d'assurance en cas de sinistre est évalué. Il est plus aisé, cette étape terminée, de synthétiser les forces et faiblesses de l'organisation sous l'angle de la continuité d'activité et de déterminer les facteurs de risques qui devront être couverts par le PCA.

Ensuite, la sensibilité de chacun des processus est évaluée en fonction des engagements de l'entreprise. En fonction de la durée d'une interruption d'activité sur une échelle de temps (par exemple : 1 heure, ½ journée, 1 jour, 2 jours et plus) et de la période de survenance (fin de mois, ...), la sévérité des pertes potentielles en termes commerciaux, d'image, financiers et réglementaires est estimée (faible, moyenne, importante) pour chaque nature de risque. Une analyse qui intègre les répercussions d'un incident sur le reste de la chaîne de traitement et la survenue d'autres risques. Le produit fini est un classement des processus par sensibilité au risque : probabilité de survenance du risque, durée de dysfonctionnement et impacts.

Des solutions de secours, mais à quel coût ?

L'objectif du second volet est de proposer, d'évaluer et finalement de concevoir les mesures à mettre en œuvre face aux risques non couverts. L'étude s'effectue sur trois niveaux : processus dans une logique d'entreprise étendue, systèmes d'information et locaux.

Dans un premier temps, les équipes travaillent en prévention. Elles déterminent les traitements qui peuvent être accélérés ou anticipés pour limiter leur sensibilité aux échéances horaires (cut off intraday) et périodiques (fin de mois, arrêts, ...). Cet état mensuel à diffuser pour le 15 du

¹ Etude réalisée par le cabinet Macarthur Stroud en mars 2002 sur un échantillon de 650 entreprises

mois suivant ne peut-il être finalisé dès le 5 ? Le nombre de traitements critiques au moment de la reprise après incident sera ainsi réduit. En parallèle, la mise en place de points de reprise facilite la relance des traitements et sécurise les informations : sauvegarde ou édition d'informations en intraday, calcul et enregistrement de résultats intermédiaires, archivage systématique de données à l'extérieur (contrats client par exemple),....

Ensuite, une palette de solutions à différents niveaux de sophistication existe pour définir le plan de sauvegarde, pour sécuriser les systèmes informatiques et de communication. Quel type de sauvegardes (sur support magnétique en fin de journée, par réplication, ...), comment sont-elles acheminées et où seront-elles conservées ? quelle configuration technique pour les serveurs (mise en miroir des systèmes de stockage) ? comment transmettre des informations à un tiers suite à la rupture d'une ligne spécialisée, en utilisant une ligne RTC, un email, un fax, un coursier ou faut-il dédoubler la ligne spécialisée, ... ? Les prix et les durées de mise en œuvre sont évaluées à grosse maille pour chacune des dispositions étudiées.

Enfin, pour redémarrer l'activité dans les délais les plus courts en cas d'accès rendu impossible aux locaux, les options pour la mise en œuvre d'un site secondaire distant sont détaillées : back up mutuel entre organisations similaires, site de secours géré par l'entreprise elle-même ou dépendant d'un prestataire, La liste du matériel de remplacement est établie : fournitures de bureaux, mobilier,

La priorité est donnée aux solutions et aux fournisseurs limitant au moindre coût les risques importants pour constituer le plan de secours cible. Un arbitrage est ensuite nécessaire à partir des ratios coût / risque couvert, soit du risque que l'entreprise choisit d'assumer et de son niveau d'exigence par rapport au délai de reprise attendu.

Le troisième volet couvre la mise en place du plan de secours. En parallèle, les contrats de service avec les principaux fournisseurs (sous-traitant informatique, fournisseur de flux financiers, help desk des éditeurs de progiciels financiers, dépositaires, brokers, ...) sont le cas échéant renégociés en renforçant les aspects continuité de services : engagement sur les moyens mis en œuvre et les délais d'intervention. De même, les polices d'assurance de l'entreprise peuvent être révisées.

Ces étapes terminées, l'organisation en situation de crise est préparée à travers la définition du plan de crise :

- logistique (liste de contacts, matériel à disposition, ...)
- et communication interne ;
- procédures opérationnelles dégradées claires et facilement applicables dans l'urgence ;
- coordinateur et autres membres du comité de crise ;
- stratégie de communication externe et d'activation des prestataires externes.

Les conditions pratiques de la remise de l'activité en situation normale seront dépendantes du degré de sévérité et des impacts d'une interruption. S'il peut être défini dans les grandes lignes, le plan de reprise est généralement précisé en fonction de la situation réelle.

Faire vivre son PCA

Le quatrième volet est sans doute le plus difficile. Il est nécessaire de mettre en place des moyens de surveillance pour tester fréquemment les solutions de secours, par exemple en vérifiant que les sauvegardes sur support magnétique sont complètes et lisibles. Des simulations de sinistres annuelles permettront de dérouler complètement le plan de secours pour les services concernés et de le mettre à jour si besoin. Le PCA doit de plus être constamment adapté à l'évolution des activités de l'entreprise : nouvelle activité, changement de système, réorganisation des processus, incident non recensé,....

Près de 45% des entreprises n'ont pas revu leurs PCA depuis plus d'un an et 12% depuis plus de deux ans². La direction doit instaurer un comité de sécurité en charge du maintien en conditions opérationnelles, réunissant des représentants de chaque direction. Pour obtenir des responsables de services une mise à jour régulière du plan, elle doit l'intégrer à leurs objectifs et pratiquer régulièrement des contrôles par l'intermédiaire de l'audit interne.

Les entreprises disposant d'un PCA limiteront leurs risques opérationnels en couvrant les risques relatifs à la continuité de l'exploitation en cas de sinistre majeur. Elles garantiront le niveau de services à leurs clients et sécuriseront ainsi leur activité. Les clients mais également les actionnaires de l'entreprise se montrent de plus en plus intéressés par la gestion des risques opérationnels. En effet, une gestion efficace optimise l'utilisation des fonds propres et diminue en définitive la volatilité des performances financières. Mais ceci ne peut se faire sans une volonté des dirigeants de s'engager à long terme dans une démarche de maîtrise de ces risques.

² Etude réalisée par le cabinet Macarthur Stroud en mars 2002 sur un échantillon de 650 entreprises