Plan de Continuité d'Activité, Plan de Reprise d'Activité

Synthèse de la conférence thématique du CLUSIF du 10 avril 2014.

Aujourd'hui, toutes les entreprises et organisations, quel que soit leur secteur, utilisent les systèmes d'information pour accélérer et fiabiliser les processus de la chaîne de valeur. Et le bon déroulement de ces processus est bien entendu indispensable au fonctionnement de l'entreprise.

La contrepartie logique est que le mauvais fonctionnement du système d'information entraine inexorablement le ralentissement voire l'arrêt d'un ou plusieurs processus de l'entreprise, entrainant des conséquences comme la perte brute de chiffre d'affaire ou l'atteinte à l'image de marque.

C'est donc pour faire face à de vrais enjeux que les entreprises ont travaillé au développement de **Plans de Continuité, de Plans de Reprise d'Activité et de Plans de Gestion de Crise** (PCA, PRA et PGC). Au-delà de l'aspect informatique, partie le plus souvent bien prise en compte par les organisations, l'aspect humain dans les processus du PCA et de Gestion de Crise revêt une importance primordiale.

Fort de cet état des lieux, le CLUSIF a souhaité partager son expérience, en collaboration avec le Club de la Continuité d'Activité (CCA), lors de la conférence du 10 avril 2014. Six intervenants ont partagé leurs expertises et retours d'expérience : Lazaro PEJSACHOWICZ (CLUSIF), Nicolas de THORÉ (Club de la Continuité d'Activité – CCA), Stéphanie RUELLE (CCA), Thierry AUTRET (Groupement des Cartes Bancaires), François TÊTE (Devoteam), Vazrik MINASSIAN (Adenium) et, en animateur de la table ronde, Jean-Marc GREMY (CLUSIF).

Introduction par le CLUSIF – Par Lazaro PEJSACHOWICZ.

Lazaro PEJSACHOWICZ introduit la conférence par une illustration. L'une des filiales américaines du Crédit Lyonnais est installée au 51ème étage d'une des tours jumelles du World Trade Center de New York. Le 11 septembre 2001, suite à l'effondrement de la Tour, les locaux de l'entreprise sont alors détruits mais heureusement les utilisateurs ne sont pas touchés, ils n'étaient pas encore arrivés à leur bureau. Le SI de l'entreprise a redémarré dans un délai de trois jours et cette dernière disposait de positions de repli utilisateurs situées au 32ème étage d'une tour voisine. Or la psychose était telle que personne n'a voulu s'y rendre. L'entreprise avait un contrat permettant d'activer une cellule d'aide psychologique à ses équipes. Une semaine plus tard les utilisateurs étaient de nouveau à leur poste.

À travers ce cas, on constate que la gestion de crise est largement tributaire des facteurs humains et se doit donc de prévoir des situations de sinistres très variées et se former à résoudre en situation réelle de nombreux cas difficiles à anticiper.

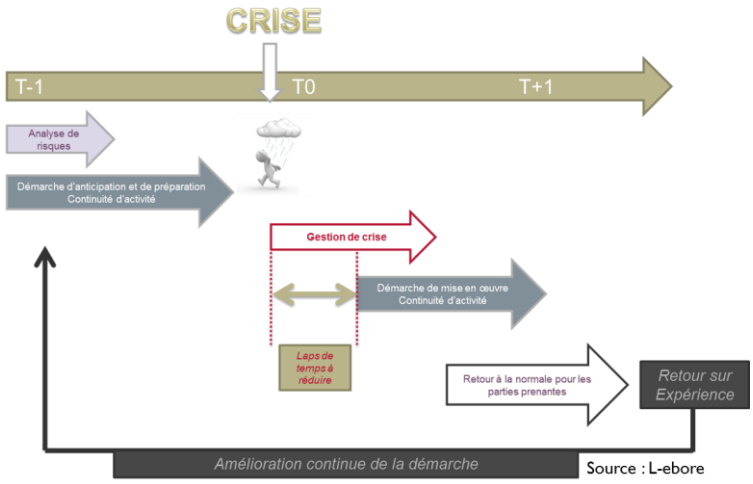
Présentation du Club de la Continuité d'Activité (CCA) – Par Nicolas de THORÉ

Le CCA compte à ce jour 150 membres : RSSI, RPCA, fonctions RH, juristes, chercheurs et prestataires. Le CCA poursuit trois objectifs : faire partager au sein de ses membres les bonnes pratiques et retours d'expériences, parfaire la maîtrise de chacun en termes de solutions, réglementation et normes et, en dernier lieu, leur permettre de développer une démarche pérenne dans leur entreprise.

Nicolas de THORÉ a rappelé les principaux livres blancs édités par le CCA : le lexique structuré de la continuité d'activité, PCA et RH - Guide de bonnes pratiques, PCA et PRA - Guide de bonnes pratiques et la traduction de la norme ISO 22301 pour l'AFNOR.

Panorama de retours d'expériences par le CCA – Stéphanie RUELLE et Nicolas de THORÉ

Tout d'abord, le lien entre la Continuité d'Activité et la gestion de crise tient avant tout aux facteurs humains et contextuels. Stéphanie RUELLE a illustré, par des exemples de gestion de crise, la nécessité de mettre en place des moyens de prévention du risque à froid. Le rôle du RPCA est d'anticiper, à froid les conséquences de la crise. C'est pour cela qu'il convient de mettre en place une gestion globale et transverse du risque.



Ensuite, la notion de passage en Crise et la définition du terme de Crise dépendent des hommes et du contexte dans laquelle celle-ci évolue. En situation de stress, chaque membre de la Cellule de Crise réagit en fonction de son vécu (son passé) mais aussi selon ses compétences. Pour une gestion de crise optimale il est approprié de veiller à la diversité des profils et des compétences qui constituent la Cellule de Crise. Concernant la gestion des astreintes, lorsqu'un incident majeur survient, l'enjeu fort est de comprendre les sujets, leur contexte humain et d'être sensibilisé sur le périmètre à couvrir. Un incident majeur se transforme très souvent en crise à cause des facteurs humains dans un contexte donné.

Enfin l'une des difficultés majeures à surmonter en gestion de crise est le déni des acteurs concernés. Les individus pensent surmonter ce qui au départ n'est qu'un incident majeur et se transforme par la suite en crise. Le déni, c'est la certitude que l'on va y arriver mais surtout la peur d'exprimer que l'on n'y arrivera finalement pas.

Pour conclure la session, Nicolas de THORÉ revient sur quatre exigences essentielles pour le RPCA : la première, traiter les risques de continuité de façon différenciée (par exemple la pandémie, l'indisponibilité du SI, l'indisponibilité métier) ; la seconde, être en phase avec la stratégie de couverture de risque et les priorités définies par la Direction Générale de l'entreprise ; la troisième, procéder au traitement des risques par étapes et en dernier lieu s'accorder avant tout sur la terminologie commune à utiliser au sein de l'entreprise.

L'implication des utilisateurs dans le PCA après plusieurs années d'exercice. Une réussite, toujours à confirmer – Thierry AUTRET

Après la description des enjeux métiers du Groupement des Cartes Bancaires, Thierry AUTRET rappelle le contexte des exercices du plan de continuité. L'entreprise n'a jamais activé son PCA, n'ayant pas eu de crise de disponibilité en trente ans d'existence.

L'intervenant met en avant les facteurs clés de réussite de son PCA et de l'exercice de repli utilisateur : le support de la Direction Générale, un correspondant PCA au sein de chaque Direction, la sensibilisation avant le test de l'ensemble des équipes par une formation (un mois avant l'exercice), une communication spécifique aux chefs de services, (cela permet de justifier le temps passé à la réalisation du test), un briefing la veille, puis enfin le débriefing le lendemain du test.

Le premier test a été vécu comme un « choc psychologique » par les équipes. Cela a été une véritable prise de conscience et un exercice très formateur pour le Groupement. Le test s'est déroulé comme suit : chaque utilisateur avait des tests à réaliser, pas à pas, dans son nouvel environnement de travail. Certaines applications ont été testées en conditions réelles de production.

Suite au test de repli, les équipes ont compris l'importance de la formalisation des procédures et ont été sensibilisées en vue du prochain exercice.

Le bilan est positif mais doit toujours être confirmé. Il faut éviter la routine et régulièrement sensibiliser la Direction Générale.

Certification PCA ISO 22301 en France : intérêt et bénéfices. – Vazrik MINASSIAN

Pour appuyer son propos, Vazrik MINASSIAN a présenté le retour d'expérience de la certification ISO 22301 de l'entreprise SOITEC (fabriquant de matériaux semi-conducteurs pour les marchés de l'électronique et de l'énergie). Comme souvent, le PCA a été mis en œuvre à l'occasion d'un nouveau contrat client (à l'époque, à l'aide la norme BS 25999).

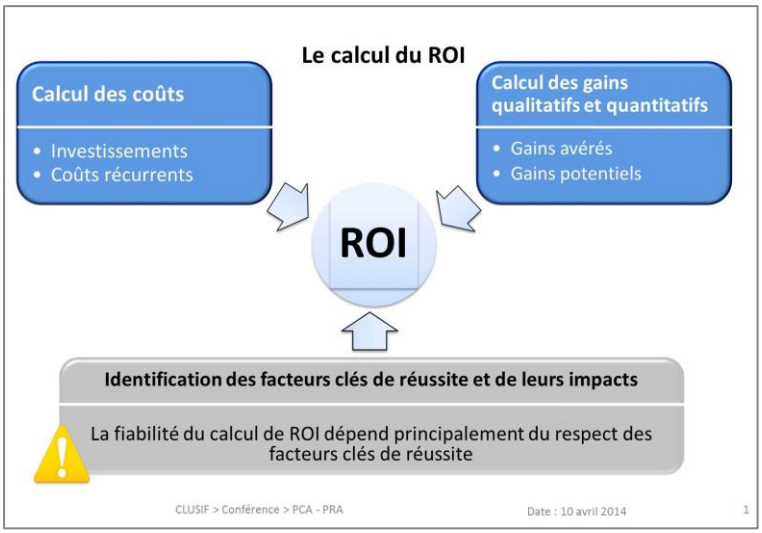
Tout d'abord grâce au Système de Management de la Continuité d'Activité (SMCA), le RPCA n'est plus isolé dans l'organisation. Le Plan de Continuité devient alors un outil de pilotage du changement.

L'avantage de la norme, pour une entreprise implantée mondialement, est de définir une terminologie commune à l'ensemble des équipes.

Dans une entreprise industrielle dans laquelle les certifications qualité et environnementales sont implémentées, la certification ISO 22301 a été grandement facilitée et prenait tout son sens au sein de la Direction de la Qualité.

Comment identifier la justification économique du PCA, peut-on parler de ROI ? – François TÊTE

Au cours de cette dernière intervention, François TÊTE a abordé la difficulté de parler de ROI quantifiable en termes de PCA. Parler de ROI va permettre de lister l'ensemble des gains pour une entreprise qui dispose d'un Plan de Continuité. Au-delà de la réduction des primes d'assurance, le PCA va en premier lieu réduire l'impact des risques de perte d'image de marque, de perte de production, de perte financière, de perte de productivité et de pénalités contractuelles. Ensuite, il permet à l'entreprise une meilleure productivité grâce à une meilleure connaissance des processus métiers. Le RPCA mettra aussi en avant les gains en termes d'augmentation de nouveaux marchés liés aux exigences des nouveaux clients en continuité.



Tous ces atouts sont des éléments clés permettant de convaincre les Directions Générales. En l'absence de sinistres nous pouvons aussi lister d'autres gains tels que l'ajustement des contrats de maintenance du SI (concernant en particulier les architectures actives/actives) ou l'utilisation des composants du SI à des fins de maintenance.

L'intervenant conclut sa présentation par la question : l'étude du ROI du PCA sert-elle à montrer que l'entreprise maitrise son budget ou bien démontrer que le PCA répond aux exigences des métiers en termes de couverture de risques ?

Table Ronde animée par Jean-Marc GREMY

Nicolas de THORÉ – CCA, Vazrik MINASSIAN - Adenium, François TÊTE - Devoteam, Thierry AUTRET - Groupement des Cartes Bancaires, Florian CARRIERE - Solucom et Jean-Marc GREMY (animateur de la table ronde) – CLUSIF.

Quelle est la contribution de l'informatique au PCA ?

Pour Florian CARRIÈRE il faut raisonner par les impacts plus que par les menaces. Il fait le constat que les organisations n'ont pas suffisamment confiance en leur plan de continuité au regard du budget que ces dernières y consacrent. L'enjeu est d'industrialiser le SI, transformer la production. On constate qu'il cohabite souvent trop de solutions de réplication de données au sein d'une même DSI. Le RSSI et le RPCA ont un rôle à jouer pour pousser à la transformation de la DSI.

Qui est la personne la mieux placée pour écrire le scenario de l'exercice de crise : le métier ?

Pour François TÊTE, la Direction des risques est la plus à même de choisir le scenario de crise. Mais, avant tout, il convient de bien différencier les tests de l'IT (PSI) de l'exercice de crise proprement dit. Il prend l'exemple de la crue centennale et qualifie ce scenario d'ultime car cela permet de tester l'ensemble des composants du dispositif de continuité.

Pour Thierry AUTRET les scenarii ne sont qu'un moyen de s'entrainer à gérer l'imprévu : il se produit ce que l'on n'a pas été en mesure de prévoir. Il souligne la difficulté de remonter le PSI suite à une cyber attaque. Il sera donc nécessaire, parfois, de faire appel à l'arbitrage du dirigeant concerné, pour établir l'équilibre entre besoin de continuité et contrainte de sécurité

Vazrik MINASSIAN met en avant les bénéfices de disposer d'une cellule de crise pluridisciplinaire et de bien distinguer le test du PSI du test PCA (par exemple l'indisponibilité des locaux). Il convient de tester les différents scenarii du PSI puis du PCA, de stabiliser chaque scenario puis d'envisager le test de la globalité du PCA en impliquant la Direction Générale de l'entreprise.

Les risques de cloud en termes de CA ? Effet domino ? Risques de sécurité ?

Les solutions de continuité utilisant le cloud peuvent apporter aux entreprisesl'opportunité de monter des plateformes de secours pour des reprises d'activité sous quelques jours à des coûts raisonnables. En revanche, pour une reprise en moins de quatre heures, il faut mettre en œuvre des solutions dédiées.