Allée de la Réflexion

AN 2000, J+180

Plans de continuité An 2000 : Comment s'en resservir ?

Ouf ! C'est fait. Le passage de l'an 2000 s'est effectué sans encombre. « Passage de non-Bug » diront certains. Et aujourd'hui de penser, les investissements n'ont-ils pas été surdimensionnés ? Et dans ce cadre, les plans de continuité ont-ils eu leur raison d'être ? Oui, si l'on a fait en sorte que les éléments du plan puissent être réutilisés.

Replaçons-nous six sept mois en arrière. Bon nombre de directions générales craignaient de voir les systèmes informatisés indisponibles, au point, dans certains cas, de mettre en péril la survie de leur entreprise. Par conséquent, la plupart d'entre elles ont su prendre les mesures adéquates par la conduite de processus (inventaires, changements, tests etc.) et par la mise en œuvre ***de plans de continuité***. Ces derniers ont, certes, coûté, mais ils pourront être réutilisés dans le futur, à condition toutefois d'avoir suivi la démarche convenable.

Avant tout concevoir un plan modulaire …

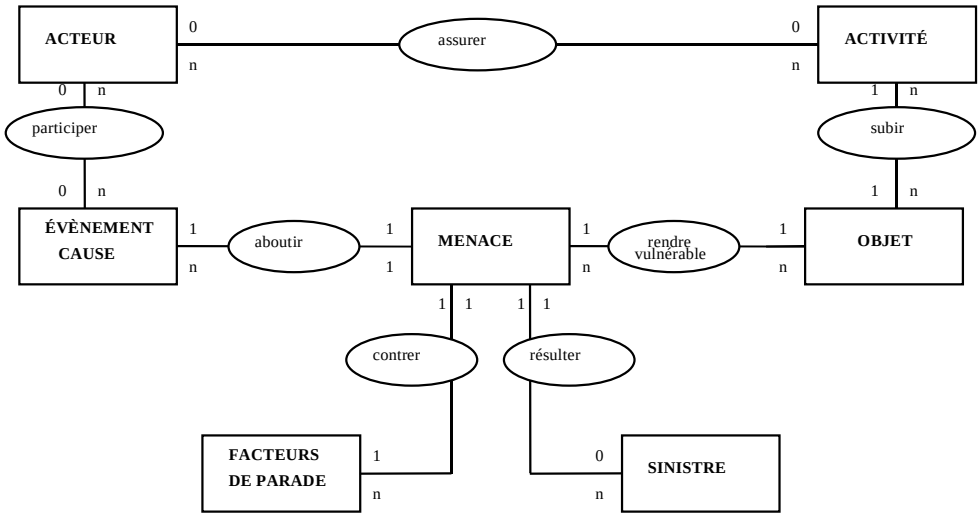
Un plan de continuité n'est pas un processus unique, mais une ***gamme de solutions à mettre en œuvre,*** compte tenu de la nature de l'incident qui survient. C'est pourquoi il est préférable de parler plutôt de modules exécutables, déclenchés à la suite d'un événement indésirable. C'est la nature de l'impact qui décide du type de plan de secours à mettre en œuvre. L'ensemble de ces modules constitue alors le ***plan de continuité*** de l'entreprise, dans la mesure où chacun d'entre eux a pour objectif de se porter garant de la continuité de service, face à la réalisation d'une menace spécifique***. Le plan de continuité est stable, mais il n'est qu'un canevas***. En revanche, les modules évolueront. Certains mourront, d'autres naîtront. L'entreprise vit. Ses composants changent, son environnement aussi avec les risques associés.

Mais, avant de bâtir un tel plan, il faut construire un référentiel définissant sa structure de fonctionnement.

Quelle doit être la constitution du référentiel ?

Penser mécanique du risque avant de construire le système

Avant de l'élaborer, il importe de bien comprendre ***ce à quoi il doit répondre***. En fait, il doit permettre la mise en place d'un système chargé de diminuer les risques. Or ces derniers sont issus d'une « mécanique » dont les composants pourraient être modélisés comme suit :



Ce modèle, présente les ressources (acteurs, activités, objets) faisant face aux éléments du risque. Quels sont-ils ?

Au centre se trouve la menace. Une menace est un **danger** engendré par un ou plusieurs événements et dont **la réalisation provoque un sinistre**. Ces événements peuvent survenir à tout moment ; de plus, l'apparition de certains d'entre eux n'est précédée d'aucun signe précurseur, ce qui les rend totalement imprévisibles donc indétectables.

La menace est permanente ; elle ne provoquera un sinistre, sur un objet, que si elle se déclenche. C'est pourquoi elle est ***indépendante du système***. Dans ces conditions, le risque est **la probabilité de voir une menace se réaliser** pour engendrer un sinistre. Le risque est plus une mesure, un résultat, qu'une entité en elle-même.

Cette probabilité est fonction de la menace, elle-même, et de la facilité avec laquelle un système peut être atteint, c'est à dire de la ***vulnérabilité***. Dans le modèle, elle est exprimée par la relation « Menace Objet ». De fait, il est clair que réduire les risques consiste à prendre des mesures pour diminuer la vulnérabilité de sa cible, afin de garantir la confidentialité, l'intégrité et la disponibilité du système d'information à protéger. Apparaissent donc deux grands axes, d'un côté celui des risques, de l'autre celui des parades avec pour enjeu, le patrimoine au centre. Il faut donc recenser les éléments qui constitueront le référentiel, et les classifier ensuite sur ces deux axes.

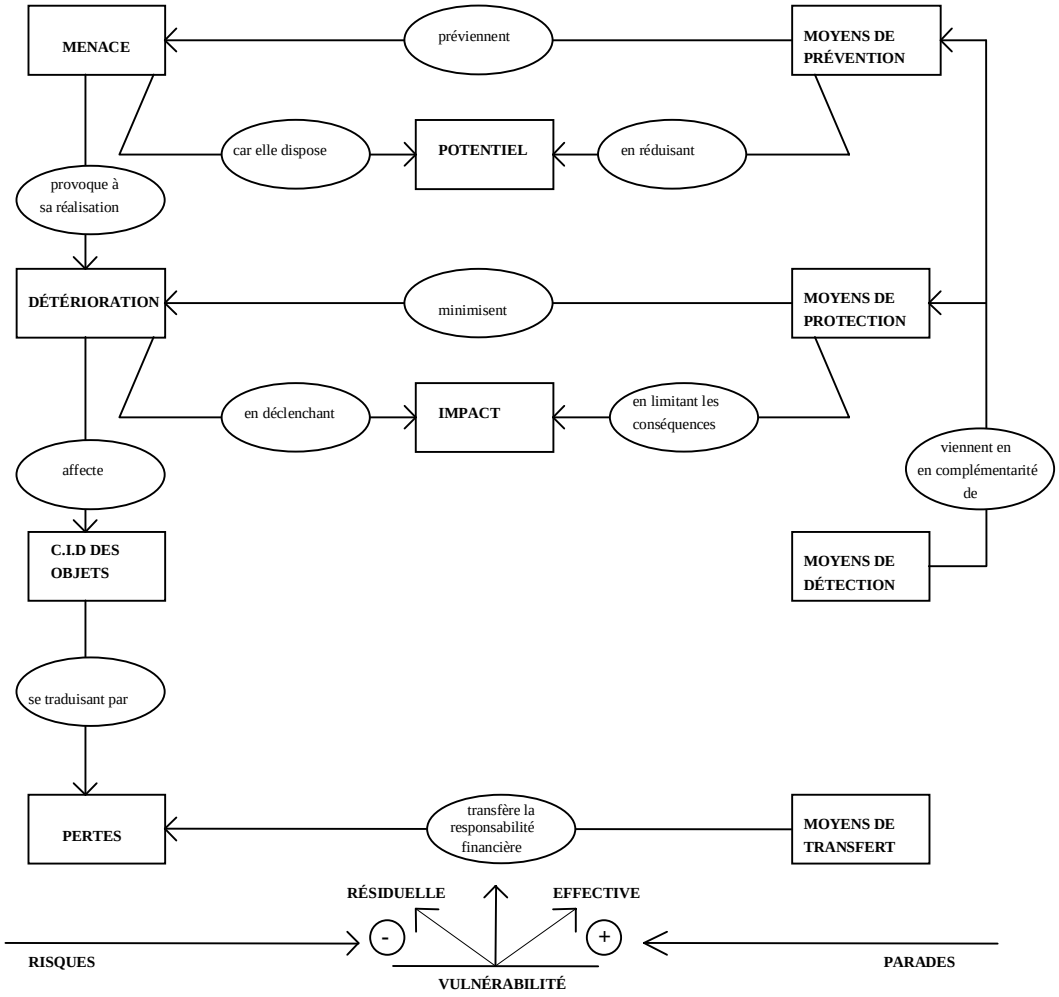
Classer les entités sur 2 axes

Définir les entités, supportant le référentiel, fournit un cadre de réception permettant de répertorier les agressions, d'évaluer l'impact sur le système et d'installer des parades pour les contrer. De ces parades, seront issus les processus constituant le plan de continuité.

L'identification des entités repose donc sur une double classification :

- celle des risques ;
- celle des parades.

Le modèle suivant en définit le principe. La partie gauche du schéma présente les entités qui constituent la classification des risques. Face à ces entités, correspondent des facteurs de parades, représentés sur la partie droite du schéma. Ce sont les moyens chargés d'agir non seulement sur les entités du risque mais plus précisément sur les éléments (situés au centre du schéma) destinés à évaluer l'importance du risque encouru.



Tout d'abord classer les risques selon leur dynamique

Les menaces

La menace exprime un danger permanent, ce qui ne veut pas dire qu'elle va obligatoirement se réaliser. Les différentes origines sont :

- l'environnement physique ;
- l'accident ;
- la malveillance ;
- l'environnement social.

Les dangers de l'environnement physique émanent de deux origines.

- La première origine regroupe les événements météorologiques exceptionnels (orages, pluies diluviennes etc.) et les phénomènes naturels tels que les catastrophes à caractère événementiel (tremblements de terre, crues, glissements de terrain etc..).
- La seconde identifie les agressions industrielles. Citons pour mémoire, les vibrations, les sectionnements de câbles lors de travaux d'un chantier public ou encore l'explosion dans un centre industriel.

Toutes ces agressions sont ***externes*** à l'entreprise.

L'accident peut avoir une origine humaine ou non. Il peut être de nature physique (il s'agit alors d'une ***panne***) ou logique (on parle, dans ce cas, ***d'erreur***). Les pannes sont diverses : court-circuit, fuite d'eau, erreur disque sur un ordinateur etc. Les erreurs peuvent émaner de la maladresse d'un individu

ou résulter des conséquences du déclenchement d'une panne. Elles se retrouvent souvent dans la conception, la réalisation et l'exploitation des applications informatiques.

Ce qui caractérise la malveillance, c'est l'***acte voulu*** et effectué par un individu pour détériorer volontairement une ressource. Il faut donc distinguer :

- le sabotage matériel ou immatériel ;
- le détournement. (logiciel, informations, fonds) ;
- le vol de matériels ;
- la violation d'accès.

Enfin, il ne faut pas oublier que des préjudices peuvent résulter de l'indisponibilité de telle ou telle catégorie du personnel. Les causes peuvent être diverses : grèves, départs imprévus, indisponibilités brutales etc..

Les détériorations

La détérioration n'est effective que si, et uniquement si, la menace s'est réalisée. En conséquence, la définition pourrait être la suivante « La détérioration est l'action ***consécutive à la réalisation d'une menace***, provoquant des ***dégâts*** qui causent un ***préjudice financier et moral***. ».

Concernant les détériorations, il est nécessaire de distinguer :

- l'altération, qui exprime le fait qu'un processus ou une information fournit un résultat différent de celui auquel on est en droit de s'attendre ;
- la dégradation, qui provoque une baisse des performances dans la réalisation ou l'exécution d'un processus ;
- l'endommagement d'une ressource, qui l'empêche provisoirement de fonctionner ;
- la destruction d'une ressource, qui implique sa reconstruction ou son remplacement ;
- l'utilisation parasite, qui met involontairement une information à la disposition d'un tiers.

À cela, il faut ajouter qu'une détérioration peut être ponctuelle, évolutive ou répétitive. Elle est :

- ponctuelle, lorsqu'il s'agit d'un acte unique et immédiat ;
- évolutive, lorsqu'elle s'étend naturellement ;
- répétitive, lorsqu'elle provoque des dégâts par occurrences successives.

L'impact C.I.D

À détérioration égale, le préjudice différera bien entendu, suivant les objets touchés. En effet, nous avions précédemment précisé que tout objet avait une valeur en terme de C.I.D, (Confidentialité, Intégrité, Disponibilité).

Aussi l'impact des menaces et détériorations peut-il se répartir de la façon suivante.

C.I.D	menaces type	détériorations
confidentialité	Détournement Vol Violation d'accès	Divulgation Utilisation parasite
intégrité	Accident (erreur) Sabotage Violation d'accès	Altération Endommagement Destruction
disponibilité	Accident (panne) Sabotage Violation d'accès	Dégradation Endommagement Destruction

La perte

Lorsqu'un sinistre est déclaré, l'entreprise doit accomplir des actions destinées à rétablir la situation initiale. Bien entendu, ceci engendre des coûts qui constituent le montant de la perte. La méthode MARION recense ces coûts de la façon suivante :

- le dommage matériel, qui correspond aux frais occasionnés par la réparation ou le remplacement du matériel ainsi que les frais annexes ;
- les frais supplémentaires, qui sont engendrés par la mise en œuvre de moyens spécifiques pour revenir à un état normal (exemple : le plan de secours) ;
- les pertes d'exploitation, qui se traduisent par une diminution de la marge brute de l'entreprise ;
- les pertes de fonds et de biens, qui correspondent à la disparition de biens financiers et de biens matériels en stock ;
- les autres pertes, qui correspondent à des frais divers.

À cela, il faut ajouter que toutes les pertes ne sont pas logées à la même enseigne.

En effet, rétablir une situation peut prendre un certain temps. En conséquence, entre le moment où sont constatés les dégâts et le retour à la normale, se déroule une période qui peut être segmentée en trois phases.

- La première phase voit la réalisation de la menace. La perte est directement issue de la détérioration. À ce stade, on constate les dégâts pour un certain montant permettant de répondre à la question : "*Pour combien dois-je m'assurer ?*".
- La deuxième phase correspond au temps de réparation. Seront pris en compte les frais engendrés pour reconstruire le système d'information.
- Enfin, la troisième phase marque le passage au retour « *officiel* » à une situation normale. Néanmoins, là encore certaines pertes peuvent être comptabilisées. Dans ce cas, elles résultent de dysfonctionnements.

Ainsi, les pertes peuvent être réparties de la façon suivante.

	DÉTÉRIORATION	**RÉPARATION**	**REPRISE**
DOMMAGE MATÉRIEL	Pertes de valeur Coûts d'expertise	Coûts de réparation Coûts de remplacement Coûts d'étude	
FRAIS		Coûts de transport Coûts de location Personnel de secours Agios Frais de restauration Primes et heures supplémentaires.	Frais de ressaisie Primes et heures supplémentaires.
PERTES D'EXPLOITATION	Perte clientèle Impact fournisseur	Perte clientèle Impact fournisseur Perte de C.A	Perte clientèle Impact fournisseur Perte de C.A
PERTES DE FONDS ET DE BIENS		Vente de titres Renouvellement du stock	Renouvellement du stock
AUTRES PERTES		Frais de justice	

Ensuite, classer les parades sur leur finalité

Les facteurs de parade se regroupent en quatre classes :

- Les moyens de prévention ;
- Les moyens de protection ;
- Les moyens de détection ;
- Les moyens de transfert.

Les moyens de prévention

Les moyens de prévention sont des mesures prises pour empêcher la réalisation ou l'aboutissement de toute menace. Ceci a pour conséquence, de ***diminuer la probabilité*** de voir un risque apparaître. Différents niveaux d'interventions sont nécessaires.

- Il est possible d'agir sur les ressources en les occultant, (pas de publicité) ou en évitant les reprises (redondance de matériel et logiciel).
- Des barrages techniques peuvent être mis en œuvre en bloquant les voies d'accès aux ressources (surélévation du centre, blindage, badges magnétiques etc.) ou en limitant les habilitations à certaines personnes par des systèmes de filtrage et d'identification.
- Des mesures de motivation et de meilleure connaissance des problèmes constitueront des éléments intégrés dans une politique du personnel adaptée (catégories de sujets), une campagne de sensibilisation et de formation, des conditions de travail correctes etc. Il est clair que le responsable de ressources humaines doit être impliqué dans ce type d'actions.

Néanmoins, les moyens de prévention ne suffisent pas, ils doivent être complétés par des moyens de protection.

Les moyens de protection

Les moyens de protection sont des mesures prises pour ***limiter l'ampleur d'un sinistre***, après la réalisation d'une menace. Dans ce cas l'objectif est d'en minimiser la gravité.

- Les mesures d'anti-propagation correspondent à un cordon sanitaire pour empêcher l'extension du sinistre. Peuvent être cités l'installation de portes coupe-feu et de fermetures automatiques de clapets de ventilation ; ou encore la mise en place de filtrage, destinés à vérifier l'état de cohérence des données avant diffusion de celles-ci.
- Le masquage de l'information se traduit par la mise en place d'une technique pour assurer la confidentialité des données transportées ; par exemple, le cryptage des messages sur un réseau.
- La certification des données permet de prendre des dispositions contre la perte ou l'altération des informations. Il faut s'assurer en particulier de l'authenticité de ces dernières en instaurant des droits d'utilisation et en pratiquant la redondance.
- La reconfiguration nécessite des moyens pour reconstituer le système d'informations qui n'est plus disponible en l'état. Ce genre d'action peut constituer un projet à part entière. C'est le cas typique du plan de secours.

Il est important de constater que tous ces éléments précités, constituent des garanties pour corriger, réparer, voire reconstruire des objets du système d'information.

Les moyens de détection.

Les moyens de détection complètent les deux précédents.

- Des mesures de motivation renforceront les actions de sensibilisation en montrant le risque réel encouru, et surtout ce qu'il implique, notamment du point de vue juridique.
- Des statistiques établiront la fréquence des incidents émanant des facteurs précédents, permettant ainsi d'entreprendre des actions pour bien localiser l'origine du problème. L'exemple peut être fourni par la fréquence d'invalidité d'un mot de passe, ce qui nécessite une recherche des conditions dans lesquelles ce dernier est désactivé.
- Des contrôles de cohérence, sans détecter obligatoirement l'origine du mal, permettent de confiner certaines informations afin de pouvoir confirmer leur validité.

- Des contrôles de charges suivent une évolution et déclenchent l'alerte lorsqu'un certain seuil est dépassé.

Concernant la détection, il serait opportun dans la classification des données, de réserver une classe spécifiant ce critère. Elle permettrait alors de répertorier dans le dictionnaire, tous les « *détecteurs* » pouvant se présenter sous la forme de ratios, de taux, de coefficients etc.

Les moyens de transfert

Les moyens de transfert sont des mesures cherchant à récupérer tout ou partie du montant du préjudice. En conséquence, il s'agit uniquement d'un transfert de responsabilité financière du risque sur des tiers. La plupart du temps, ces derniers sont représentés par les assurances.

Néanmoins, il faut signaler que l'action en justice permet de récupérer une partie des pertes, à condition toutefois que le dossier soit solide.

Enfin, évaluer la confrontation Risque Parade

Jusqu'à présent, nous avions présenté une classification des risques, et face à cette dernière nous avions établi une autre classification, celle des parades. Or, il est clair que les risques n'ont pas tous la même importance ; pour la simple raison que les menaces sont plus ou moins probables, et les détériorations, plus ou moins graves. Il faudra donc établir des mesures en rapport avec le risque encouru.

Pour ce faire, il est nécessaire de prendre en compte les éléments suivants :

- le potentiel de la menace ;
- l'impact de la détérioration.

Le potentiel

Le potentiel de la menace exprime le caractère plus ou moins plausible d'une agression susceptible de provoquer une détérioration. Son évaluation repose sur trois facteurs.

Nous distinguerons donc :

- Le niveau de perception du risque par l'agresseur qui ne mesure pas toujours l'importance des conséquences de son acte. Il y a véritablement une différence entre le risque perçu et le risque réel.
- L'ampleur des moyens d'évaluation de la capacité de réalisation d'une menace. Cette capacité peut avoir pour origine un niveau d'expertise, élevé de la part des acteurs ou bien un environnement géographique peu sûr.
- Enfin, l'exposition des ressources, pour lesquelles il est nécessaire de connaître l'attrait qu'elles représentent. Pour cela, il faut distinguer l'enjeu qui détermine l'avantage que peut avoir tel ou tel objet et le niveau de ciblage de l'entreprise vis-à-vis de ses concurrents. Est-elle la seule à avoir un objet privilégié ou est-elle une cible parmi tant d'autres ? Autrement dit, comment être en sécurité parmi ses voisins.

L'impact

L'impact mesure les conséquences d'une détérioration des objets. Tout comme la vulnérabilité, l'impact est intégral en dehors de toute mesure de protection. Il devient résiduel dans le cas contraire. Dès lors, l'objet est considéré en « état protégé ».

Profiter des projets Y2K pour établir le référentiel

À quoi ont servi les investissements des projets Y2K ?

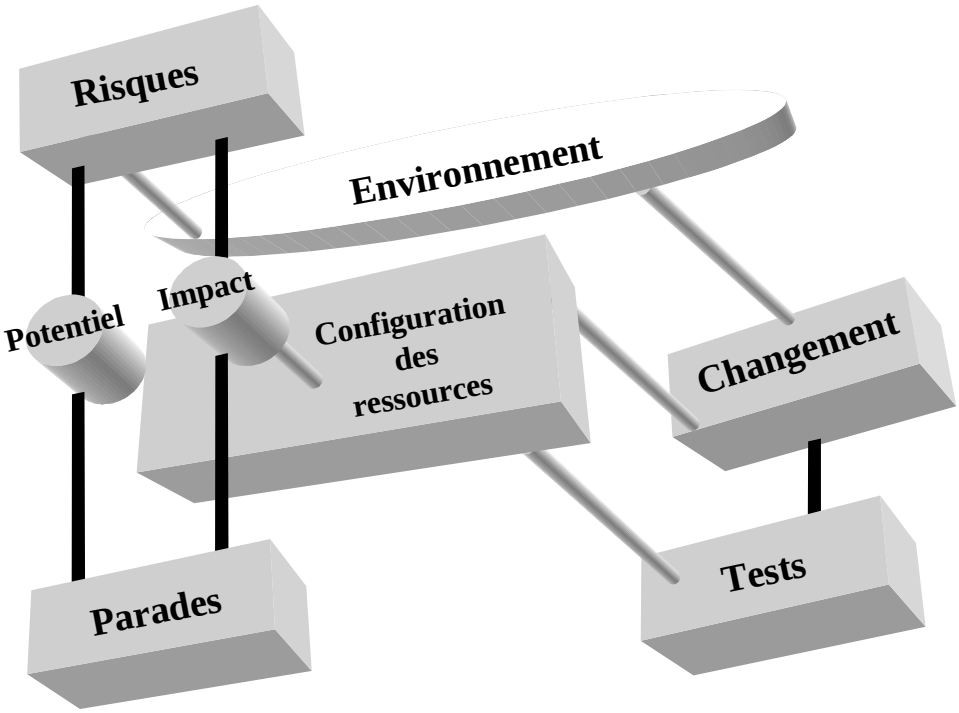
Globalement, à remettre à niveau l'état du patrimoine.

Mais dans le patrimoine, il faut non seulement inclure les objets, en tant que ressources matérielles et logicielles, mais aussi leur état de qualification et de protection. Il faut garantir le bon fonctionnement et la non altération du système traité.

Par conséquent, la gestion du référentiel composé de tous les éléments précédemment décrits, n'a de véritable efficacité que si elle fonctionne en adéquation avec :

- la gestion de configuration ;
- la gestion de changement ;
- la gestion des tests ;

Et ce comme suit :



Cette vision (très globale) présente le principe de fonctionnement. En y regardant bien, ce schéma fait apparaître deux éléments majeurs.

Tout d'abord, il met en valeur trois volets, chacun d'entre eux ayant une finalité bien précise.

> Le premier volet est représenté par la relation triangulaire gestion de configuration (ressources), gestion de changement, gestion de qualification (tests). Dès lors qu'il y a changement, les objets le subissant doivent être confinés comme étant en état d'évolution. Ensuite les tests qualifient les objets. La finalité est dans ce cas de garantir l'aptitude des ressources au bon fonctionnement.
>
> Le deuxième volet fait suite au premier. Il regroupe tous les concepts venant d'être décrits (risques, parades). Il s'agit alors d'établir l'impact du changement sur le plan de continuité. Objectif : garantir l'état de protection des ressources.
>
> Mais cette garantie, n'est effective que si les menaces ont été revues en fonction de l'environnement. C'est le troisième volet établissant l'impact du changement sur ce dernier afin de faire évoluer la nature des menaces. Cela doit se faire dans le cadre d'une étude de potentialité.

Ensuite, le schéma met en évidence un processus où tous les éléments de sécurité sont inclus dans un cycle récurrent. Dès lors, il est possible de voir un plan de continuité évoluer avec les changements, à

condition toutefois que le ***référentiel soit formalisé*** et que ***les règles de fonctionnement soient établies***.

De manière générale, les projets Y2K ont couvert ce cycle. Profiter du projet Y2K pour consolider une activité récurrente ne peut être que bénéfique.

À titre indicatif, le tableau suivant y établit les liens :

Cycle		Y 2 K	
SCHÉMA	PROCESSUS	ACTIONS	RÉSULTATS
Ressources	Gestion de configuration	Plan d'inventaire.	Dossiers d'inventaires
Changement	Gestion des changements	Plan de déploiement	Dossiers de suivi. Comptes rendus de suivi.
Test	Gestion de qualification	Plan de test	Protocoles CR de synthèse.
Risques /Parades.	Gestion de secours	Plan de continuité	Procédures dégradées.

Mais penser aussi que le référentiel est incomplet

Construire un référentiel pour supporter le plan de continuité permet de mettre celui-ci sur des rails, afin d'encadrer et de garantir son évolution. Mais le faire dans le cadre du projet Y2K, c'est aussi se limiter au champ d'actions lié à la problématique Y2K.

Toute menace découle d'un ou de plusieurs événements. Tout événement peut avoir plusieurs origines. Concernant notre sujet, l'origine qui prime est avant tout celle de l'accident technologique. A priori, sont exclus du champ d'autres événements tel que la catastrophe naturelle ou la malveillance. Par conséquent, maintenant que l'an 2000 est passé, et que le périmètre de survie de l'entreprise est identifié par le plan de continuité Y2K, il faut penser à ***compléter le référentiel***, pour répondre ***à l'ensemble des risques encourus***.

Pour conclure

Tout au long de notre réflexion, nous avons surtout cherché à présenter les concepts d'une structure permettant de supporter un plan de continuité. Dans ce domaine, nous savons qu'il n'existe pas de solution unique, car tout système doit être ***adapté à son contexte***. Cependant, il importe d'intégrer cette notion dans ***une dimension récurrente*** pour ne pas se limiter à l'exécution d'un plan de secours une fois l'an, où des écarts dus aux évolutions sont constatés après coup.

Y2K était une menace prévisible dans sa date d'exécution. Par conséquent, chaque entreprise s'y est préparée. Mais cette situation est exceptionnelle. Exceptionnelle, car toute menace se réalise toujours inopinément et de fait déclenche un effet de surprise. Avoir profité de l'an 2000 pour concevoir le plan de continuité avec son référentiel est louable. Mais intégrer la menace Y2K dans ***un référentiel déjà existant*** est plus pertinent. Cela permet de faire évoluer un plan de continuité (déjà testé pour d'autres situations) à ce nouvel événement***, tout en répondant à la problématique du risque dans sa globalité***. Pensons à cette société en Charente maritime qui a dû appliquer son plan de secours non pas en réponse au « BOGUE AN 2000 » mais tout simplement parce que son centre informatique avait été inondé par la tempête de fin décembre.

Sur cet exemple, puissent les entreprises ***intégrer cette dimension dans leurs forces vives !***

Pour approfondir la réflexion

D. GUINIER - Novembre 1991 - Sécurité et qualité des systèmes d'information Approche systémique - Éditions MASSON.

Cet ouvrage aborde la sécurité des systèmes d'information de l'entreprise, sous l'angle de l'analyse des systèmes et des processus. Y sont développés les problèmes, les méthodes et les solutions, le tout étayé par des études de cas.

J.P. JOUAS – A. HARARI – J.M. LAMERE – J. TOURLY - Septembre 1992 - Le risque informatique - Éditions d'organisation.

L'intérêt réside dans le travail de modélisation des risques. Le présent article s'est inspiré de cet ouvrage pour la classification et plus précisément l'évaluation du risque (potentialité et impact).

ISO 13 335 – Information technology – Guidelines for the management of IT Security 1996 - 1998.

Cette norme a une approche plus globale. Elle ne fait pas la distinction entre les mesures de prévention et de protection, ni entre l'impact et la potentialité. Elle se positionne sur le principe que les parades protègent des menaces afin de réduire les risques. Ces menaces exploitent les vulnérabilités des ressources qui ont une valeur potentielle en terme d'impact sur les activités de l'entreprise. Les liens entre le management de la sécurité et la gestion de configuration et la gestion des changements y sont clairement exprimés.

ADELI-IQSL - 1997 - Le PÉRILoscope 97 - Maîtriser les risques des projets informatiques

Voici une étude qui s'adresse plus particulièrement aux praticiens. À partir de la norme précédente, cet ouvrage, disponible auprès d'ADELI, propose une démarche rigoureuse pour identifier, maîtriser et gérer les risques, dans le cadre d'un projet de développement. Il est accompagné d'un recueil pratique très complet des ***techniques*** *et* ***des outils de management*** *des risques.*

Laurent HANAUD
Membre du comité d'ADELI