

Globalement, on rencontre trois situations.

1. L'entreprise est capable de citer ses activités les plus critiques et d'indiquer à quoi celles-ci correspondent dans son organisation, ses implantations géographiques et les moyens dédiés à leur réalisation : c'est un cas relativement idéal. La description, en revanche, n'est peut-être pas modélisée à l'aide d'outils appropriés ni avec rigueur, mais c'est un point de départ utile pour l'analyse d'impact.
2. L'entreprise présente ses activités de manière simple et succincte. Elle a réalisé un premier niveau d'organigramme indiquant qui est responsable de quelle activité. En revanche, il n'existe aucune liste de ce qui pourrait être critique dans ses activités, ni aucune indication de moyens ou de site. Pour commencer l'analyse d'impact, on s'adressera donc aux responsables désignés.
3. L'entreprise a réalisé une étude approfondie dite « analyse de processus » avec des outils et une formalisation forte. Malheureusement, ces processus sont souvent transversaux à son organisation et il n'est pas toujours aisé de savoir quels sont les moyens impliqués et les responsables. La vision « activité » et la vision « processus » pouvant être totalement indépendantes l'une de l'autre, il faudra obtenir, pour une bonne analyse d'impact, une vision commune entre les responsables de processus et les responsables de départements ou services.

Concernant tous ces aspects, le document de « politique de continuité » (voir le chapitre 12) se révèle d'un grand secours. C'est lui qui doit indiquer par quel côté le problème doit être abordé.

À la fin de l'analyse d'impact (BIA), on obtient ainsi en résultat une liste des activités les plus critiques de l'entreprise.

### **Activités, fonctions, processus... : le piège du vocabulaire**

Une remarque importante ici : le vocabulaire peut être source de confusion. On parlera indifféremment dans les entreprises « d'activités », de « fonctions », de « processus », voire de *process* (en anglais) avec des significations et des hiérarchies variables.

Dans le cadre de la continuité d'activité, il faut rechercher un niveau de découpage raisonnable de l'entreprise, qui doit être regardée comme un tout autonome face au sinistre. On préférera ainsi raisonner par responsable, par département ou par groupe de moyens.

Il faut remarquer ici que les entreprises qui ont une certification qualité (type ISO 9000) sont souvent bien préparées pour mener des analyses d'impact, car il est en général aisé d'y trouver des responsables pour les entretiens et le découpage réalisé est viable.

### **Identifier les activités**

Il est possible de découper les activités de l'entreprise en plusieurs niveaux. L'exemple qui suit montre un découpage en deux niveaux : fonctions et processus. Le tableau indique en plus si le processus mérite d'être étudié ou non, c'est-à-dire qu'il est porté un premier jugement sur les candidats au titre de processus critique.

Pour chacune de ces fonctions et processus, on indique s'il faut étudier ou non l'impact d'un sinistre éventuel. Pour remplir ce tableau, il est conseillé de faire

appel aux directeurs d'activités (*business owners*) ou aux responsables de processus (*process owners*). Il est également préférable de limiter le nombre de niveaux de découpage à une proportion raisonnable.

Tableau 1-1 : Exemples de fonctions et processus d'une entreprise

Fonction	Processus	À étudier ?
Vente	Prise de commandes	Oui
	Reporting	Oui
	Gestion d'échantillons	Non
Marketing	Promotions	Non
	Gestion du catalogue	Oui
	Gestion des salons	Non
	Gestion des partenaires	Oui
Logistique	Réception des livraisons	Oui
	Organisation des expéditions	Oui
	Gestion du stock	Oui

Ce n'est qu'une fois ces choix effectués qu'on pourra estimer les impacts d'un sinistre.

### Estimer les impacts financiers et opérationnels

Les impacts financiers se chiffrent en euros ou par une mesure qualitative échelonnée telle que « nul/faible/moyen/fort » ou notée de 0 à 3, etc., de manière comparable à ce qui a été présenté dans le premier chapitre.

Les pertes financières sont en général données par jour. Il est important de conserver le même type de mesure pour tous les processus étudiés, de manière à pouvoir établir des comparaisons.

Tableau 2-2 : Estimation des pertes pour l'exemple précédent

Fonction	Processus	Perte par jour
Vente	Prise de commandes	600 000 €
	Reporting	60 000 €
Marketing	Gestion du catalogue	500 000 €
	Gestion des partenaires	300 000 €
Logistique	Réception des livraisons	100 000 €
	Organisation des expéditions	200 000 €
	Gestion du stock	50 000 €

Concernant l'impact opérationnel, il vaut mieux d'abord élaborer une grille d'analyse avant d'interroger les responsables d'activités. Cette grille, qui pourra évoluer par la suite en fonction des discussions, abordera par exemple les aspects suivants :

- les problèmes de flux de trésorerie, de mouvements de fonds, les questions logistiques ;
- la perte de confiance des partenaires (clients, investisseurs...) ;
- la dégradation de l'image de l'entreprise ;
- la démoralisation du personnel ;
- les sinistres chez des revendeurs ;
- les violations réglementaires inévitables (déclarations obligatoires devenues impossibles, etc.).

*Tableau 2-3 : Évaluation des impacts opérationnels sur trois aspects*

			Impact de la perte : 0 (nul) à 5 (très fort)		
Fonction	Processus	Perte par jour	Logistique	Image	Revendeurs
Vente	Prise de commandes	600 000 €	3	5	0
	Reporting	60 000 €	0	0	0
Marketing	Gestion du catalogue	500 000 €	2	3	3
	Gestion des partenaires	300 000 €	3	2	5
Logistique	Réception des livraisons	100 000 €	5	2	2
	Organisation des expéditions	200 000€	5	3	3
	Gestion du stock	50 000 €	3	2	4

Une certaine pratique consiste à faire évaluer les critères en aveugle par différentes personnes. Il est aussi possible de confier cette évaluation à un expert externe. Plusieurs approches peuvent donc être adoptées, en retenant *in fine* les moyennes entre les différentes approches, par exemple, et en se faisant expliquer les gros écarts d'évaluation si on en constate.

### Identifier les processus critiques

Pour établir un classement final et en déduire les processus critiques, plusieurs possibilités existent. Sur l'exemple précédent, il est possible d'opérer comme suit :

1. transformer l'évaluation de la perte par jour en un chiffrage échelonné de 0 à 5 ;

2. affecter à chaque colonne une pondération, telle que :
- un poids double pour les pertes financières et la dégradation de l'image ;
  - un poids simple pour les problèmes de logistique et ceux concernant les revendeurs.

On obtient ainsi une note finale, qui permet de classer les processus en fonction de leur degré critique.

Tableau 2-4 : Évaluation des processus en fonction de leur degré critique

Fonction	Processus	Impact de la perte : 0 (nul) à 5 (très fort)				Note finale
		Perte par jour	Logistique	Image	Revendeurs	
Vente	Prise de commandes	5	3	5	0	23
	Reporting	1	0	0	0	2
Marketing	Gestion du catalogue	4	2	3	3	19
	Gestion des partenaires	3	3	2	5	18
Logistique	Réception des livraisons	1	5	2	2	13
	Organisation des expéditions	2	5	3	3	18
	Gestion du stock	0	3	2	4	11
<b>Coefficient retenu</b>		2	1	2	1	

Dans ce tableau, on peut ainsi sélectionner, d'après leur note finale, les processus suivants comme étant les plus critiques :

- Vente : prise de commandes (23) ;
- Marketing : gestion du catalogue (19) ;
- Marketing : gestion des partenaires (18) ;
- Logistique : organisation des expéditions (18).

Ce type d'approche nécessite bien entendu plusieurs itérations entre les différents responsables concernés pour arriver à une vision partagée. En général, le tableau d'évaluation de l'impact est rempli avec l'aide des personnes suivantes :

- les colonnes relatives à l'impact de la perte sont évaluées par les opérationnels ;
- les poids (ou coefficients) sont fixés par la direction générale.

Par ailleurs, il est aussi possible de procéder en établissant des règles de sélection des processus critiques du type de celles présentées ci-après. Sera ainsi retenu comme critique :

- tout processus ayant un 5 dans une colonne d'impact ;
- tout processus comportant deux 4, etc.

La méthode de détermination des processus critiques peut faire l'objet d'un point de la note de cadrage (voir en fin de chapitre).

Surtout, il est important que la règle ait bien été discutée entre tous les responsables concernés, car chacun a tendance à considérer spontanément que c'est son processus qui est le plus critique.

L'établissement de règles admises par tous est un préalable nécessaire si on veut éviter les tensions lors des réunions de présentation des résultats des analyses d'impact réalisées. Idéalement, ce point devrait être abordé, au moins dans ses grandes lignes, dans la politique de continuité (voir chapitre 12).

À la fin de l'analyse, on dispose d'une liste des activités, fonctions et processus critiques, c'est-à-dire dont la perte éventuelle affecterait le plus l'entreprise.

### Déterminer les configurations

---

Une fois les processus critiques déterminés dans l'entreprise, il convient d'établir, pour chacun d'entre eux, les points suivants :

- la durée maximale tolérable d'interruption de l'activité (MTD) et les priorités pour les actions de reprise ;
- les éléments critiques dans le domaine de l'informatique ;
- les autres éléments critiques.

Ces éléments connus, il sera alors possible d'en déduire les contraintes qui portent sur eux. Cela servira pour les choix techniques (voir partie III) et pour l'élaboration du plan de reprise (voir partie II).

### MTD et priorités

Il s'agit de déterminer, pour les processus critiques sélectionnés précédemment, le temps maximal durant lesquels ils peuvent être interrompus : le MTD (*Maximum Tolerable Downtime*).

Cette durée pourra être évaluée en fonction de la perte financière, par exemple : plus la perte est forte, plus la durée devra être faible. Il est également possible de procéder à une évaluation à partir des impacts estimés (échelonnés par exemple de 0 à 5). Des exemples sont fournis dans les tableaux page suivante.

#### Remarque

Sur le tableau 2-6 on notera que le temps maximal d'interruption admissible est donné en jours et que le processus le plus critique ne doit pas s'interrompre plus d'une demi-journée.

L'établissement de priorités est utile pour réaliser un arbitrage durant le plan de reprise : il s'agit de décider quel processus sera relancé avant quel autre.

Il apparaît par ailleurs que la priorité ne suit pas tout à fait la hiérarchie des MTD :

- L'organisation des expéditions a une priorité de 1, alors que son MTD la place en seconde position. Cela s'explique par le fait que, d'un point de vue opérationnel, la reprise des autres processus dépend du bon redémarrage de celui-ci.
- Il en va de même de l'expertise niveau 1, dont la priorité est fixée juste après celle de la hotline.

Tableau 2-5 : Évaluation des processus critiques sélectionnés

Fonction	Processus	Impact de la perte : 0 (nul) à 5 (très fort)				Note finale
		Perte par jour	Logistique	Image	Revendeurs	
Vente	Prise de commandes	5	3	5	0	23
Marketing	Gestion du catalogue	4	2	3	3	19
	Gestion des partenaires	3	3	2	5	18
Logistique	Organisation des expéditions	2	5	3	3	18
Support client	Hotline	1	2	5	3	17
	Expertise Niveau 1	1	2	4	5	17
Paiement	Couplage carte bancaire	4	1	4	1	18
	Couplage VAD (vérification avant départ)	3	1	3	3	16
<b>Coefficient</b>		<b>2</b>	<b>1</b>	<b>2</b>	<b>1</b>	

Tableau 2-6 : Évaluation en termes de MTD et de priorités de reprise

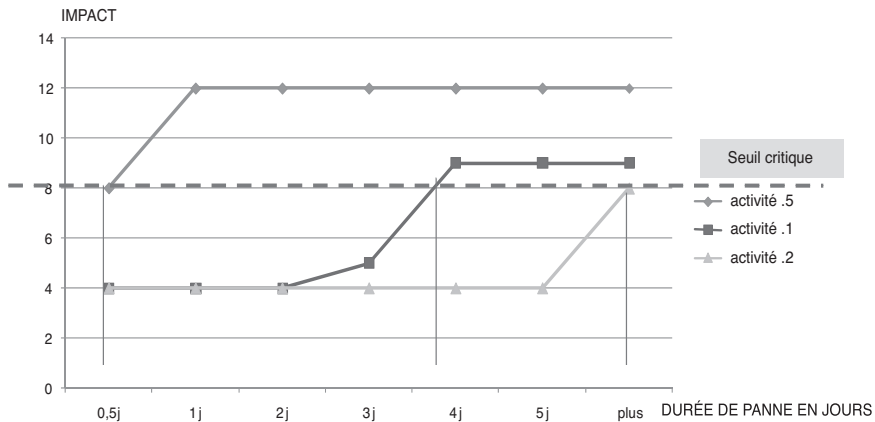
Fonction	Processus	Gravité : 0 (nulle) à 30 (très forte)		
		Gravité	MTD (en jours)	Ordre de priorité
Vente	Prise de commandes	23	0,5	1
Marketing	Gestion du catalogue	19	1	2
	Gestion des partenaires	18	1	2
Logistique	Organisation des expéditions	18	1	1
Support client	Hotline	17	2	2
	Expertise Niveau 1	17	2	3
Paiement	Couplage carte bancaire	18	1	2
	Couplage VAD (vérification avant départ)	16	3	4

De même, dans le cas de cette société, la perte de la hotline peut sembler peu importante ou sous-estimée (impact évalué à 17 sur 30). Cela tient au fait que les clients ont aussi l'alternative de se tourner vers un revendeur. Cet exemple montre donc bien qu'il ne faut surtout pas perdre de vue la réalité opérationnelle.

### Le facteur temps

Il arrive très souvent qu'en cours d'analyse d'impact sur les activités, le responsable interrogé ne puisse évaluer l'impact « dans l'absolu » de la perte de tel processus et pose la question de la durée de la perte à considérer.

Bien évidemment, tel arrêt supportable durant une heure devient intolérable s'il dépasse deux jours... Dans ces cas là, il est intéressant de faire remplir des tableaux qui prennent le facteur temps en compte (voir les schémas ci-après). Ces tableaux, une fois remplis, font apparaître l'augmentation de la « douleur » avec la durée de la panne et permettent de définir un seuil critique qui donne le MTD.



Avec la durée de la panne, l'impact monte plus ou moins vite.

Figure 2-3 : Impact de la durée de la panne

Processus Entité	Durée d'arrêt	Impact évalué				DMIA <sup>1</sup>
		Financier	Image	Contrat	Règlement	
Gérer la relation client	< 1 h	1	1	1	1	1 jour
	De 1 h à 4 h	2	2	2	2	
	De 4 h à 1 jour	3	3	3	3	
	> 1 jour	3	3	3	3	
Réclamation client	< 0,5 h	2	2	2	3	1 h
	De 0,5 h à 1 h	3	3	3	3	
	> 1 h	3	3	3	3	
Gérer le recouvrement client	< 2 jours	1	1	1	1	5 jours
	De 2 à 3 jours	2	2	2	2	
	De 3 à 5 jours	3	3	3	3	
	> 5 jours	3	3	3	3	
Rétablissement client sous 24 heures	< 2 h	1	1	1	1	1 jour
	De 2 h à 4 h	2	2	2	2	
	De 4 h à 1 jour	3	3	3	3	
Gérer les ventes en ligne	< 3 jours	2	2	2	2	4 jours
	De 3 à 4 jours	3	3	3	3	

1. Délai maximum d'interruption admissible.

### Systemes et applications informatiques critiques

On cherche maintenant à déterminer la correspondance entre les processus critiques et les applications et moyens informatiques. De manière évidente, les applications informatiques qui soutiennent les processus critiques deviennent elles-mêmes critiques à partir du moment où leur indisponibilité oblige le processus à s'arrêter ou à recourir à des procédures manuelles.

Le tableau suivant, qui mentionne les éléments critiques principaux, illustre cela par l'exemple : cela concerne aussi bien une application informatique particulière qu'une connexion réseau ou un plateau de téléphonie.

Il est ici important de faire preuve de pragmatisme. En effet, il ne sert à rien d'entrer dans les détails de quinze applications différentes si toutes ces applications subissent le même sort en termes de disponibilité (si elles sont, par exemple, installées sur la même machine). Il faut alors raisonner par groupe d'applications.

*Tableau 2-8 : Exemples de systèmes et applications critiques*

Fonction	Processus	Applications et systèmes critiques
Vente	Prise de commandes	Téléphonie Application <i>Vador</i> sur Unix, site de Lyon
Marketing	Gestion du catalogue	Serveurs web de gestion du catalogue, site de Lyon et hébergeur
	Gestion des partenaires	Application <i>Agépar</i> sur mainframe, site de Paris
Logistique	Organisation des expéditions	Logiciel SAP S&D Couplage avec logistique Infodis
Support client	Hotline	Centre d'appels, site de Paris
	Expertise niveau 1	Plateau téléphonique, site de Lyon
Paiement	Couplage carte bancaire	Accès au système d'autorisation
	Couplage VAD (vente à distance)	Accès à la VAD et programme VAD

Les services informatiques ont par ailleurs probablement mis au point des configurations par « service » (au sens de service à l'utilisateur), avec un niveau de finesse variable. Les contraintes de service seront alors appliquées à tout cet ensemble.

D'autre part, la réflexion doit tenir compte des deux grandes tendances suivantes :

- Avec les évolutions des réseaux ou des grilles de calcul ces dernières années, il est fortement conseillé de noter la situation géographique des moyens techniques lorsque celle-ci n'est pas la même pour tous. Il n'est pas certain, en effet, que le serveur HTTP (accueil), le serveur web et le serveur de bases de données se trouvent dans la même salle ou sur le même site.
- La virtualisation des serveurs a conduit à procéder à des regroupements sur les mêmes machines physiques, au sein de partitions dans de gros serveurs. C'est la tendance inverse de la précédente. Ce regroupement a donc des effets sur la criticité : si une application dans le lot est critique, le serveur (au minimum) le sera aussi.

Enfin, certains systèmes sont bien évidemment utilisés par tous, comme :

- les PC et imprimantes (partagées ou non) ;
- la messagerie d'entreprise (Notes, Exchange, etc.) ;
- les réseaux locaux d'échanges et de partage ;
- les serveurs de stockage de type NAS (*network-attached storage*), de partage de fichiers ou les extensions de disques ;

- les télécopieurs ou le couplage à la télécopie, etc.

Ces systèmes généraux nécessitent une prise en compte spéciale, car non affectée à une activité ou un processus particulier (voir le chapitre 4). Leur degré de criticité sera différent en fonction de la possibilité de substitution (utilisation d'un PC de secours gardé en réserve) ou non (le serveur de courriels est perdu ou inaccessible).

### Ressources humaines et autres ressources critiques

L'apparition d'une pandémie grippale a récemment mis en lumière l'importance des ressources humaines qui sont bien entendu à considérer dans l'analyse.

Il pourra être intéressant d'en faire une liste particulière prenant en compte les compétences lorsqu'un phénomène rare peut survenir, et tout particulièrement en cas de pandémie (voir chapitre 11).

Enfin, il convient de lister également les autres ressources nécessaires au bon fonctionnement des processus critiques et souvent associées aux ressources humaines.

On pourra ainsi passer en revue des éléments tels que :

- les locaux informatiques et industriels ;
- les bureaux ;
- les équipements de production (machines-outils) ;
- les matières premières ;
- le mobilier de bureau ;
- les télécopieurs, imprimantes et photocopieurs ;
- les équipements de sécurité ;
- les équipements de télécommunication (autocoms, etc.) ;
- les outils et pièces de maintenance ;
- les documents critiques ;
- les archives papiers ;
- les fournitures de bureaux.

La tâche de définir la liste des moyens indispensables pour travailler incombe aux responsables d'activités ou de processus. Cette liste devra contenir un descriptif de chaque élément et un recensement des quantités.

### Déterminer les paramètres de reprise

---

Pour chaque groupe d'applications et de systèmes qui correspondent à des activités critiques, on détermine ensuite les paramètres de reprise. Ceux-ci sont au nombre de trois : RTO, RPO et WRT, tels que définis précédemment.

Dans les sigles précédents, la lettre O signifie « objectif » : il faut donc se souvenir que ces durées sont des valeurs cibles à atteindre et qu'avant de les fixer il faut être réaliste, car elles seront contraignantes. Cela nécessitera plusieurs

allers et retours entre les responsables d'activités et le service informatique pour aboutir à des chiffres viables.

*Tableau 2-9 : Inventaire des ressources critiques*

Fonction	Processus	Matériel	Ressources critiques
Vente	Prise de commandes	Téléphonie	6 téléphones avec messagerie vocale, mise en attente et routage
		Télécopie	1 fax entrant 1 fax sortant feuilles A4
		Imprimante	1 imprimante laser noir et blanc (15 p/min)
		Copieur	1 copieur haute vitesse
		Papeterie	12 blocs-notes A5 50 stylos bille papier blanc et jaune (1 500 p/jour)
		Documents cruciaux	liste alphabétique des clients avec code client liste des produits avec codes produits liste des contrats de maintenance avec date de fin 150 formulaires de commandes
		Mobilier	7 bureaux standard 10 chaises 1 table douze places avec 12 chaises 1 armoire à clés trois parties

De même, le WRT correspond à la période de travail intermédiaire avec des procédures partiellement dégradées et des tâches de reprise de données dans les systèmes informatiques. Il faut prévoir des procédures simples, des formulaires et des aides diverses (PC portables avec logiciels) pour améliorer le vécu de cette période.

### RTO et WRT

Rappelons que le RTO (*Recovery Time Objective*) est le délai qui s'écoule entre la perte des moyens à cause du sinistre et leur récupération dans un état acceptable. Autrement dit, c'est le temps pendant lequel l'employé doit se débrouiller sans le système informatique.

Le WRT correspond à la période qui suit le retour de l'informatique : l'employé ou les informaticiens mettent les données à niveau, aidés en cela idéalement par des formulaires manuels et par l'assistance technique du service informatique.

Avec les utilisateurs qui peuvent donner des indications et des contraintes, on peut commencer à envisager des valeurs possibles pour RTO et WRT.

Tableau 2-10 : Détermination des RTO et WRT

Fonction	Processus	Applications et systèmes critiques	RTO	WRT
Vente	Prendre les commandes	Système de prise de commandes	1 jour	2 jours
		Système de gestion des clients	2,5 jours	0,5 jour
		EDI (échanges de données informatisés)	2 jours	1 jour
Service client	Traiter les commandes	Système de prise de commandes	1 jour	1 jour
		Facturation client	1,5 jours	0,5 jour
		Gestion d'inventaire	1 jour	1 jour

On notera que plus le RTO est long, plus y a de chances (ou malchances) que le WRT le soit aussi. Plus l'absence de l'informatique a été longue, plus la quantité de données à ressaisir est importante. Si l'on veut réduire le WRT, il faut donc faciliter les saisies dans le nouveau système et limiter le RTO autant que faire se peut.

### Ajustements sur les MTD

Le MTD est le temps maximum d'interruption admissible – tout compris. Il va ainsi correspondre à la somme du RTO et du WRT. Ce paramètre est assez souvent évalué indépendamment des autres par des responsables d'entités ou de départements. Il n'est pas rare qu'il soit présenté comme un chiffre non négociable.

Or, rien ne dit a priori que l'égalité  $MTD = RTO + WRT$  puisse être respectée. En effet, le terme de droite ( $RTO + WRT$ ) est souvent trop élevé pour convenir à la valeur indiquée comme « seuil de douleur » par le MTD. Il faut donc, là encore, discuter et faire maints ajustements pour parvenir à des valeurs réalistes.

Tableau 2-11 : Ajustement des valeurs de RTO et WRT sur les MTD

Fonction	Processus	MTD (en jours)	RTO (en jours)	WRT (en jours)
Vente	Prise de commandes	0,5	0,25	0,25
Marketing	Gestion du catalogue	1	0,5	0,5
	Gestion des partenaires	1	0,5	0,5
Logistique	Organisation des expéditions	1	0,5	0,5
Support client	Hotline	2	1,5	0,5
	Expertise Niveau 1	2	1,5	0,5
Paiement	Couplage carte bancaire	1	1	0
	Couplage VAD (vente à distance)	3	1	2

Notons que ces chiffres peuvent, pour une première estimation, ne pas être totalement réalistes. Il arrive en effet que se présentent les situations suivantes.

- Le MTD fixé par le directeur métier n'est pas réalisable, car le RTO (subi) est trop élevé : la récupération des moyens techniques prend trop de temps, par exemple. On cherchera alors soit à raccourcir cette durée en améliorant les possibilités de bascules sur des systèmes de secours, soit à limiter les prétentions en termes de MTD.
- La durée du WRT est telle qu'elle ne peut permettre d'atteindre le MTD fixé : on travaillera alors à abrégé les travaux manuels de reprise (par le recours à la saisie en intérim ou en mettant au point divers scripts de traitements, par exemple) ou bien, là encore, on abaissera les exigences en termes de MTD.

Il apparaît donc possible de jouer sur ces trois paramètres : MTD, WRT et RTO. En général, une concertation avec les directeurs métier et les responsables du service informatique permet d'arriver à un compromis cohérent en termes de reprise technique et de travail de mise à jour manuelle, donnant qui plus est satisfaction pour le délai d'interruption maximal.

Bien entendu, il faudra tenir compte des coûts associés à tout cela, concernant aussi bien la perte d'exploitation que la mise en œuvre de solutions onéreuses et à disponibilité élevée ou encore que la reconstruction rapide.

### RPO

Le RPO (*Recovery Point Objective*) indique la durée rétroactive permettant d'obtenir une donnée fiable et correctement utilisable. Celle-ci correspond en général au temps qui sépare le sinistre de la dernière sauvegarde utilisable.

Précisons que la dernière sauvegarde utilisable ne correspond pas forcément à la dernière sauvegarde effectuée. C'est le cas, par exemple, lorsque plusieurs traitements sont liés entre eux et que l'un d'eux possède une sauvegarde plus ancienne que celle des autres. Il pourra alors être nécessaire de remonter au moment des dernières sauvegardes communes à tous.

Qui dit sauvegarde ne dit pas forcément bande magnétique, même si ce support était le plus courant ces trente dernières années. Il existe depuis quelque temps des sauvegardes sur disque, des copies instantanées (*snapshot* ou clichés) ou encore des miroirs distants sur site éloigné. Les bandes magnétiques présentent toutefois l'intérêt d'être amovibles et de pouvoir être conservées en lieu sûr. On se reportera sur ces points au chapitre 8.

Concernant la restauration, la technologie actuelle offre tout un ensemble de moyens permettant de reconstituer un état propre des données situé plus ou moins loin dans le passé. À partir de ces données récupérées, il est également possible dans certains cas de ré-appliquer informatiquement les mises à jour perdues : il suffit pour cela d'avoir mis en place un sous-système maintenant un journal (*log*) des actions effectuées, et d'avoir retrouvé ledit journal. Le processus de reconstruction prend en général du temps et de la puissance machine.

Reconstruire les données jusqu'au terme du journal (c'est-à-dire jusqu'à un moment très proche de celui du sinistre) peut nécessiter un délai allant de quelques minutes à quelques jours. En général, le journal ne sera pas stocké avec les données, de manière à ne pas tout perdre en même temps. Malheureusement, ces techniques très utiles portent rarement sur l'ensemble des données à traiter, et il faut donc utiliser simultanément plusieurs techniques plus ou moins récentes et plus ou moins automatiques. Tous ces aspects techniques sont couverts plus en détail dans la partie III.

Pendant la durée du RPO, les données non sauvegardées peuvent connaître plusieurs situations :

- soit elles sont conservées dans des systèmes provisoires (PDA, ordinateurs portables, PC, Internet, etc., avant un transfert qui n'a pas eu lieu) ;
- soit elles n'ont pas été sauvegardées mais peuvent être reconstituées via les journaux (ou *logs*) qui seront appliqués durant la récupération du travail (WRT) ;
- soit elles sont perdues mais peuvent être reconstituées en appliquant des traitements de rattrapage (souvent des traitements par lots ou *batches*) ;
- soit elles ont été notées par écrit et peuvent donc être ressaisies ultérieurement (plus ou moins facilement) ;
- soit elles sont perdues définitivement.

Ces diverses situations doivent être prises en compte pour récupérer les données durant la période de WRT. En effet, plus le RPO est long, plus le WRT le sera aussi. Enfin, il est possible que des données aient été définitivement perdues.

En réalité, le RPO est imposé par les choix techniques qui ont été faits pour se prémunir d'un sinistre. Il dépend le plus souvent de la fréquence des sauvegardes. Il arrive que celle-ci ait été décidée pour répondre aux besoins des responsables d'activité, mais c'est rarement le cas.

Lors d'une analyse d'impact, on peut se limiter à constater les RPO suite aux choix techniques réalisés dans le passé. On peut aussi noter les insuffisances existantes et préconiser des valeurs plus appropriées aux contraintes de MTD. Pour obtenir ces valeurs dans la réalité, des actions techniques devront alors être prévues (voir sur ces points le chapitre 3).

Dans cet exemple, la colonne RPO indique :

- un chiffre de 0 à 5 jours : en effet, la sauvegarde étant effectuée le vendredi soir, le RPO dépend alors de la date du sinistre ;
- nsp : pour les cas où il n'y a pas à proprement parler de données à récupérer ;
- 1 jour : délai maximum lorsque la sauvegarde est journalière ;
- 0,5 jour : le délai est court, dans cet exemple, car il suffit de récupérer des fichiers systèmes et très peu de données.

Rappelons que ces chiffres indiquent la plage durant laquelle les données sont soit perdues, soit à reconstruire. Ils ne donnent pas d'indication sur la durée de cette reconstruction (qui est incluse dans le WRT ou temps de récupération du travail).

*Tableau 2-12 : Exemples de RPO*

Fonction	Processus	Applications et systèmes critiques	RPO
Vente	Prise de commandes	Téléphonie Application <i>Vador</i> sur Unix, site de Lyon	1 jour
Marketing	Gestion du catalogue	Serveurs web de gestion du catalogue, site de Lyon et hébergeur	0 à 5 jours
	Gestion des partenaires	Application <i>Agépar</i> sur mainframe, site de Paris	1 jour
Logistique	Organisation des expéditions	Logiciel SAP S&D Couplage avec logistique Infodis	1 jour
Support client	Hotline	Centre d'appels, site de Paris	nsp
	Expertise Niveau 1	Plateau téléphonique, site de Lyon	nsp
Paiement	Couplage carte bancaire	Accès au système d'autorisation	0,5 jour
	Couplage VAD (vente à distance)	Accès à la VAD et programme VAD	1 jour

### Procédures de secours

Les procédures de secours – ou de mode dégradé – visent à permettre le travail malgré la perte des moyens informatiques et non informatiques causée par un sinistre. Les processus concernés sont ceux qui ont été au préalable sélectionnés comme critiques. Ces procédures, moins efficaces que les procédures habituelles, peuvent recourir à des tâches manuelles (par exemple : saisie sur papier ou, mieux, sur formulaires, appels téléphoniques, etc.) qui nécessiteront peu de moyens.

Il s'agit alors :

- de collecter les procédures existantes et de s'assurer qu'elles sont viables ;
- de déterminer celles qui manquent et qu'il conviendrait de réaliser.

Ces procédures de secours peuvent avoir à cohabiter avec les procédures normales durant des phases transitoires. Ceci représente d'ailleurs une difficulté supplémentaire à gérer. Dans certains cas, en effet, la procédure dite « normale » devra être suspendue et une procédure « de secours » activée.

Cela peut concerner en particulier des aspects extrêmement sensibles comme l'attribution de droits d'accès au système en cas de panne. Si la procédure normale prévoit des circuits durant deux jours alors que le temps presse, on

recourra à une procédure d'urgence dûment notée et suivie à la lettre. Car, bien qu'on sorte du cadre de la procédure normale, il n'est pas question non plus de se retrouver dans un vide procédural. Ce type de difficulté se découvre et se traite durant les tests du plan de continuité (voir le chapitre 6). Ces procédures de secours doivent également prendre en compte le fait que les informations qu'elles produisent doivent pouvoir être ultérieurement entrées le plus aisément possible dans le système informatique, une fois celui-ci de nouveau opérationnel.

### **Exemple : De l'intérêt du taxi dans les modes dégradés**

La société SLGS doit faire parvenir toutes les nuits un fichier à la Banque de France. Cette activité est critique et le système électronique de transfert de fichiers l'est donc aussi.

Une nuit, le transfert critique tombe en panne et il devient impossible d'envoyer le fameux fichier. La panne survient à deux heures du matin. L'heure limite de remise étant cinq heures et le transfert ne prenant que vingt minutes, deux ingénieurs réseau sont réveillés et étudient la réparation possible du système de transfert : ils ont plus de deux heures devant eux.

Le responsable du site arrive plus tard et constate les faits : le temps passe et le fichier n'est toujours pas parti ! Se souvenant de la pratique d'autrefois, il sort le fichier sur une cassette à bande, appelle un taxi et la lui confie : le centre de la Banque de France n'est qu'à une heure de route. La solution de contournement ou le mode dégradé est tout trouvé !

**Moralité :** pensez plus aux véritables objectifs et moins aux moyens.

## Documentation de l'analyse d'impact sur les activités

---

L'analyse ou le bilan d'impact sur les activités (BIA) produit un document récapitulatif. Ce document (ou ensemble de documents) est réalisé au fur et à mesure de la progression de l'étude décrite précédemment et doit être conservé dans un système documentaire adapté. Il fera l'objet d'audits ultérieurs (voir le chapitre 14).

Ce document comporte au moins les éléments suivants :

### **Analyse d'impact sur les activités (BIA)**

1. Note de cadrage du BIA
  - 1.1. Objectifs de l'étude
  - 1.2. Découpage du sujet à étudier
  - 1.3. Hypothèses de départ
2. Analyse des processus d'affaire
  - 2.1. Identification des fonctions et processus
  - 2.2. Estimation des impacts financiers et opérationnels
  - 2.3. Liste des processus critiques pour l'entreprise

3. Configurations concernées
  - 3.1. Évaluation du MTD et des priorités relatives
  - 3.2. Détermination des systèmes et applications informatiques critiques
  - 3.3. Détermination des autres éléments critiques
4. Paramètres de reprise (pour les processus critiques)
  - 4.1. RTO et WRT
  - 4.2. RPO
  - 4.3. Procédures de secours existantes ou à créer
5. Conclusion du document BIA
  - 5.1. Traçabilité des décisions prises
  - 5.2. Proposition de décisions à prendre
  - 5.3. Proposition de suite à donner



# Le développement d'une stratégie de continuité

Au cours des analyses présentées dans les deux chapitres précédents, l'entreprise a fait le point sur les risques qu'elle encourt et a déterminé ses activités critiques, dont la perte lui causerait les dommages les plus forts. Les délais de reprise et les temps d'immobilisation maximum acceptables de ces activités ont été étudiés et sont désormais connus.

Il reste maintenant à effectuer les actions préventives nécessaires et à prévoir les modalités de reprise pour que les exigences des activités critiques puissent être remplies. C'est l'objet de ce chapitre, qui explique comment déterminer ces actions et comment définir la manière dont la continuité d'activité est assurée dans l'entreprise. Tout ce dispositif constitue la stratégie de continuité de l'entreprise.

Les aspects techniques de ce chapitre ne sont qu'esquissés, afin de ne pas nuire à son déroulement ; ils seront abordés plus en profondeur dans la troisième partie de cet ouvrage.

Produire une stratégie de continuité est un travail nécessitant cinq phases principales d'étude et de décision.

1. Dans une première phase, à partir de l'analyse d'impact sur les activités (BIA – voir le chapitre 2) qui a précédé, les besoins en termes de reprise sont affinés et déterminés précisément.
2. Au cours de la deuxième phase, on passe en revue les solutions possibles et réalistes.
3. La troisième phase permet de déterminer les délais inhérents aux solutions proposées en rapport avec les exigences formalisées durant l'analyse d'impact pour chaque activité.
4. La phase quatre consiste à réaliser une étude de coût et faisabilité sur les solutions possibles.
5. Enfin, la phase cinq mène à une conclusion et à une prise de décision : la stratégie est prête et documentée.

Cette stratégie servira de fondement au développement du plan de continuité proprement dit.

### Phase 1 – Expression des besoins en termes de reprise

---

Cette première étape est réalisée à partir des conclusions de l'analyse d'impact sur les activités (BIA). Elle se focalise exclusivement sur les processus jugés critiques.

#### Vocabulaire

Dans la suite de ce chapitre, les mots *processus* et *activités* sont employés indifféremment.

#### Exigences des processus critiques

Dans la liste des ressources associées aux processus critiques (établie normalement lors du BIA), on reprend les différents paramètres de reprise que sont les MTD (temps maximal d'interruption admissible), WRT (temps nécessaire à la récupération du travail), RTO (délai cible de récupération des moyens de travail) et RPO (délai cible de récupération des données).

On y ajoute, le cas échéant, les besoins supplémentaires en cas de crise. Il s'agit principalement de besoins en personnel – définition de l'équipe de gestion de crise nécessaire pour le ou les processus considérés – ainsi qu'en moyens matériels tels que :

- un site de secours (ou des bureaux) d'où la crise sera gérée ;
- des moyens de communication ;
- des possibilités d'accès (doubles de clés, cartes magnétiques, etc.).

Ces points sont précisés et détaillés dans le chapitre 4.

#### Étude des besoins

Pour chaque processus critique, les besoins sont listés et classés en catégories. Ce classement se révèle en effet utile pour pouvoir confier l'étude des divers besoins à des équipes différentes. On pourra, par exemple, reprendre les catégories de besoins suivantes :

1. bureaux et locaux de travail ;
2. systèmes, infrastructures et locaux informatiques ;
3. données et enregistrements critiques ;
4. production industrielle et fabrication.

La gestion de ces listes réclame un soin particulier, de manière à suivre au plus près les évolutions du terrain.

Les ressources humaines, lorsqu'elles sont considérées dans le cadre d'un sinistre externe (non pandémique), figurent de fait dans la première rubrique (les bureaux et chaises étant pour des employés...).

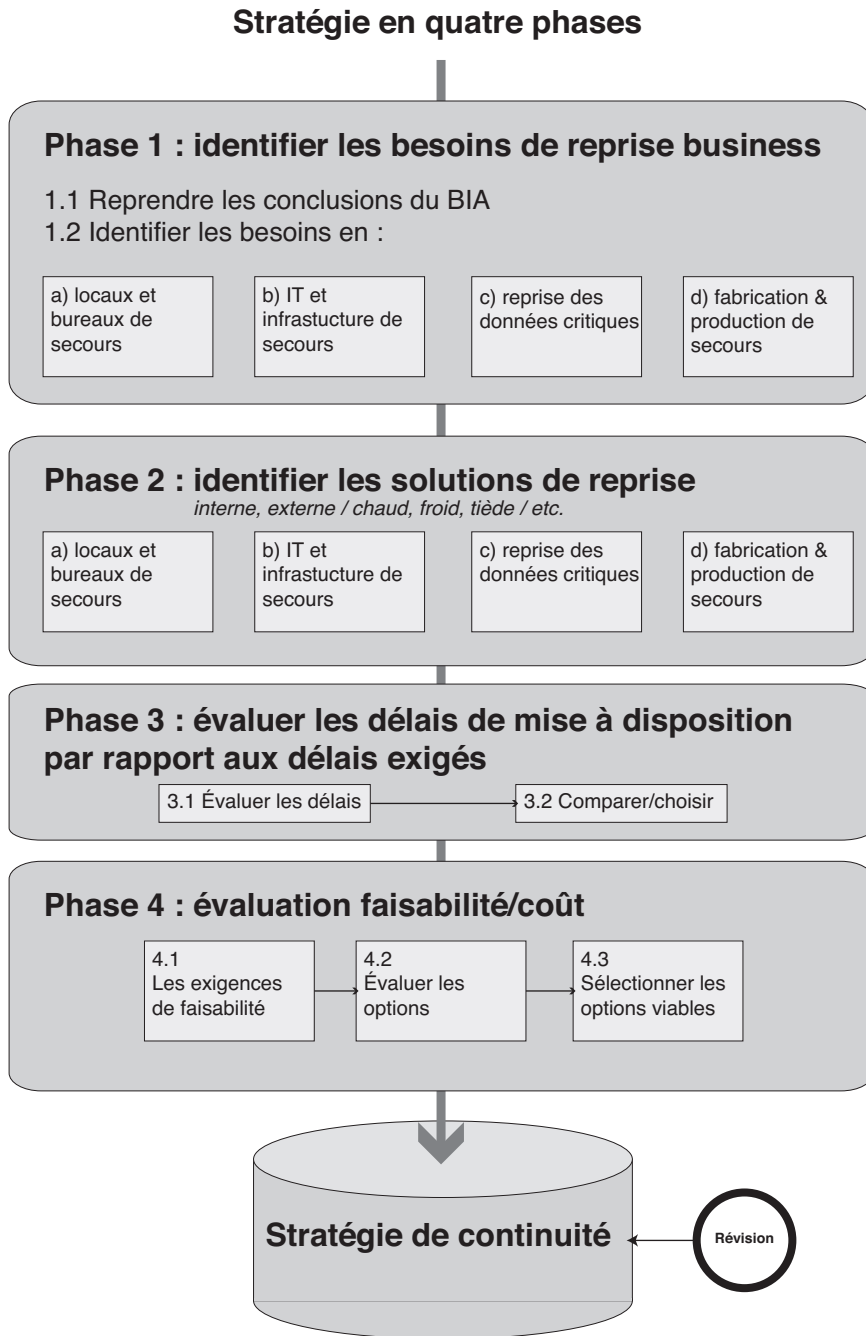


Figure 3-1 : Schéma synoptique de la démarche en quatre phases

En revanche, s'il s'agit du sinistre de pandémie, qui a pour caractéristique principale de ne toucher que les êtres humains, il est recommandé de définir un plan spécial pandémie (voir chapitre 11).

### **1. Bureaux et locaux de travail**

On classe dans cette catégorie les besoins concernant :

- les locaux généraux – situation et nature (par exemple : est-il possible d'utiliser une salle dans un hôtel ? à quelle distance du site sinistré ? aura-t-on besoin d'utiliser des bureaux provisoires mobiles ?) ;
- le mobilier de bureau et meubles divers ;
- les moyens de communication ;
- les fournitures (papiers, stylos, etc.) ;
- des locaux particuliers (locaux réfrigérés ou coffre fort, par exemple) ;
- des formulaires spéciaux (pour faciliter la saisie par écrit, par exemple) ;
- le matériel informatique de bureau (PC avec licences adéquates, imprimantes, etc.).

On indiquera, quand il y a lieu, la tolérance acceptable sur ces moyens.

### **2. Systèmes, infrastructures et locaux informatiques**

Cette catégorie comprend les besoins en termes de :

- locaux informatiques – taille, emplacement et caractéristiques techniques ;
- fournitures électriques nécessaires ;
- capacité de refroidissement et de filtrage de l'air ;
- serveurs de stockage ;
- bandothèques et robots dérouleurs de bandes magnétiques ;
- connexions pour les télécommunications, débits, taux de transfert, etc. ;
- imprimantes spécifiques et alimentation en papier associée ;
- systèmes d'exploitation, sous-systèmes, bases de données, middleware ;
- outils de reprise et de restauration de données ;
- licences d'utilisation associées ;
- postes de travail ;
- PC avec licences adéquates et imprimantes individuelles associées.

La précision s'impose sur la plupart des éléments de cette liste, qui doivent être correctement spécifiés (type, version, mises à jour, niveau, etc.). Il faut en effet assurer une cohérence et une compatibilité optimales de l'ensemble.

### **3. Données et enregistrements critiques**

En complément de la catégorie précédente, il convient de considérer les besoins en documents, données et toute autre information nécessaire à l'activité.

### **Données informatiques**

Classiquement, on étudie les aspects suivants, généralement gérés dans diverses entités de l'entreprise :

- les sauvegardes informatiques (correctement effectuées sur les points de reprise applicative, de manière à pouvoir être chargées et exploitées sur le site de secours) ;
- les lieux où ces sauvegardes doivent être conservées (hors sites) ;
- les formats de ces sauvegardes (média, types de cassettes ou de disques, outils de sauvegarde, formats des enregistrements, contraintes diverses) ;
- les regroupements logiques des éléments sauvegardés (lots de cassettes cohérents, valises regroupant ces lots, etc.) ;
- éventuellement, les moyens logistiques pour acheminer les sauvegardes sur les sites (taxi, camionnette, etc.).

Là encore, la plus grande précision est indispensable, car ces aspects ne tolèrent pas l'approximation. Une cassette manquante ou une sauvegarde effectuée à la mauvaise date provoqueraient, par exemple, l'impossibilité de restaurer les données.

### **Données non informatisées**

Le bureau « sans papiers » étant loin d'être généralisé, il est par ailleurs indispensable de référencer tous les dossiers papiers, microfiches, disques optiques, etc., utilisés dans l'activité de tous les jours ou vitaux en termes de conservation.

Il faut ici prendre en compte tout ce qui est conservé sur le site, dans les bureaux, armoires ou en sous-sol, sans oublier les sites d'archivage. À ce propos, une réflexion sur ce sujet peut se révéler utile pour faire évoluer la politique de gestion et d'entreposage de ces documents.

### **4. Production industrielle et fabrication**

Bien que ces aspects se situent à la marge de cet ouvrage, citons ici les besoins concernant :

- les équipements de production critiques (machines, stocks de pièces intermédiaires, etc.) ;
- les produits cruciaux à conserver en stock (produits finis, semi-finis ou matières premières, etc.) ;
- des locaux alternatifs permettant de fabriquer en tout ou en partie et de poursuivre la production, en précisant leurs caractéristiques.

#### **Remarque générale**

- Ces listes doivent faire l'objet d'une attention minutieuse.
- Elles doivent être remplies et détaillées par des spécialistes choisis en fonction de chaque cas.
- Elles évoluent au cours du temps : les tests et la maintenance du plan (voir les chapitres 6 et 13) veilleront sur ce point à conserver leur pertinence.

- La gestion du changement dans le système informatique doit veiller à bien tenir à jour ces configurations.

## Phase 2 – Étude des options possibles pour la reprise

Afin de répondre aux besoins de reprise exprimés, on étudie un certain nombre d'options envisageables. Ces options doivent être analysées sans idées préconçues sur le fait qu'elles seront finalement retenues ou pas. Il est en effet toujours plus intéressant d'explorer toutes les solutions, sans a priori.

Les classements permettant de structurer la démarche, dans le domaine de la continuité d'activité comme pour toute autre analyse, ces options peuvent une fois encore être regroupées en différentes catégories. L'exclusion éventuelle d'une catégorie, pour quelque raison que ce soit, n'interviendra que plus loin dans la démarche.

### Catégories d'options ouvertes

Deux classements sont proposés ici, selon que l'on considère le fournisseur de l'option (interne, externe, etc.) ou son degré de préparation.

#### ***En fonction du fournisseur***

Un premier classement peut être effectué en fonction du fournisseur de l'option.

- **Options internes** : il s'agit d'options qui engagent l'entreprise avec ses propres ressources et moyens, par exemple : un site de bureaux de secours appartenant à l'entreprise. Le fournisseur est donc interne à l'entreprise.
- **Options contractuelles auprès de fournisseurs** : dans ce cas, on fait appel à un fournisseur externe avec lequel un contrat a été conclu. Sur ce point, on peut noter le développement d'accords d'un type particulier : les accords de réciprocité entre confrères.
- **Options impliquant des employés** : c'est un cas particulier à étudier, impliquant les employés de l'entreprise (les employés peuvent travailler depuis leur domicile par exemple). Il vaut mieux avoir prévu ce cas de figure dans les accords d'entreprise ou, éventuellement, dans le contrat de travail. Le « fournisseur » est alors d'un type un peu particulier, puisqu'il s'agit de l'employé. Si cet employé est un prestataire, on pourra se reporter au cas précédent (fournisseur externe).

#### ***En fonction du degré de préparation***

On peut également classer les différentes options en fonction de leur niveau de préparation et, par conséquent, de leur rapidité de mise à disposition.

- **Options toutes prêtes** : tout est prêt pour prendre le relais en cas de sinistre, les divers moyens sont disponibles, réservés et à jour. C'est en général une option rapide à mettre en œuvre, mais coûteuse.

- **Options prévues** : un accord a été passé avec un fournisseur ou un autre site de l’entreprise pour que les moyens soient mis à disposition dans un délai convenu. C’est souvent le cas dans les situations contractuelles avec une entreprise de secours ou dans les accords de réciprocité avec des confrères, par exemple. Pour cette option, les délais de mise en œuvre sont d’ordre moyen.
- **Options au cas par cas** : rien de particulier n’est prévu a priori, mais on sait que, si le besoin se fait sentir, on y répondra par une action particulière en interne ou une commande en externe. Rien n’empêche d’ailleurs de préparer cette commande. C’est en général l’option la moins coûteuse, mais aussi la moins sûre.

De façon similaire, on classera aussi les moyens informatiques selon leur degré de préparation opérationnelle. Traditionnellement, on parle alors de moyens de secours à *froid* (peu préparés), *tièdes* (préparés) ou *chauds* (prêts à l’usage).

### **Ventilation des options selon les catégories**

Le tableau suivant donne un exemple de ventilation des catégories d’options retenues.

Tableau 3-1 : Ventilation des options retenues dans les différentes catégories

	Interne	Externe	Employés
Froid	Site précâblé à 200 km	Non retenu	Travail à domicile
Tiède	Site de développement activable	Contrat avec une société d’infogérance pour les serveurs Unix	PC prééquipé à domicile
Chaud	Non retenu	Contrat de haute disponibilité sur les applications X et Y	Non retenu

On constate dans cet exemple que les solutions froides retenues ne font pas l’objet de contrats sur le marché et que seule la solution chaude est réalisée avec un prestataire externe.

L’élaboration de tableaux de ce type permet la discussion et la prise de décision durant les réunions de suivi.

### **Options envisagées**

En fonction des besoins exprimés et des catégories d’options définies précédemment, il devient possible de lister et d’analyser les options les plus susceptibles de donner satisfaction. Encore une fois, cela consiste à se livrer à un exercice d’imagination des solutions qui pourraient convenir. Il ne s’agit pas

pour autant de rêver et de s'éloigner de la réalité technologique et financière : les avantages et inconvénients des options listées seront jugés plus loin (phase 3).

On adoptera la même segmentation que pour l'expression des besoins :

1. bureaux et locaux de travail ;
2. systèmes, infrastructures et locaux informatiques ;
3. données et enregistrements critiques ;
4. production industrielle et fabrication.

**1. Bureaux et locaux de travail**

Le tableau ci-après donne un exemple d'options envisageables qui seront étudiées pour les locaux et bureaux, classées en fonction de leur fournisseur.

*Tableau 3-2 : Options pour les locaux et bureaux*

Locaux et bureaux		
Catégorie	Option	Description
Solution contractuelle avec fournisseur externe	Site mobile	Site mobile de secours livré en un lieu prévu, et en général prééquipé en mobilier, téléphones et postes de travail.
	Salles de réunion d'hôtel	Hôtel prévu à l'avance.
	Site fixe	Site de secours en un lieu donné, proposé en tant que service par un prestataire, également prééquipé.
Solution interne à l'entreprise	Autre site de l'entreprise	Site de secours dormant ou pas, prééquipé ou non.
Recours à l'employé	Travail à la maison	L'employé travaille depuis son domicile et peut éventuellement accéder au système informatique, téléphonique, etc.

**2. Systèmes, infrastructures et locaux informatiques**

De même, le tableau suivant traite des options concernant les sites informatiques de secours, plus ou moins équipés des matériels et systèmes nécessaires. Ces options sont ici encore classées en fonction de leur fournisseur (interne, accord externe, offre commerciale). La description des sites doit correspondre au plus près à une réalité constatée et/ou réalisable.

*Tableau 3-3 : Options pour les sites informatiques*

<b>Sites informatiques de secours</b>		
<b>Catégorie</b>	<b>Option</b>	<b>Description</b>
En toute propriété	Site distant appartenant à la société	Site de secours de la société, en un lieu déterminé prévu et en partie préparé.
	Site mobile	Site mobile de secours livré en un lieu prévu, en général prééquipé en mobilier, téléphones, postes de travail ou serveurs, réseaux, etc.
Accord avec un tiers	Accord de réciprocité avec un confrère	Chacun réserve de la place à l’autre en cas de sinistre.
Offre commerciale	Site dédié (offre du marché)	Site de secours dédié, proposé en tant que service par un prestataire, plus ou moins prééquipé.
	Site partagé (offre du marché)	Site de secours partagé, proposé en tant que service par un prestataire, plus ou moins prééquipé.

On peut aussi constituer d’autres tableaux abordant un sujet spécifique pour lequel une décision s’impose, comme le niveau de préparation des sites (voir le tableau suivant).

*Tableau 3-4 : Niveaux de préparation possibles pour les sites informatiques de secours*

<b>Sites informatiques de secours</b>		
<b>Catégorie</b>	<b>Option</b>	<b>Description</b>
Non préparé	Site froid	Site de secours non équipé en matériel informatique mais disposant de moyens pour en accueillir (alimentations électriques, air conditionné, chauffage, eau, sprinklers, lignes télécoms, faux-planchers et passage de câbles, etc.).
Prévu	Site tiède	Site de secours déjà équipé de certains moyens informatiques nécessaires, mais pas de tous, nécessitant donc d’être complété dans un certain délai ; demande une préparation.
Prêt à l’emploi	Site chaud	Site de secours dont l’équipement est très proche de celui du site à secourir.

Pour chaque option envisagée, on peut présenter les niveaux que l’on souhaite étudier (froid, tiède, chaud).