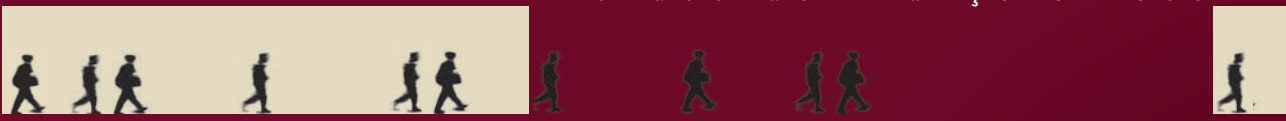
EMMANUEL **BESLUAU**
Préface de **François Tête**



Management de la Continuité d'activité

Assurer la pérennité de l'entreprise : planification, choix techniques et mise en œuvre

EYROLLES

Management de la Continuité d'activité

Assurer la pérennité de l'entreprise :
planification, choix techniques
et mise en œuvre

CHEZ LE MÊME ÉDITEUR

Dans la collection Solutions d'entreprise

A. Fernandez-Toro, préface de H. Schauer. – **Management de la sécurité de l'information.**
Implémentation ISO 27001. Mise en place d'un SMSI et audit de certification.
N°12218, 2007, 256 pages.

C. Dumont. – **ITIL pour un service informatique optimal.** *Mis à jour avec ITIL V3 et la norme ISO 20000.*
N°12102, 2e édition, 2007, 378 pages.

S. Bordage, D. Thévenon, L. Dupaquier, F. Brousse. – **Conduite de projet Web.**
60 modèles de livrables prêts à l'emploi. Un outil de création de business plan. 3 études de cas.
N°12325, 4e édition, 2008, 408 pages.

É. O'Neill. – **Conduite de projets informatiques offshore**.
N°11560, 2005, 336 pages.

Ouvrages sur la gestion de projet

F. Pinckaers, G. Gardiner. – **Tiny ERP/Open ERP.** *Pour une gestion d'entreprise efficace et intégrée*.
N°12261, 2008, 278 pages (collection Accès libre).

V. Messager Rota. – **Gestion de projet.** *Vers les méthodes agiles*.
N°12165, 2007, 258 pages (collection Architecte logiciel).

P. Mangold. – **Gestion de projet informatique.**
N°11752, 2006, 120 pages (collection Compact).

F. Vallée. – **UML pour les décideurs.**
N°11621, 2005, 282 pages (collection Architecte logiciel).

Autres ouvrage

L. Bloch, C. Wolfhugel. – **Sécurité informatique.** *Principes et méthode.*
N°12021, 2007, 262 pages (Collection Blanche).

C. Llorens, L. Levier, D. Valois. – **Tableaux de bord de la sécurité réseaux.**
N°11973, 2e édition, 2006, 560 pages (collection Blanche).

B. Boutherin, B. Delaunay. – **Sécuriser un réseau Linux.**
N°11960, 3e édition, 2007, 250 pages (collection Cahiers de l'Admin).

P. Legand. – **Sécuriser enfin son PC.** *Windows XP et Windows Vista.*
N°12005, 2007, 500 pages (collection Sans taboo).

D. Séguy, P. Gamache. – **Sécurité PHP 5 et MySQL.**
N°12114, 2007, 240 pages (Collection Blanche).

F. Manzano. **Mémento VMware Server.** *Virtualisation de serveurs*.
N°12320, 2008, 14 pages.

R. Bergoin, C. Bourg. **Mémento Cisco.** *IOS – Configuration générale.*
N°12347, à paraître 2008, 14 pages.

C. Dumont. **Mémento ITIL.** N°12257, 2007, 14 pages.

EMMANUEL **BESLUAU**

Préface de **François Tête**

Management de la Continuité d'activité

Assurer la pérennité de l'entreprise : planification, choix techniques et mise en œuvre

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

© Groupe Eyrolles, 2008, ISBN : 978-2-212-12346-3

Préface

Il est toujours trop tard, quand le sinistre arrive, pour mettre en œuvre un plan de continuité d'activité... Un proverbe chinois illustre ce propos : « les tuiles qui protègent de la pluie ont toutes été posées par beau temps ».

Enfin un ouvrage complet, pratique et documenté sur la continuité d'activité, en français de surcroît !

Ayant moi-même vécu en entreprise des situations de sinistre, je peux témoigner de la nécessité d'être préparé à de telles situations, malheureusement plus fréquentes qu'on ne le croit. Un jour, la salle informatique de la banque dans laquelle je travaillais a brûlé. Nous n'avions aucun plan, ni rien de prévu dans une telle situation, à l'exception d'une sauvegarde externalisée.... La banque aurait dû disparaître. Or c'était en 1977, et l'informatique n'avait pas l'importance vitale qu'elle possède à présent. La banque a pu redémarrer, au prix fort, dans les cinq jours suivants, grâce à des locaux et des moyens fournis par un constructeur. Nous ne sommes revenus à une situation normale que six mois plus tard.

Après ce sinistre, qui avait enfin décidé la direction générale à mettre en place des solutions de secours et un plan associé, j'ai pris conscience de la valeur qu'il faut attribuer à une bonne préparation et aux démarches du type de celles présentées dans ce livre pratique.

En outre, dans ma vie professionnelle, j'ai côtoyé et conseillé de nombreux responsables d'entreprise. Tous m'ont fait part de leur souhait d'y voir enfin plus clair dans la démarche visant à mettre en place de manière pragmatique le management de la continuité d'activité dans leur entreprise. En effet, la mise en place d'un plan de continuité est un projet atypique. C'est un projet transverse qui prend en compte globalement toutes les activités et processus de l'entreprise.

Le Club de la Continuité d'Activité réunit tous les acteurs œuvrant dans ce domaine. Il a pour missions de partager les points de vue et retours d'expérience, de parfaire la maîtrise des solutions et de pérenniser la place du management de la continuité dans l'entreprise. Par là, il joue un rôle moteur auprès des organismes de normalisation et du législateur.

Le Club de la Continuité d'Activité accueille avec intérêt tout ce qui peut contribuer à développer les bonnes pratiques, comme le fait cet ouvrage. Riche d'une expérience très diversifiée de la production informatique, Emmanuel Besluau

connaît bien tout ce que l'on peut attendre des technologies. Son approche, qui présente à la fois les principes d'organisation et les architectures techniques, se révèle très intéressante et assez unique.

Nul doute que ce livre contribuera à faire avancer la prise de conscience sur ce sujet important qu'est la continuité d'activité.

François TÊTE
Président du Club de la Continuité d'Activité
www.clubpca.eu

Table des matières

Partie III – L'ingénierie de la continuité

Partie IV – La gouvernance de la continuité

Avant-propos

Un grand nombre d'entreprises ne survivraient pas à une interruption de leur système d'information pendant seulement trois jours. À l'heure où le principe de précaution prévaut, alors que les mesures de sécurité ont pour objectif de prévenir contre des menaces éventuelles, des approches nouvelles, organisationnelles et techniques, se sont développées pour faire face aux conséquences des sinistres sur l'activité de l'entreprise.

Le management de la continuité d'activité permet ainsi de rendre l'entreprise plus résiliente dans un monde de risques. Autrefois limitée à la « gestion de crise » ou considérée comme une sous-partie de la gestion des risques ou de la sécurité, cette approche commence à s'imposer comme une discipline à part entière.

Or, les observateurs de l'entreprise s'accordent à considérer que la continuité d'activité n'a pas actuellement en France l'attention qu'elle mérite de la part des directions générales. En effet, l'analyse des risques reste très limitée, l'impact des sinistres potentiels n'est pas suffisamment étudié et les processus les plus critiques de l'entreprise ne sont que rarement identifiés. En l'absence de ces considérations, toute atteinte à l'intégrité des moyens vitaux de l'entreprise est souvent chèrement payée, voire insurmontable pour la plupart des entreprises, qui n'y sont pas préparées.

Certes, quelques plans de reprise de l'activité existent ici ou là et l'on peut louer les pionniers qui s'y consacrent. Malheureusement, il s'agit le plus souvent de scénarios trop simples, centrés sur les moyens et auxquels fait défaut une vision d'ensemble de la continuité. En outre, les directions de la production informatique ont tendance à mettre en place des solutions ambitieuses qui, en l'absence d'une perspective sur les services utilisateurs, laissent des lacunes importantes. Les investissements consentis en informatique peuvent ainsi apparaître comme disproportionnés si l'on considère la faiblesse de certains maillons organisationnels.

Confiance exagérée dans la technologie, défiance désabusée pour les dispositifs d'organisation, le vécu de la continuité d'activité en France reste largement insatisfaisant. Une prise de conscience des apports réels du management de la continuité d'activité s'impose : c'est l'objectif de cet ouvrage, qui aborde les aspects méthodologiques aussi bien que la mise en œuvre concrète en s'appuyant sur des exemples et situations vécues édifiantes.

À qui s'adresse cet ouvrage ?

Cet ouvrage intéresse tout professionnel concerné par la continuité d'activité : les directions générales y découvriront comment structurer leur approche, les responsables du plan de continuité y trouveront un cadre de travail avec des recommandations, tandis que les directeurs métier y gagneront une idée plus claire de leurs responsabilités et de leur rôle en matière de continuité. Quant aux spécialistes techniques, ce livre leur fournit nombre d'indications et de recommandations leur permettant de mettre en œuvre la continuité au niveau technique.

Structure de l'ouvrage

Afin de ne négliger aucun aspect stratégique, organisationnel ou technique, cet ouvrage se présente en quatre volets, qui guideront pas à pas les différents acteurs et responsables vers une gestion efficace de la continuité d'activité en entreprise.

- La première partie est consacrée à un sujet essentiel souvent négligé dans les études de continuité : le risque. Comment en prendre conscience et déterminer les faiblesses de l'entreprise ? Et surtout, comment limiter, d'une part l'exposition au risque et d'autre part les conséquences encourues ?
- Partant d'une approche plus traditionnelle quoique rénovée, la deuxième partie décrit comment construire les équipes et attribuer les missions pour obtenir un plan de reprise efficace et comment organiser les tests et exercices pour qu'il le reste. Des canevas précis de plannings et de campagnes de tests réutilisables y sont fournis.
- En troisième partie est proposé un tour d'horizon technologique et informatique qui décrit les différents mécanismes en jeu, en relativisant leur apport et en insistant sur les moyens montrant le meilleur retour sur investissement.
- Enfin, après l'analyse, l'élaboration du plan et l'étude des moyens techniques disponibles, la quatrième partie traite des aspects essentiels de gouvernance supervisant la mise en œuvre de la continuité, à travers la prise de conscience nécessaire, les décisions de politique et le contrôle indispensable à mettre en place.

Remerciements

Je remercie mes collègues du Duquesne Group et tout particulièrement René Dugué et Donald Callahan, qui m'ont poussé à consacrer le temps nécessaire à cet ouvrage. Je tiens aussi à décerner une mention spéciale à Denis Goulet, Québécois dans un monde anglophone et précurseur du management de la continuité d'activité en français, ainsi qu'à Michel Grosbost, animateur d'initiatives du plus grand intérêt au sein du Club de la Continuité d'Activité.

PARTIE I

L'entreprise dans un monde de risques

L'entreprise est exposée à des menaces qui ne deviennent un risque que lorsque ses processus sont visés. Pour autant, avoir une vision claire de l'interférence entre les menaces et les processus critiques de l'entreprise ne va pas de soi. Pour avancer, toute organisation doit donc mener des actions visant à prendre conscience de son environnement et à comprendre son propre fonctionnement. Ce n'est qu'à cette condition qu'elle aura en main les paramètres lui permettant de maîtriser sa continuité.

Cette démarche complexe, permettant d'agir en pleine connaissance de cause, est nécessaire pour aborder concrètement la continuité d'activité. Elle est présentée tout au long des trois premiers chapitres :

- Le chapitre 1 regroupe, sous la notion de « maîtrise du risque », à la fois la démarche d'appréciation des menaces qui pèsent sur l'entreprise et les tactiques permettant de les éviter ou de s'en protéger.
- Le chapitre 2 est consacré à ce que l'on appelle « l'analyse d'impact sur les activités » qui, en détaillant les différentes activités de l'entreprise, cherche à déterminer celles dont la perte est le plus dommageable à l'entreprise.
- Le chapitre 3, partant des constats des chapitres précédents, permet de développer une « stratégie de continuité » en sélectionnant, parmi les différentes options, les actions à mener pour améliorer la résilience de l'entreprise.

Ces trois chapitres sont structurés de telle manière que le lecteur pourra sans peine suivre dans l'ordre la procédure proposée pour mener sa propre étude de continuité dans l'entreprise. Ils peuvent ainsi quasi servir de squelette à l'élaboration de la première partie d'un plan de continuité.

Chapitre 1

La maîtrise du risque

Pour assurer sa continuité, l'entreprise doit savoir à quelles menaces d'interruption de ses activités elle est exposée. L'analyse des risques lui permettra de chiffrer les évaluations des pertes et les probabilités d'occurrence des sinistres.

Ainsi, connaissant mieux le champ des risques encourus, l'entreprise pourra étudier les options permettant d'en réduire les effets. Ce n'est qu'alors qu'elle sera en situation de décider quelles actions réaliser pour maîtriser le risque.

Appréciation des risques

Il est tentant de se prémunir globalement contre les « coups durs », sans analyser ce qui pourrait se passer réellement. Cette approche est d'ailleurs la plus naturellement suivie. Elle présente cependant plusieurs inconvénients :

- L'entreprise est préparée à faire face à un événement qui a en fait peu de chance de se produire, alors qu'elle a négligé des menaces qui, elles, sont bien plus probables.
- L'absence de connaissance précise des menaces peut rendre les plans de reprise irréalistes car ne tenant pas compte de l'ensemble de la situation créée par le sinistre, qui a été trop caricaturé dans les études.
- Les tests réalisés pour les plans de reprise, par exemple, sont facilités par le fait que certains aspects du risque ne sont pas pris en compte. L'entreprise acquiert alors une confiance exagérée dans ses capacités de reprise. Or, si la démarche de simplification suivie au cours des tests peut être intéressante, elle ne doit pas s'effectuer sans avoir été volontairement décidée.

Il devient donc nécessaire de passer en revue un certain nombre de menaces et d'étudier leurs conséquences possibles sur l'activité de l'entreprise. C'est la combinaison de ces menaces et de leurs conséquences néfastes probables que l'on appelle un risque.

Identification des menaces

Sont considérées comme des menaces toutes les situations qui peuvent survenir ayant pour conséquence une détérioration des moyens utilisés pour mener à bien l'activité de l'entreprise.

> **Vocabulaire : emploi du terme « moyens »**
>
> Dans cet ouvrage, le terme « moyens » est employé dans un sens très générique. Il recouvre aussi bien les moyens techniques (machines, pièces, etc.) que les services (eau, gaz, électricité) ou les locaux (bâtiments de bureaux ou industriels). Le terme peut aussi inclure les ressources humaines, même si ces dernières possèdent une valeur incomparable aux autres.

L'analyse des menaces est un sujet complexe qui ne se prête pas à une modélisation aisée. Toute modélisation suppose en effet une simplification qui peut se révéler préjudiciable à l'exhaustivité de la démarche. Il faut donc garder à l'esprit, en cas de simplification, qu'une approche complémentaire plus approfondie est souhaitable. Par conséquent, il est recommandé de mener au moins deux approches différentes.

En outre, une approche trop formelle et inutilement théorique peut elle aussi se révéler inefficace. Mieux vaut ne pas perdre l'objectif de vue : il s'agit de savoir à quoi l'on s'expose et comment on y fera face. Il est donc primordial de rester pragmatique.

Il peut arriver qu'une entreprise ne souhaite pas aborder certains risques dans le champ d'une étude. Quelles qu'en soient les raisons (politiques, souci de confidentialité, etc.), il est souhaitable de le mentionner lors du cadrage de l'étude du risque (voir le document page 30).

Caractéristiques des menaces

Toute menace comporte trois caractéristiques principales qui méritent l'attention :

1. **Elle a des conséquences considérées comme nuisibles à l'activité.** Ces conséquences peuvent être de gravité variable. Un incendie, par exemple, peut endommager l'ensemble d'un site informatique ou, au contraire, être circonscrit aux poubelles de la cantine. On voit bien ici que le même événement menaçant « incendie » peut avoir différentes conséquences.
2. **Elle possède une probabilité d'occurrence.** Cette probabilité est considérée comme suffisamment forte pour que l'on ait à s'en soucier. Quantifier les probabilités d'occurrence est un art difficile dans bien des cas, mais il est au moins possible de déterminer ce qui est plus probable par rapport à ce qui l'est moins, en raisonnant uniquement par valeur relative.
3. **Elle a une origine,** soit humaine, soit technique, soit naturelle. Cette caractéristique est importante, car elle influencera les moyens mis en œuvre en prévention. Il est également possible de limiter l'analyse du risque à une

seule de ces origines (par exemple : technique et informatique). Il s'agit alors d'une décision de cadrage à porter au dossier (voir le document page 30).

En première analyse, il est donc possible d'établir une liste des menaces et de leurs conséquences. Le tableau suivant en donne un exemple.

Tableau 1-1 : Exemples de menaces en première analyse

Menaces	Conséquences
Crue du fleuve	Site inondé
Panne électrique	Serveurs non alimentés
Tempête de neige	Personnel absent

> **Rappel : risque**
>
> La combinaison d'une menace et d'une conséquence est appelée un risque.

Diversité des risques

Pour un événement dont les conséquences peuvent être très diverses, on pourra être amené à procéder à un découpage. En effet, les conséquences pouvant être plus ou moins graves en réalité, cela permet une meilleure analyse. En outre, cela peut permettre de mieux cerner les probabilités d'occurrence des risques ainsi mis en évidence.

Exemple 1 : inondation

Considérons la menace « crue du fleuve », sur un site informatique proche d'un fleuve.

Il se trouve, dans ce cas particulier, que trois types d'inondations sont susceptibles de se produire, avec des conséquences très variables sur le site lui-même.

1. Une inondation ayant lieu tous les dix ans en moyenne, qui empêche la circulation sur l'accès principal au site : il faut alors arriver par un accès secondaire, qui ne permet pas les livraisons par poids lourds.
2. Une inondation survenant tous les trente ans qui, en plus des conséquences citées dans le paragraphe précédent, rend impraticable le rez-de-chaussée du bâtiment, où l'eau monte à vingt centimètres : la limite de vingt centimètres est choisie volontairement, car au-delà, le site ne peut plus être mis sous protection.
3. Des inondations plus graves (mais aussi plus rares), où l'eau monte au-delà des vingt centimètres : parmi celles-ci, une inondation dite centenaire est gravée dans les mémoires (et sur les murs), bien qu'on ne l'ait plus observée depuis 1906 ; elle envahirait tout le rez-de-chaussée, jusqu'à deux mètres de haut.

Cet exemple montre bien que les situations décrites ont différentes probabilités d'occurrence et des conséquences de gravité variable. Ces conséquences étant différentes, les réactions face à elles le sont aussi.

1. Dans le premier cas, les livraisons par poids lourds sont interrompues : cela peut représenter une gêne pour certains éléments et l'on pourra être amené à revoir certains stocks en conséquence.
2. Lorsqu'il y a moins de vingt centimètres d'eau, on doit alors procéder à diverses interventions d'isolement. La perturbation sur le site est plus importante.
3. Au-delà de vingt centimètres d'eau, le site est globalement sinistré. Même si l'on peut faire des distinctions entre des crues d'importance variables, pour ce site, seule la limite des vingt centimètres compte en termes pratiques. Il ne sert à rien d'étudier des crues à cinquante centimètres, un mètre, etc.

La menace « inondation » peut alors être découpée en trois pour être considérée comme trois risques différents, chacun étant la combinaison de probabilités et de conséquences différentes. On ne traitera donc pas l'inondation comme un seul événement, doté de conséquences moyennes et d'une probabilité d'occurrence moyenne unique.

Notons aussi qu'on a, dans cet exemple, pris en compte la réalité des choses, et qu'un autre site situé légèrement plus haut, ou ne disposant que d'un seul accès, face à la même menace ne présenterait pas les mêmes risques. L'évaluation du risque doit donc tenir compte du contexte.

Pour synthétiser, la menace « inondation » devient alors :

Tableau 1-2 : Menace « inondation » analysée

Menaces	Conséquences
Inondation de type 1	Site épargné, mais accès poids lourds impossible
Inondation de type 2	20 cm d'eau au rez-de-chaussée
Inondation de type 3	> 20 cm d'eau, dégâts inacceptables

Un événement qui peut se produire de manière graduée (hauteur de la crue du fleuve, par exemple), avec des fréquences relativement connues, se prête plutôt bien à ce genre de découpage. Celui-ci permet, par ailleurs, une riposte adaptée à chaque type de risque, d'où son intérêt.

Exemple 2 : panne d'électricité

Un exemple similaire est fourni par la « panne de courant » qui, là encore, peut avoir des conséquences variables, en particulier en fonction de sa durée.

1. Panne de moins de cinq minutes : les serveurs critiques du système informatique sont pris en charge par les onduleurs sans interruption.

2. Panne de plus de cinq minutes et de moins d'une heure : les onduleurs ont été relayés par un générateur Diesel qui a été démarré à cette occasion.
3. Panne de plus d'une heure : le générateur arrive en fin d'autonomie (plus de fioul) et les serveurs critiques doivent être arrêtés de façon correcte.

Sur ce site et avec les matériels employés, on a alors le schéma suivant :

Tableau 1-3 : Menace « panne d'électricité » analysée

Menaces	Conséquences
Panne électrique 5 min	Passage sur onduleur des serveurs critiques
Panne électrique < 1 h	Onduleur, puis passage sur générateur Diesel
Panne électrique > 1 h	Idem, puis arrêt propre des serveurs au bout de 2 h

La limite à une heure est choisie en fonction des matériels et des diverses réserves en place (capacité des batteries, quantité de fioul, etc.). Dans un autre contexte, cette limite aurait pu être tout autre.

La notion de catastrophe

À l'inverse de ce qui précède, un événement violent et rare, aux conséquences quasi imprévisibles, ne se prêtera pas à une analyse fine. On peut alors préférer envisager un risque global de perte totale comme hypothèse de travail. Un exemple type en est la chute d'avion sur un site à proximité d'un aéroport. On utilise d'ailleurs dans ces cas là le mot « catastrophe », qui indique bien que la situation n'est pas du même ordre de grandeur.

Ici apparaît bien la difficulté du raisonnement par les risques et la nécessité d'analyser les menaces en les découpant. En effet, un événement très violent et très rare peut présenter le même risque qu'un événement à conséquences moyennes se présentant assez souvent : sa probabilité est cent fois plus faible, mais ses conséquences cent fois plus fortes. Le produit des deux est donc équivalent. Cela entrera en jeu dans le raisonnement lors du chiffrage du risque.

Pourquoi décomposer ?

Une menace globale fait donc l'objet d'une décomposition en « sous-menaces », plus faciles à cerner ou à éliminer, et faisant l'objet de risques distinctement perçus.

Les critères suivants peuvent être retenus pour mener la démarche de découpage.

- Si la menace a des conséquences multiples et aléatoires, il faut la décomposer en autant de risques que de conséquences possibles.
- Si la menace est trop vague, il convient de la décomposer en couples menaces/conséquences, plus faciles à cerner.

- Si la menace possède des sources ou causes de natures différentes (humaine et naturelle, par exemple), il convient de faire la séparation selon ces causes, car la réaction peut être différente.
- Si la décomposition n'apporte aucune précision ou concerne des événements ayant des probabilités de valeur proches, il ne sert à rien de décomposer davantage.
- Si la décomposition permet de distinguer des événements dont on possède des probabilités d'occurrences, il faut alors décomposer sans hésiter.
- Si la décomposition permet d'isoler un risque que l'on élimine volontairement (par exemple, les risques d'origine humaine), il peut être intéressant de décomposer.
- Si la décomposition permet de faire la distinction entre des situations acceptables ou gérables et d'autres qui ne le sont pas, il faut le faire pour isoler ces situations.

Dès lors, toute modification des paramètres qui ont abouti à la décomposition est à suivre avec attention. Le risque – ou le « paysage du risque » – s'en trouve modifié. Pour une même menace, les conséquences elles-mêmes peuvent changer. Reprenons les deux exemples mentionnés plus haut pour illustrer ce propos.

1. **Inondation** : des travaux réalisés par le département et la commune font que le site n'est plus atteint par les crues qui, autrefois, auraient nécessité une intervention (crues de vingt centimètres).
2. **Panne d'électricité** : les serveurs informatiques sont toujours plus nombreux et consomment plus qu'autrefois, alors que la capacité des onduleurs n'a pas évolué. Il faut désormais compter sur seulement trente minutes d'autonomie (et non plus une heure).

Ces exemples montrent qu'une analyse de risque doit être revue régulièrement, entre autres pour s'assurer que les hypothèses existantes sont toujours justes, et pour prendre en compte de nouvelles hypothèses.

Sources des menaces

Dans une approche globale du risque, il est intéressant d'étudier les sources des menaces, en les classant selon les trois domaines : technique, humain et naturel.

- La source – ou l'origine – **technique** concerne toute menace qui provient d'un mauvais fonctionnement d'un matériel ou d'une partie d'un matériel. On classe dans cette catégorie les pannes de machines, l'usure de pièces ou matériaux provoquant des ruptures, des écroulements, etc., mais aussi les bogues logiciels qui peuvent bloquer des équipements. Cette source de menace est en général facilement étudiée.
- La source dite **humaine** est invoquée lorsque l'origine de la menace est une volonté ou une erreur humaine. On trouve dans cette catégorie l'erreur pure

et simple, mais aussi la grève, le désir de nuire, le sabotage, le terrorisme. Il est courant que certaines situations soient exclues de l'étude ou traitées séparément, pour des raisons de confidentialité. En revanche, on insistera sur les aspects concernant l'erreur humaine, en concevant des systèmes qui limitent les situations pouvant conduire à une erreur.

- Enfin, la source dite **naturelle** concerne les désordres climatiques (intempéries, foudre, tornade, sécheresse, tempête de glace, etc.), les accidents géologiques (tremblements de terre, volcans, tsunamis, affaissements), hydrauliques (inondations, torrents de boue, avalanches) ou autres (météorite). Les épidémies et autres pandémies, bien que liées à l'homme, sont souvent classées dans cette catégorie car elles ne découlent pas d'une volonté humaine.

Ces origines peuvent se combiner ou se succéder. Par exemple, la canicule peut provoquer l'erreur humaine, qui pourra conduire à une défaillance matérielle.

Le tableau suivant donne un exemple de liste de menaces.

Tableau 1-4 : Menaces classées selon leur source

Technique	Humaine	Naturelle
Panne électrique	Grève	Tremblement de terre
Panne de disque dur	Hacker	Tempête
Panne de contrôleur réseau	Maladie	Inondation
Panne de climatisation	Erreur de manipulation	Foudre
Chute d'avion	Accident du travail	Épidémie
Fuite d'eau	Malveillance	Éruption volcanique

Cette classification se révèle intéressante pour la suite de l'analyse. En effet, les options de parade étudiées plus loin seront très différentes en fonction des sources potentielles de menace.

Le 11 septembre 2001, les attentats sur les tours jumelles de New-York ont inauguré la cause humaine pour une chute d'avion. Cet exemple tragique laisse apparaître que l'on ne traite pas de la même manière la source technique (un avion est techniquement suffisamment fiable) et la source humaine (empêcher la prise en main des commandes par des terroristes).

De plus, les catastrophes naturelles étant pour la plupart communes à une région géographique, les stratégies de secours doivent en tenir compte (voir les chapitres 3 et 10) pour que l'exposition au risque ne soit pas la même sur le site principal et le site de secours, par exemple.

Enfin, en termes de documentation de l'étude et de traçabilité des choix, il est intéressant de noter toutes les options ou hypothèses, même si l'on décide par

la suite de mettre de côté certaines sources ou menaces pour quelque raison que ce soit.

Menaces retenues pour analyse

Dans chacune des trois catégories, des événements menaçants peuvent être distingués, en tenant compte de la réalité technique, humaine et du terrain. Parmi ces événements, un certain nombre est retenu pour analyse, les autres laissés de côté comme non pertinents.

Le tableau suivant donne un exemple.

Tableau 1-5 : Événements menaçants retenus pour un site

Source	Événement menaçant
Fuite d'eau	Montée des eaux en salle machine
Grève	Entrée impossible dans les bureaux
Erreur humaine	Pelleteuse sectionnant les câbles du réseau
Tremblement de terre	Bâtiments fragilisés et partiellement en ruine
Malveillance	Accès à des données confidentielles
Hackers	Paralysie d'un site web

Une telle analyse s'appuie sur les caractéristiques de l'existant et sur les événements éventuellement constatés dans l'entreprise, la région, le pays ou le secteur d'activité.

Conséquences sur les actifs de la société

On entre là dans le vif du sujet : analyser les conséquences des événements menaçants sur les actifs de la société.

Le mot « actif » est pris au sens le plus large : il désigne ici tout ce qui concourt à la bonne marche de l'entreprise. Une classification des actifs pouvant se révéler utile, distinguons par exemple :

- **les ressources humaines** – personnel, compétences particulières, savoir-faire humains, titulaires de droits d'accès spéciaux aux logiciels, etc. ;
- **les ressources intangibles** – fichiers, bases de données (informatiques ou non), informations confidentielles ou secrètes, procédures, mais aussi l'image de la société sur son marché, sa bonne réputation, etc. ;
- **les biens tangibles** – locaux, machines, logistique, serveurs et postes de travail, téléphonie, réseau, etc.

Cette classification est importante, car elle permet de ne rien négliger. Une atteinte à l'image de la société peut en effet s'avérer financièrement plus grave que la perte de trois serveurs informatiques suite à un incendie…

Une attention particulière sera portée par ailleurs aux matériaux à risques (explosifs, produits hautement inflammables, gaz toxiques, etc.) qui, de par leur nature, représentent un risque intrinsèque. En général, ces aspects sont traités dans des approches de type « sécurité », ayant produit des documents auxquels il sera utile de se référer.

Plusieurs sources existent dans l'entreprise pour recenser les biens tangibles :

- les fichiers des états d'amortissement, lorsqu'il y a lieu ;
- les fichiers tenus ou détenus par les gestionnaires desdits biens (dans le service informatique, par exemple) ;
- les données des bases de gestion des configurations CMDB (C*onfiguration* M*anagement* D*atabase*) dans les services informatiques qui en gèrent ;
- les données gérées par les responsables d'actifs (*asset managers*, en anglais) ou propriétaires d'actifs (*asset owners*), pour les sociétés qui ont mis en place ces concepts.

Il est cependant clair que ces listes et inventaires des actifs ne donneront hélas pas tous le même résultat. Quoiqu'il en soit, il faut raisonner à partir de groupes logiques d'éléments concourant ensemble à la bonne réalisation des processus de l'entreprise. Là encore, il faut centrer l'analyse sur la réalité des faits et les caractéristiques locales. Le tableau suivant donne un exemple.

Tableau 1-6 : Menaces sur les actifs et conséquences

Source	Événement menaçant	Actif critique	Conséquences
Fuite d'eau	Montée des eaux en salle machine	Matériel informatique	Arrêt des matériels informatiques
Tempête de neige	Routes impraticables	Ressources humaines	Compétences absentes
Erreur humaine	Pelleteuse sectionnant des câbles	Réseau IT	Réseau coupé
		Centre IT	Électricité coupée
Hackers	Accès frauduleux au web	Données confidentielles	Données confidentielles copiées
		Image de la société	Image ternie sur le marché

Arrivé à ce stade, on possède donc une liste des effets nocifs des principales menaces portant sur les principaux actifs de la société. Il s'agit maintenant de chiffrer ces effets nocifs. Une telle valorisation se révèle indispensable pour établir des comparaisons et attribuer des priorités.

Chaque fois que cela est possible, on cherchera à faire des estimations quantitatives de pertes, en euros. Dans les autres cas, on pourra recourir à des estimations qualitatives.

Valorisation quantitative des pertes

Il s'agit de répondre à la question suivante : si tel événement se produit sur les actifs considérés, combien perd la société ? L'estimation est établie pour une occurrence de sinistre, la perte se chiffrant en euros. Il faut faire preuve de bon sens et accepter d'entrer dans des raisonnements « à la louche », qui seront affinés plus tard.

L'une des approches possibles consiste à mettre en rapport la valeur totale avec le taux d'exposition, comme dans l'exemple suivant.

> **Exemple pour un site informatique**
>
> Un site informatique est valorisé à 48 millions d'euros, le matériel informatique qui s'y trouve étant évalué à 8 millions d'euros.
>
> – Une chute d'avion – qui, par hypothèse, détruit tout – provoquera une perte de 48 + 8 = 56 millions d'euros.
>
> – Une inondation du rez-de-chaussée, où se trouve le matériel informatique, pourra être estimée à 1/100 de 48 millions pour les locaux (l'immeuble ayant dix étages, et en estimant le coût des dégâts à 1/10 de la valeur de l'étage « rez-de-chaussée », donc 1/100 d'exposition *in fine*) et 8 millions pour l'informatique (car l'ensemble de l'informatique se trouve à cet étage), soit 8,48 millions d'euros.
>
> – La même inondation, sur un site où l'informatique est située dans les étages, pourra être évaluée à 1/100 du total, soit 0,56 millions d'euros (même raisonnement que précédemment sur l'immeuble, et en considérant que l'informatique subit tout de même, elle aussi, un sinistre de 1/100).

Une fois encore, l'exemple montre qu'il faut distinguer les sinistres en fonction de leurs conséquences sur les actifs.

On voit aussi qu'il faut bâtir un scénario de pertes cohérent. Il n'est pas question bien sûr de la perte réelle qui, elle, est inaccessible à l'analyse, mais d'une perte potentielle raisonnablement évaluée. Les hypothèses établies (par exemple, la valeur du bâtiment) doivent être les mêmes pour les différents scénarios étudiés. Si les hypothèses de départ changent (par exemple, si le bâtiment vaut plus cher), toutes les évaluations qui en découlent sont à revoir.

Remarquons que nous procédons ici à une évaluation des pertes dans le cas où la menace se réalise, en dehors de toute considération sur la probabilité de cette menace.

On obtient ainsi une « valeur moyenne pour perte unique » ou SLE (*Single Loss Expectancy*).

Valorisation qualitative des impacts

Pour tous les cas où il est délicat de chiffrer les pertes en euros (par exemple, dans le cas des pertes de vies humaines), on pourra procéder à des raisonne-

ments qualitatifs, consistant à évaluer le degré d'impact d'une des façons suivantes :

- qualifier l'impact de « faible », « moyen » ou « fort », ce qui a l'intérêt de donner assez rapidement une image de l'impact – en revanche, ces évaluations sont plus difficiles à manipuler lorsqu'il faut faire des calculs. La multiplication par des probabilités peut poser problème ou amener à une gymnastique mentale peu courante !
- évaluer le degré d'impact par des chiffres (1, 2, 3, par exemple) ou sur une échelle allant de 1 à 10, voire de 1 à 100 : le calcul est plus aisé, mais dans certaines situations, la tendance est alors de tout niveler dans une moyenne peu discriminante ;
- procéder à une notation en équivalents non linéaires telle que : faible = 1, moyen = 10 et fort = 100, c'est-à-dire, dans ce cas, en puissances de 10 ; elle présente l'intérêt de bien distinguer les situations, le risque étant, à l'inverse, d'être trop caricatural.

> **Exemple : perte de données informatiques**
>
> Pour chiffrer une perte de données informatiques, on pourra par exemple réaliser l'évaluation suivante :
>
> – perte de données récupérables : impact = 1 ;
>
> – perte de données clients non récupérables par les systèmes informatiques : impact = 10 ;
>
> – perte non récupérable et divulgation d'informations confidentielles : impact = 100.

Ces deux types de valorisation peuvent tout à fait être menés en parallèle, afin de comparer les impacts et les pertes. On obtient ainsi une « valeur moyenne pour impact unique » ou SIE (*Single Impact Expectancy*).

Chiffrage des probabilités annuelles

Il s'agit de calculer ou de déterminer la probabilité que l'événement considéré se produise dans une année (ART, pour *Annualized Rate of Threat occurrence*). C'est un exercice la plupart du temps difficile, car procédant par approximations successives, en commençant par des ordres de grandeurs avant d'affiner l'analyse.

Une pratique consiste à prendre les inverses des durées moyennes constatées entre deux sinistres : si un événement se produit en moyenne tous les *n* années, on lui donnera une probabilité annuelle d'occurrence (ou ART) de 1/n. Il existe un fondement mathématique derrière ce calcul, mais cela sort du champ de cet ouvrage. Pour des sinistres n'ayant jamais eu lieu, c'est plus difficile : on peut considérer la durée sans sinistre dans ce cas et prendre son inverse.

Pour du matériel, la probabilité d'occurrence d'une panne correspond, en arrondissant, à l'inverse de la « moyenne des temps de bon fonctionnement » ou MTBF, exprimée en années (voir le chapitre 7). Par exemple, pour un disque dur ayant une MTBF de 400 000 heures (soit 45,66 ans), on aura une ART de 2,2 %. Corollaire de ce calcul, si l'on dispose de cent disques de ce type au centre infor-

matique, on constatera en moyenne deux pannes par an (100 × 2,2 %). Ce constat ouvre d'ailleurs une voie pour le chiffrage des ART.

Pour d'autres événements, on raisonne plutôt par des estimations couramment partagées, telles que :

- La chute d'avion à proximité d'un aéroport aura une ART de 1/30 (proximité voulant dire moins d'un mile…). On pourra aussi considérer qu'un site situé à deux fois la distance possède une ART quatre fois moindre (2^2). On pourra aussi prendre en compte le fait que l'on se situe ou non sous une voie de passage aérien.
- L'inondation centenaire aura une ART de 1/100.
- La panne de courant due au prestataire fournissant l'électricité pourra être chiffrée avec des ART de l'ordre de 1/4 pour des pannes de cinq minutes ou 1/7 pour une panne d'une heure, par exemple, en fonction des lieux et de ce que l'on a déjà constaté.

L'annexe 2 fournit quelques références de sources de chiffres. La figure 1-1 donne un exemple de suivi des crues de la Loire.

www.vigicrues.ecologie.gouv.fr

Figure 1-1 : Les crues de la Loire constatées à Blois

En outre, il est possible de raisonner par intervalles de temps, à savoir si l'événement se produit une fois tous les dix ans ou une fois tous les cinquante ans. On en déduira les ART (c'est-à-dire les inverses : 1/10, 1/50, etc.).

Des calculs plus fins et plus approfondis peuvent aussi être réalisés à partir de méthodes d'analyse des défaillances telles que les arbres de défaillance ou les chaînes de Markov. On se reportera pour cela aux ouvrages spécialisés.

Calcul du risque

Une fois que l'on a collecté les chiffres précédents, on peut alors calculer ce qui suit :

- la moyenne des pertes annuelles attendues, de manière quantitative ;
- la moyenne des impacts annuels, estimés de manière qualitative.

Ces chiffres sont aussi appelés « risques » ou « niveaux de risque » dans le langage courant.

Moyenne des pertes annuelles (ALE)

La moyenne des pertes annualisées (ALE pour A*nnualized Loss Expectancy*) correspond au risque moyen annuel. Elle est calculée à partir de la valorisation quantitative des pertes (SLE ou S*ingle Loss Expectancy*), multipliée par la probabilité d'occurrence annuelle d'une menace (ART) :

ALE = ART × SLE

Tableau 1-7 : Calcul de l'ALE pour les exemples précédents

Source	Événement menaçant	Conséquences	SLE	ART	ALE
					En m€
Inondation	Eau au rez-de-chaussée	Locaux (site 1) et informatique inondés	8,48	0,033	0,28
		Locaux seuls inondés (site 2)	0,56	0,033	0,02
Aéroport	Chute d'avion	Locaux détruits	56	0,025	1,40
					En k€
Alimentation électrique	Coupure : 5 min	Passage sur onduleur : aucune conséquence	0	0,25	0,00
	Coupure : 1 h	Arrêt de 50 serveurs : 2 heures	2,86	0,14	0,41
	Coupure : 1 jour	Arrêt général : 1,5 jours	7 500	0,05	375,00

On remarque que les événements étudiés aboutissent à des risques très dissemblables et se situant dans des ordres de grandeurs différents (de 410 euros à 1,4 millions d'euros). Cela permet souvent de relativiser les approximations faites.

Sans aller plus loin, on peut d'ores et déjà déterminer les risques contre lesquels on souhaite agir. Les risques qui ressortent du calcul comme étant faibles ont d'ailleurs très souvent déjà été l'objet d'un effort particulier pour qu'il en soit ainsi.

Moyenne des impacts annuels (AIE)

Pour les cas où les évaluations ne se font pas en euros, la moyenne des impacts annualisés (A*nnualized* I*mpact* E*xpectancy* ou AIE) est calculée à partir de la valorisation qualitative de ces impacts (SIE ou S*ingle* I*mpact* E*xpectancy*), multipliée par la probabilité d'occurrence annuelle d'une menace (ART), elle-même évaluée sur une échelle :

AIE = ART × SIE

Tableau 1-8 : Exemples de calcul de l'AIE

Source	Événement menaçant	Conséquences	SIE	ART	AIE
Informatique	Échec dû à une montée de version mal faite	Personne ne peut travailler	4	2	8
	Panne de serveurs vitaux	Les personnes clés ne peuvent plus travailler	3	1	3
Réseau	Routeur défectueux	1/3 du personnel ne peut plus travailler	2	4	8
					Notes de 0 (faible) à 5 (fort)

Dans ces exemples, les impacts et les probabilités ont été hiérarchisés avec une échelle et des estimations réalisées par des responsables. Dans le cas présenté, on leur a demandé d'évaluer les conséquences et les probabilités sur une plage de 0 (faible) à 5 (maximum). Ce type d'approche est aussi intéressant, dans le sens où les avis des évaluateurs pouvant diverger, cette différence en soi peut fournir des informations instructives.

Lorsque l'on mène des évaluations avec des échelles, il est également possible de recourir à une grille de cotation, comme dans le tableau qui suit :

- L'axe horizontal indique la durée moyenne (en années) entre deux occurrences de sinistres (à partir de tous les cinquante ans, jusqu'à tous les ans : numérotation de 50 à 1).
- L'axe vertical indique la gravité de l'impact du sinistre (graduée de I à V, par exemple).

Tableau 1-9 : Grille d'acceptation des impacts en fonction de leur fréquence

	50	15	10	4	1
V					
IV					
III					
II					
I					

La signification des niveaux de gris est la suivante :

- blanc : acceptable ;
- gris clair : acceptable sous conditions (par exemple, s'il existe une alternative en mode dégradé) ;
- gris foncé : inacceptable.

Tel événement d'impact de niveau III sera ainsi acceptable s'il se produit tous les quinze ans ou moins souvent.

La zone moyenne (gris clair) signifie qu'il faut mener diverses actions dans le but de se retrouver dans la zone acceptable (blanc). Celles-ci viseront soit à diminuer les conséquences, soit à limiter la fréquence d'apparition des menaces.

Analyse contrastée par entités

Dans certains cas, il est intéressant de mener l'analyse décrite dans les paragraphes précédents en la détaillant, lorsque cela est pertinent, par entités de l'entreprise.

Considérons une entreprise ayant trois départements sensibles :

1. un laboratoire de recherche ;
2. un service des ventes ;
3. un service de gestion des stocks.

Le service informatique est fournisseur interne de ces trois entités. Ce service informatique a déterminé six événements menaçants, en tenant compte de son expérience, et souhaite les analyser sur les années à venir. Il demande donc à chaque département d'évaluer la probabilité d'en être victime et les conséquences que cela aurait pour lui.

Les évaluations sont effectuées sur une échelle allant de 1 (faible) à 5 (fort), au moyen d'interviews croisées, de manière à comparer les départements les uns par rapport aux autres. On obtient alors le tableau suivant.

Tableau 1-10 : Évaluation des risques par les entités

1 : faible 5 : fort		Laboratoire de recherche			Ventes			Gestion des stocks			Risque total
Événement menaçant	Conséquences	SIE	ART	Risque	SIE	ART	Risque	SIE	ART	Risque	
Passage en production bloqué	Application Start inutilisable	3	2	**6**	1	1	**1**	4	3	**12**	**19**
Problème sur traitements IT	Fichiers à j-1	1	3	**3**	4	2	**8**	5	1	**5**	**16**
Connexion au siège perdue	Base de données inaccessible	4	3	**12**	3	3	**9**	2	2	**4**	**25**
Batch de nuit non terminés	Fichiers mis en ligne tardivement	1	3	**3**	4	3	**12**	5	3	**15**	**30**
Transferts de fichiers défectueux	Fichiers non envoyés/reçus	1	2	**2**	3	2	**6**	5	2	**10**	**18**
Virus non détecté à temps	PC inutilisables	1	1	**1**	4	2	**8**	4	2	**8**	**17**
Total				**27**			**44**			**54**	**125**

Remarques sur le tableau

– *Passage en production bloqué* signifie qu'une nouvelle application n'a pas pu être démarrée correctement ; elle ne fonctionne donc pas.

– *Start* est le nom d'une application de gestion de stocks dans cette entreprise.

– *Fichiers à j-1* signifie que les fichiers sont de la veille et non pas du jour : cela peut constituer un handicap.

– *Connexion au siège perdue* signifie que le réseau permettant de connecter le siège social à l'informatique ne fonctionne pas : les gens qui travaillent au siège ne peuvent donc accéder aux bases de données.

– Les *batch de nuit* sont des traitements par lots de mise à jour de fichiers.

Lorsqu'on regarde les évaluations faites dans ce tableau, on constate que :

- Du point de vue des départements, c'est le service de gestion des stocks qui court le plus de risques (deux fois plus que le laboratoire), avec deux évaluations de risques de 12 ou plus (passage en production bloqué et batch de nuit non terminés).

- Du point de vue de l'informatique, deux événements sont plus menaçants que les autres, tous départements confondus : les batch de nuit non terminés et la connexion au siège perdue.
- On ne peut discerner un seul événement qui soit le plus menaçant pour tous les départements.
- Trois événements sont toujours classés dans les deux plus menaçants : le passage en production bloqué, la connexion au siège perdue et les batch de nuit non finis. Le service informatique voudra par conséquent faire baisser les trois plus gros risques correspondant à ces trois événements et les traitera donc en priorité.
- Le service de gestion des stocks voudra que l'on étudie le problème de transfert de fichiers défectueux, qui pour lui est son handicap numéro trois. Si le service informatique ne peut rien faire pour en réduire la fréquence, il peut réfléchir à un moyen pour réduire les conséquences de ce problème (chiffrées à 5).
- Pour le laboratoire, en revanche, le problème des batch de nuit non terminés est un souci mineur (risque 3 sur 27) alors que c'est le souci numéro un des deux autres services.

Il ressort donc de cet exemple que l'on peut coupler analyse du risque et estimation des impacts sur les différentes activités dans l'entreprise. Cette analyse est importante, car pour un même événement, la probabilité qu'il touche tel ou tel département de l'entreprise est variable. En outre, pour chaque entité touchée, l'impact ou la perte peuvent là encore être différents. Cet exemple montre aussi que les points de vue peuvent diverger selon que l'on travaille à l'informatique ou dans l'un des trois services interrogés.

Autres méthodes d'analyse pratiquées

Il existe d'autres méthodes pour analyser les risques. Certaines font appel à un attirail mathématique conséquent, d'autres sont à l'inverse le résultat d'un bon sens pragmatique. Pour l'intérêt qu'elles présentent, on citera ici la méthode dite des arbres de défaillance et la méthode des cercles concentriques.

Les arbres de défaillance

C'est une approche de haut en bas, employée en conception de systèmes techniques, qui permet une modélisation fine sur laquelle des calculs mathématiques sont réalisables. On procède de la manière suivante :

1. On définit un événement indésirable donné (la panne d'un système informatique complet, par exemple).
2. On décompose cet événement en sous-événements reliés par des relations logiques comme *et*, *ou* (par exemple : panne du serveur *ou* panne du stockage).
3. On poursuit cette décomposition jusqu'à ce qu'elle ne soit plus possible ou utile.

4. On obtient ainsi un « arbre » dont le sommet est l'événement indésirable et dont les branches sont les constituants élémentaires susceptibles de tomber en panne.

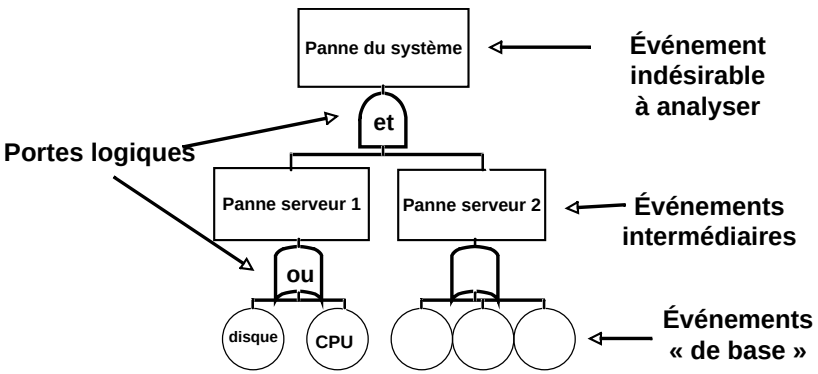


Figure 1-2 : Exemple simplifié d'un arbre de défaillance

Cette approche est très intéressante, car elle permet de :

- comprendre le système analysé ;
- mettre en évidence les principaux contributeurs aux pannes ;
- calculer des probabilités de pannes ;
- détecter les éléments qui, s'ils tombent en panne, mettent tout le système en panne : les « points uniques de défaillance ».

Il est alors possible de modifier le système pour supprimer les points uniques de défaillance, par exemple, et faire en sorte qu'une panne unique ne suffise pas à tout arrêter. Dans les systèmes les plus sensibles, on élimine de même les pannes doubles ou triples.

Les cercles concentriques

Cette méthode représente le sommet du pragmatisme réaliste. Très pratiquée outre-Atlantique, elle consiste à s'asseoir à son poste de travail et regarder autour de soi en considérant plusieurs cercles concentriques du plus éloigné au plus proche. Dans chaque cercle, on identifie les risques. Voici une description en cinq cercles.

- **Cercle 1** : ce sont les risques externes les plus éloignés, qui vont toucher tout le monde autour de l'entreprise (risques naturels, accidents d'avions, pannes d'électricité régionales, etc.).
- **Cercle 2** : c'est la zone où se situent l'entreprise, ses locaux, ses bureaux, ses accès et ses connexions et alimentations en ressources diverses ; les risques sont liés à ces éléments.

- **Cercle 3** : cela se rapproche encore un peu et touche l'environnement informatique et bureautique de travail. Les risques portent sur les données, les applications, les messageries, etc., et concernent plusieurs départements partageant les mêmes ressources.
- **Cercle 4** : on arrive ici au niveau du département, à tout risque pouvant l'empêcher de remplir ses différentes missions.
- **Cercle 5** : c'est le bureau de l'individu, avec tout ce qu'il lui faut pour travailler correctement dans son département chaque jour (moyens, système informatique) – que se passe-t-il à ce niveau en cas de défaillance ?

Cette méthode présente le mérite d'être facile à démarrer, de partager l'étude entre les différents services de l'entreprise (un cercle par service) et ainsi limiter l'oubli de certains risques (chaque risque d'un cercle devant se traduire dans ses voisins).

Dans la pratique, on pourra recourir à une combinaison de plusieurs de ces méthodes.

Évaluation des options face aux risques

Une fois les risques un peu mieux délimités dans leurs coût, impact et probabilité d'occurrence, il est temps d'étudier les différentes options qui se présentent pour y faire face.

Les quatre options de traitement du risque

Quatre options sont alors étudiées pour traiter le risque :

1. **Accepter le risque** : cela consiste à ne rien faire face au risque.
2. **Éviter ou supprimer le risque**, en sortant des conditions de sa réalisation : on effectue alors un changement important qui fait que le risque ne s'applique plus.
3. **Réduire le risque**, en jouant sur ses deux paramètres de coût/impact et de probabilité d'occurrence.
4. **Transférer le risque** à une autre entité par la sous-traitance ou l'assurance.

Tableau 1-11 : Exemples d'options de traitement du risque

Source	Option	Catégorie
Inondation	Déménager la salle à l'étage	Réduction du risque
	Déménager les locaux en altitude	Suppression du risque
Coupure d'électricité	Acquérir des générateurs	Réduction du risque
Crash d'avion	Souscrire une police d'assurance	Transfert du risque
	Répartir les bureaux sur plusieurs sites	Réduction du risque

L'étude des options doit bien évidemment tenir compte, une fois encore, de l'existant et de ce qu'il est possible de faire sans trop de difficultés.

Dans la réalité, les quatre catégories d'options sont mises à contribution simultanément. La souscription d'une police d'assurance, par exemple, s'accompagne le plus souvent de mesures de réduction du risque à un niveau économiquement supportable.

Option 1 : accepter le risque

Cette option consiste à accepter le risque tel qu'il est et à ne rien entreprendre de particulier face à lui.

Deux circonstances sont susceptibles d'amener à cette décision : soit le risque est considéré comme négligeable, soit toutes les autres options sont estimées comme trop onéreuses.

Vu de l'extérieur, accepter le risque peut paraître curieux et passer pour une démission face aux difficultés. Formalisée comme une décision de management, cette option prend toute sa force : il ne s'agit pas d'insouciance, il s'agit d'un choix réfléchi, qui doit être expliqué et documenté. Il faudra régulièrement vérifier que les motifs qui le fondent sont encore valables.

Option 2 : éviter le risque

Avec cette option, les circonstances d'apparition du risque sont totalement modifiées de manière que le risque n'ait plus lieu d'être. Par exemple, un site est déménagé en hauteur par rapport au fleuve, ou loin de tout aéroport.

Il convient alors de vérifier que de nouveaux risques n'apparaissent pas ou que ceux-ci soient désormais acceptables.

Option 3 : réduire le risque

C'est l'option la plus souvent réalisable, puisqu'il est en effet possible de jouer sur deux paramètres :

- **réduire la probabilité d'occurrence** : en faisant des travaux de terrassement, par exemple, on peut retarder la montée des eaux sur le site. Le problème des inondations et des crues du fleuve reste le même, mais la matérialisation du risque sur le site est nettement réduite ;
- **minimiser les conséquences**, une fois le risque matérialisé : en cas de coupure de courant, on met en marche un générateur électrique et la conséquence de la coupure est évitée pour les serveurs.

Réduire le risque, c'est donc modifier ce qui peut l'être raisonnablement et investir sur ce qui est efficace. En jouant sur les deux paramètres et en réalisant des actions successives, il est possible d'arriver à une réduction très efficace du risque.

Option 4 : transférer le risque

Cette option consiste à transférer le risque à un tiers qui est rémunéré pour cela. Elle se pratique sous deux formes : l'externalisation ou la souscription d'une police d'assurance.

Externalisation

Cela revient à confier à un tiers la responsabilité des moyens techniques ou humains. C'est alors ce tiers « prestataire » qui devient responsable de l'analyse des risques sur ces moyens et du choix des options face aux menaces.

Il est très important, dans ce cas, de vérifier les clauses du contrat de service qui lie désormais l'entreprise à son prestataire. Ces clauses doivent en effet mentionner des engagements de continuité de service. Différentes formes existent selon que le contrat prévoit des obligations de moyens ou des obligations de résultats.

La rédaction de ces clauses est affaire délicate. Pour l'entreprise, ces clauses constituent d'ailleurs une nouvelle forme de risque à étudier de près. Le prestataire aura tendance à exclure les risques majeurs qu'il ne souhaite pas couvrir, tandis que la société cliente devra prévoir des pénalités financières en cas de violation d'engagements de la part du prestataire.

Souscription d'une assurance

Il s'agit de souscrire un contrat auprès d'une compagnie d'assurances qui, dans le cadre des garanties contractuelles, couvrira un certain nombre de pertes.

La plupart du temps, toutes les entreprises ont au moins un contrat incendie ou perte d'exploitation. Ces contrats peuvent couvrir le coût de remplacement de serveurs incendiés ou de réfection d'un site sinistré, par exemple, ou prendre en charge des pertes de chiffre d'affaires. Il faut s'appuyer dessus en premier lieu.

Cependant, il existe aussi des contrats plus spécifiques aux « risques informatiques » qui sont apparus dans les années 1990. Ceux-ci couvrent dans une certaine limite les frais générés par un sinistre d'origine informatique : réfection de traitements, reconstitution de données, coût d'intérimaires supplémentaires et de temps machine, voire frais de réhabilitation de l'image de l'entreprise, etc.

De son côté, la compagnie d'assurances vérifie par une enquête que l'entreprise a mené des actions de prévention des risques et qu'elle possède un plan de reprise convenable. C'est d'ailleurs la limite du système : l'entreprise ne peut pas faire l'impasse sur son plan de continuité et se couvrir uniquement par l'assurance. En réalité, ces contrats « risques informatiques » rencontrent un succès très mitigé et semblent se cantonner plutôt aux PME.

Le chiffrage coût/efficacité

Chaque option choisie possède deux caractéristiques :

- elle représente un certain coût de mise en œuvre, composé généralement d'une fraction ponctuelle et d'une fraction récurrente ;
- elle permet une diminution du risque, soit en limitant l'impact d'une menace, soit en réduisant sa probabilité d'occurrence.

Ces coûts et ces diminutions de risque peuvent être évalués et chiffrés, afin de procéder à des comparaisons.

Coûts de mise en œuvre des options

Le tableau suivant donne un exemple d'options et de chiffrage des coûts associés.

Tableau 1-12 : Exemples de coûts de différentes options

Source	Option de maîtrise	Catégorie	Coût de l'option
Inondation	Déménager la salle à l'étage	Réduction du risque	300 000 €
	Déménager les locaux en altitude	Suppression du risque	1 500 000 €
Coupure d'électricité	Acquérir des générateurs	Réduction du risque	100 000 € + maintenance
Crash d'avion	Souscrire une police d'assurance	Transfert du risque	1 million d'euros/an, soit 20 millions sur 20 ans
	Répartir les bureaux plus loin, sur trois sites	Réduction du risque	600 000 €, car ces sites existent déjà

À ce stade, certaines options peuvent être éventuellement exclues, étant considérées comme trop onéreuses. Le document de cadrage dans le dossier d'étude des risques (voir page 30) doit statuer sur ce point.

Le chiffrage du coût de mise en œuvre d'une option sera réalisé avec le plus grand soin, car il aura un effet sur les scénarios proposés. Les éléments suivants doivent être pris en compte :

- coût des équipements à acquérir et amortissement ;
- frais financiers associés aux acquisitions ;
- coût de la maintenance des équipements acquis ;
- éventuels logiciels associés ;
- déménagements ;
- services divers à envisager ;
- taxes et impôts ;
- gestion et administration des biens acquis ;
- assurances ;
- frais de formation du personnel concerné ;
- frais de location, etc.

En général, chacun de ces éléments génère des coûts ponctuels et récurrents. Il est donc intéressant d'analyser les coûts en fonction du moment où ils apparaissent (immédiatement ou plus tard : chaque mois, chaque année, etc.) et de réaliser ensuite un calcul d'actualisation à la date prévue de la mise en œuvre de l'option.

Chiffrer la réduction du risque

Le chiffrage de la diminution du risque procurée par une option est délicat et doit se faire avec la même logique que le chiffrage du risque, en utilisant le même type d'arguments. On peut aussi chiffrer le risque résiduel une fois l'option mise en place et ainsi en déduire la baisse.

Tableau 1-13 : Exemples de chiffrage de réduction du risque

Menace (et perte moyenne annuelle attendue)	Option de maîtrise	Coût de l'option	Risque résiduel	Réduction du risque
Inondation (ALE : 280 k€)	Déménager la salle à l'étage	300 000 €	30 000 €	250 000 €
	Déménager les locaux en altitude	1 500 000 €	0 €	280 000 €
Crash d'avion (ALE : 1,4 m€)	Souscrire une police d'assurance	1 million d'euros par an, soit 20 millions sur 20 ans	0 €	1,4 m€
	Répartir les bureaux plus loin, sur trois sites	600 000 €, car ces sites existent déjà	0,47 m€ (1/3 de 1,4 m€)	0,93 m€

Il devient alors possible de comparer le coût de l'option et la diminution du risque qu'elle apporte en calculant le ratio suivant, appelé « coût par unité de réduction du risque » (CURR, pour *Cost per Unit of Risk Reduction*) :

$$\text{CURR} = \frac{\text{coût de l'option}}{\text{diminution du risque due à l'option}}$$

Un CURR de 1,20 euro peut se comprendre ainsi : pour réduire le risque moyen annuel de 1 euro, il faut dépenser 1,20 euro.

Tableau 1-14 : Calcul du CURR à partir des exemples précédents

Menace (et perte moyenne annuelle attendue)	Option de maîtrise	Coût de l'option	Réduction du risque	CURR
Inondation (ALE : 280 k€)	Déménager la salle à l'étage	300 000 €	250 000 €	1,20 €
	Déménager les locaux en altitude	1 500 000 €	280 000 €	5,36 €
Crash d'avion (ALE : 1,4 m €)	Souscrire une police d'assurance	1 million d'euros par an, soit 20 millions sur 20 ans	1,4 m€	0,7 € récurrent
	Répartir les bureaux plus loin, sur trois sites	600 000 €, car les sites existent déjà	0,93 m€	0,65 €

Dans l'exemple du déménagement, ce coût ne se présente qu'une seule fois, alors que le risque survient tous les ans. On voit là qu'il faut bien analyser la manière dont les coûts se présentent et sont calculés, en prenant en compte le fait que ces coûts soient uniques ou récurrents. On gardera aussi en mémoire que le risque est calculé sur un an, c'est-à-dire qu'il s'agit d'une *espérance* (au sens mathématique du terme), qui se présente tous les ans. Un classement des options en fonction des meilleurs ratios est alors possible.

Si l'on ne dispose pas de chiffres quantitatifs, mais uniquement d'une évaluation qualitative graduée (par exemple : faible, moyen, fort) et d'une grille de cotation du niveau de risque (voir page 19), on listera alors toutes les options qui permettent de sortir de la zone noire. On sera alors enclin à privilégier la moins coûteuse.

L'aversion au risque

Beaucoup d'ouvrages se sont penchés sur cette notion appliquée aux investisseurs en Bourse. En ce qui concerne la continuité d'activité, il est intéressant de noter les écarts de comportement entre les différents responsables de l'entre-

prise. En effet, le niveau de sensibilité au risque est variable, que ce soit au sujet des pertes ou des probabilités d'occurrence. À risque égal, on pourra constater les situations suivantes :

- Certains responsables ne voient que le montant des pertes et oublient – ou mettent au second plan – la faible probabilité d'occurrence : ils auront tendance à vouloir faire face aux risques rares mais induisant de forts coûts.
- D'autres, à l'inverse, sont sensibles surtout à la probabilité élevée et voudront supprimer des risques probables, même si leur conséquence est faible. Les probabilités faibles ne les intéressent pas.
- Enfin, la plupart sont sensibles surtout au coût des options de traitement du risque, quel que soit le coût du risque. Une option trop chère sera refusée.

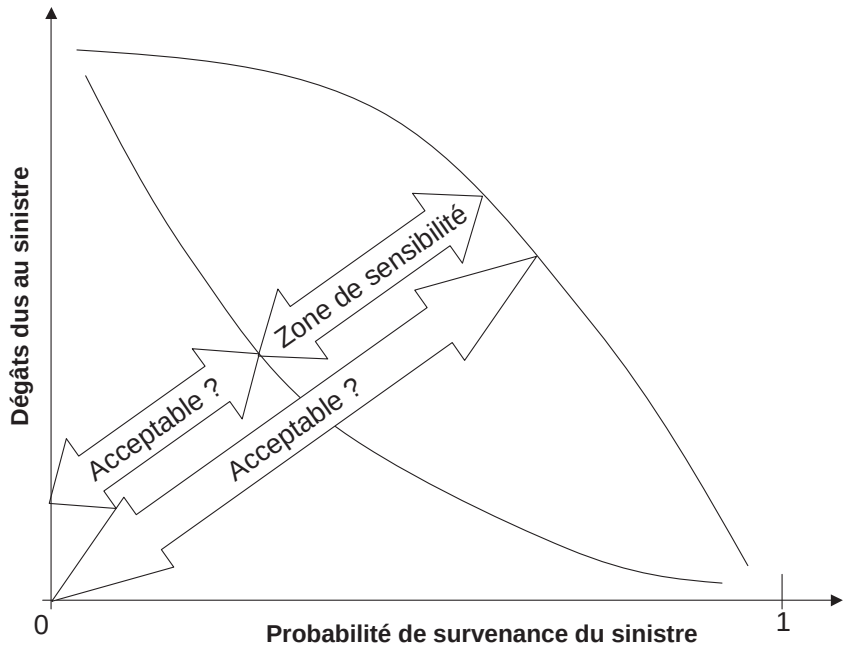


Figure 1-3 : Zone d'aversion variable au risque

Tout ceci peut expliquer que, face à des risques similaires, plusieurs responsables peuvent faire des choix d'options différents.

Le dossier d'étude des risques

L'ensemble des études qui précèdent doit être documenté dans un dossier. Celui-ci a trois objectifs :

- décrire la réflexion et les études qui ont été menées ;
- expliquer pourquoi tel aspect a été examiné ou, au contraire, pourquoi tel autre point a été mis de côté ;
- préparer la décision du comité de continuité.

La première partie de ce dossier correspond au document de cadrage mentionné plus haut.

Voici un plan type pour constituer un tel dossier.

Dossier d'étude des risques et options

1. Cadrage de la démarche
   - 1.1. Périmètre concerné
   - 1.2. Hypothèses pour les évaluations
   - 1.3. Méthode d'évaluation
   - 1.4. Sources de risque
   - 1.5. Limites de coûts et de risques acceptables
2. Menaces et risques identifiés
   - 2.1. Critères de sélection
   - 2.2. Découpages réalisés
   - 2.3. Entités de l'entreprise les plus concernées
   - 2.4. Exclusions éventuelles
   - 2.5. Techniques d'analyse
3. Actifs exposés aux menaces
   - 3.1. Catégories d'actifs retenus
   - 3.2. Groupes effectués, logique d'approche
   - 3.3. Implication des responsables d'actifs
4. Analyse des options de traitement du risque
   - 4.1. Hypothèses de chiffrage
   - 4.2. Chiffrage des coûts de réalisation
   - 4.3. Chiffrage de la réduction de risque
   - 4.4. CURR
   - 4.5. Description des effets et perturbations
5. Synthèse et préconisations
   - 5.1. Sélection d'options proposées ou éliminées
   - 5.2. Décisions à entériner
   - 5.3. Décisions ouvertes
   - 5.4. Calendrier d'exécution
   - 5.5. Suites à donner

La réalisation de ce dossier peut être partiellement itérative, afin d'impliquer correctement tous les responsables concernés par le sujet de la continuité d'activité.

Ce document peut également être découpé pour des raisons diverses (géographie, responsabilités différentes, sensibilité aux risques variable, etc.). Concrètement, cela pourra se traduire de la manière suivante :

- les sites industriels de l'entreprise étant traités séparément, il existe donc un document de ce type par site ;
- les risques d'origine humaine ne sont pas inclus dans le document, mais sont traités succinctement dans un autre dossier classé confidentiel ;
- seule la France (par exemple) est prise en compte dans l'analyse ;
- les options de maîtrise du risque dépassant un certain coût sont juste mentionnées mais ne sont pas traitées plus avant.

Enfin, il existe aussi des mises à jour ou des documents dits « delta » qui ne couvrent que ce qui a changé par rapport à une étude réalisée précédemment.

Prise de décision

Le dossier et ses préconisations sont ensuite soumis aux responsables de l'entreprise pour décision. Il est fréquent que la direction générale mette en place un comité de continuité pour centraliser la décision sur ces points. On se reportera aux chapitres 11 à 13 pour plus de détails sur la gouvernance de la continuité.

Réévaluation des options par le comité décisionnaire

Ayant ainsi en main tous les éléments, le comité de continuité prend les décisions qui s'imposent et lance les actions retenues. Il n'est alors pas rare qu'il procède à des reclassements d'options ou des requalifications.

- Face à certaines menaces, il est décidé de ne rien faire : il s'agit souvent de menaces communes à plusieurs entreprises, pour lesquelles la même attitude est adoptée.
- Le niveau de sensibilité au risque peut être réévalué, et cette modification entraîner le fait que l'option d'acceptation du risque est plus (ou moins) souvent choisie.
- Certains impacts sont requalifiés, en particulier tout ce qui concerne la réputation de l'entreprise, et qui peut être porté plus haut en termes d'impact et de conséquences sur l'image de l'entreprise auprès du grand public ou sur son marché.
- Des priorités dans le temps sont souvent affectées ou réaffectées : les options retenues devront se réaliser selon un calendrier précis, différent de celui préconisé au départ.

- Certaines options, séduisantes sur le papier, peuvent être écartées en raison de leur difficulté de mise en œuvre en parallèle des affaires courantes. C'est le cas notamment lorsque la réalisation de l'option nécessite un arrêt d'activité jugé préjudiciable à l'entreprise. Certaines options peuvent ainsi être réétudiées sous cet angle.
- Certaines options prévues dans l'étude pour toute l'entreprise pourront voir leur application limitée à un seul site, par exemple, ou à un seul département de l'entreprise.
- Plutôt que de généraliser une option à l'entreprise entière, il peut être décidé de ne commencer que sur un site ou un département, sous forme de projet pilote.

Toutes ces décisions sont entérinées par écrit.

Documentation de l'ensemble

Suivant l'objectif de traçabilité de la démarche, un document est constitué à partir des éléments suivants :

- le dossier d'étude des risques, comprenant sa partie de cadrage ;
- un relevé des décisions prises en comité de continuité ;
- éventuellement, un suivi spécial d'études complémentaires à mener.

Il peut être intéressant de conserver cet ensemble dans un environnement identifié. Certaines approches réglementaires demandent en effet que des auditeurs, par exemple, puissent accéder à ces documents et y vérifier la présence de certains éléments (voir le chapitre 13).

Mise en œuvre des options

La mise en œuvre des options de maîtrise des risques se traduit concrètement par le lancement de divers projets. On utilisera alors les méthodes et outils de gestion de projets en vigueur dans l'entreprise. Il est important toutefois de considérer quelques aspects propres au sujet abordé qui seront approfondis dans le chapitre 12.

- Il peut s'avérer nécessaire d'approfondir la faisabilité de certaines options, ce qui entraînera de possibles révisions de budget, à reporter au comité de continuité.
- Un budget spécifique a probablement été alloué à la continuité : un suivi spécial est alors nécessaire pour bien décompter les engagements, les consommations de ressources et constater la baisse effective du « reste à faire ».
- L'ensemble des actions à mener doit faire l'objet d'une coordination générale consacrée à la continuité, afin de mettre à profit les synergies et de limiter – en les regroupant – les perturbations sur les affaires courantes.

Un comité de suivi de la continuité est nécessaire pour prendre en charge ces préoccupations. Il est en effet intéressant de faire suivre tous ces projets par un

comité *ad hoc*, impliquant aussi bien des professionnels de la continuité que les opérationnels de terrain et les dirigeants de l'entreprise.

Enfin, comme dans tout projet, il ne faut pas oublier la finalité des actions menées pour ne pas changer implicitement de direction en cours de route.

Suivi et contrôle des plans d'actions

Le choix des options ayant abouti à la mise en œuvre des plans d'actions correspondants, il est indispensable d'assurer un suivi de ces actions. Il faut en effet régulièrement contrôler :

- que les hypothèses émises lors de l'appréciation des risques sont toujours valables ;
- que de nouveaux éléments ne sont pas apparus, nécessitant de recommencer l'analyse – et s'il y en a, que l'analyse décrite précédemment est bien reprise ;
- que la société n'a pas connu de modification majeure nécessitant une révision de l'étude : par exemple, en cas de fusion/acquisition ou, au contraire, de cession de l'entreprise, le périmètre, les actifs et les activités peuvent avoir changé, et l'étude devra donc être réitérée.

Des audits réguliers pourront être organisés pour s'assurer que les trois points précédents sont bien vérifiés.

Dans la réalité, les plans d'actions établis auront suivi des voies diverses : certains seront achevés, d'autres en cours, tandis que d'autres n'auront pas encore été lancés. Quelle que soit la situation de ces plans d'actions, le suivi doit avoir lieu et produire un document.

Ce suivi fait partie des actions de contrôle de la continuité d'activité et du maintien en condition du plan (voir les chapitres 12 et 13).

Chapitre 2

L'analyse d'impact sur les activités

L'analyse d'impact sur les activités (B*usiness* I*mpact* A*nalysis* ou BIA), appelée parfois aussi « bilan de l'impact sur l'activité » afin de mieux correspondre au sigle anglais BIA, consiste à étudier comment les sinistres, lorsqu'ils se produisent, affectent le déroulement des activités de l'entreprise. L'attention se porte sur les activités dites critiques, c'est-à-dire les plus vitales pour l'entreprise et dont la perte est la plus grave pour elle.

On examine les divers impacts du sinistre (financiers, organisationnels ou en termes d'image). On envisage aussi de quelle manière l'activité critique peut continuer et la situation revenir à un mode acceptable de fonctionnement, provisoire puis définitif.

Chronologie d'un sinistre

Le fil conducteur de cette étude est le temps. On considère la période qui va des derniers préparatifs avant le sinistre jusqu'au retour à la normale et à la récupération totale. La figure suivante aide à visualiser la chronologie détaillée ci-après.

Déroulement d'un sinistre

Typiquement, le déroulement d'un sinistre et le développement de ses conséquences sur l'activité d'une entreprise peuvent se décomposer en cinq étapes, comme le montre le schéma ci-après.

1 – Situation normale

Avant que le sinistre ne se produise, tout est normal et les activités sont menées convenablement. Les actions de prévention ou de protection sont aussi effectuées régulièrement et comme prévu, en particulier les sauvegardes et mises en sécurité des actifs importants (données, matières, etc.). Cela concerne notamment l'informatique et les moyens techniques divers utilisés.

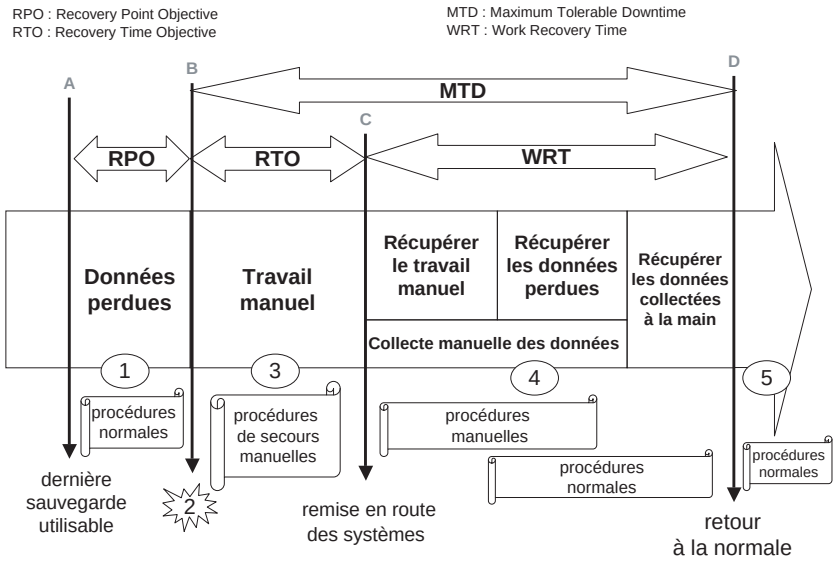


Figure 2-1 : Déroulement d'un sinistre et impacts sur les activités

Sur le schéma, la flèche A indique la dernière sauvegarde ou le dernier point de récupération utilisable.

2 – Occurrence du sinistre

Le sinistre a lieu (flèche B), causant la perte de moyens utiles à l'entreprise, qui ne peut alors plus travailler normalement. On prend en compte ici le moment effectif du sinistre, c'est-à-dire le moment où les ressources en subissent l'impact. Il se peut que le sinistre lui-même ne soit découvert que plus tard.

Assez souvent d'ailleurs, le sinistre est découvert rapidement mais son ampleur n'est précisée qu'après coup. Il arrive aussi que le sinistre ne soit pas ponctuel, comme dans le cas d'un incendie découvert mais non maîtrisé, dont on n'évaluera les dégâts qu'une fois celui-ci éteint.

Lorsque la situation est éclaircie, on est alors en mesure de savoir à partir de quel point de sauvegarde les données pourront être récupérées. Ce point est appelé RPO (*Recovery Point Objective*), c'est-à-dire « point cible de récupération ». Par facilité, on appelle aussi RPO le délai observé entre ce point de sauvegarde et le sinistre.

Lors d'un sinistre de grande ampleur, on peut observer plusieurs RPO pour plusieurs systèmes différents. En outre, dans des situations complexes, lorsqu'il est impossible de récupérer les données à partir de la dernière sauvegarde, il est parfois nécessaire de revenir plus loin en arrière, ce qui allonge ce délai de RPO.

3 – Travail en mode dégradé

Le sinistre s'étant produit, l'entreprise ne peut plus travailler normalement : elle travaille en mode dégradé.

Les situations peuvent varier, mais il est bon d'avoir prévu ce mode dégradé ainsi que des façons de contourner les impacts du sinistre. Durant cette période, on aura généralement recours au travail manuel, tandis que d'autres équipes chercheront à récupérer des moyens (informatique, locaux, etc.) permettant de travailler selon des procédures normales.

Le délai entre le sinistre et la récupération de ces moyens est appelé RTO (*Recovery Time Objective*) ou « temps de récupération cible ». Ces « moyens permettant de travailler » ne correspondent pas forcément aux moyens habituels. Par exemple, durant cette période, des données seront créées manuellement, par écrit, à l'aide de formulaires papier.

4 – Récupération des moyens

À partir de la remise en route de certains moyens informatiques à nouveau disponibles (flèche C), deux types d'activités sont menés en parallèle : les activités normales, éventuellement dégradées, et des activités consistant à compléter la restauration du système informatique en y entrant ce qui a été perdu ou généré manuellement. Cela consiste à récupérer les données à partir des sauvegardes, effectuer des traitements de récupération, entrer dans le système les transactions réalisées à la main, en bref, collecter et saisir toute donnée nécessaire au bon fonctionnement de l'entreprise.

Durant cette période, on observe une superposition de procédures normales et d'opérations manuelles. Sa durée est désignée comme WRT (*Work Recovery Time*) ou « temps de récupération du travail ».

Cette période se termine lorsque toutes les données et transactions ont été saisies dans le système et que les moyens sont à nouveau disponibles pour travailler normalement. Il arrive assez souvent que ces moyens ne correspondent pas tout à fait aux moyens existant avant le sinistre, et que certains d'entre eux soient externalisés chez un prestataire ou délocalisés sur un site de secours.

5 – Retour à la normale

À partir de ce moment (flèche D), l'impact du sinistre n'est théoriquement plus visible et l'activité de l'entreprise a repris dans des conditions normales. Il se peut que certains travaux restent encore à effectuer (au niveau de l'informatique ou des locaux), mais l'impact sur les activités, obligatoirement limité, est alors considéré comme nul.

Du point de vue de l'utilisateur…

Au-delà de cette vision générale technique, l'utilisateur professionnel derrière son bureau aura un tout autre point de vue sur ses outils et sa capacité à tra-

vailler dans la situation d'après sinistre. Il constate en effet plus simplement qu'il y a une période durant laquelle il ne peut pas ou presque travailler puis que, au bout d'un certain temps, tout est redevenu normal. C'est ainsi que l'on définit la « durée d'indisponibilité maximale tolérable » pour l'activité ou MTD (*Maximum Tolerable Downtime*). Le MTD est donc en quelque sorte un « seuil de douleur » fixé par les responsables de chaque activité.

Les délais de récupération RTO et RPO définis précédemment sont imposés par la technique et les divers choix qui ont été faits pour les sauvegardes, par exemple. Le temps de récupération du travail (WRT) est dépendant de l'efficacité des travaux faits à la main, des données saisies sur formulaires, des événements commerciaux ayant eu lieu durant le sinistre, etc. Le MTD, quant à lui, est un paramètre d'exigence émanant de chaque métier.

Comme on le voit sur le schéma, on a ainsi l'équation :

MTD = RTO + WRT

Il faut donc s'assurer que cette équivalence est réalisable. En effet, le membre de gauche (MTD) est *décidé*, tandis que celui de droite (RTO + WRT) est *subi*.

En général, on remarque que plus le point cible de récupération des données (RPO) est éloigné dans le temps, plus le temps de récupération cible (RTO) le sera également. En effet, logiquement, plus la quantité de données perdues est importante, plus les traitements à réaliser pour les récupérer demanderont de temps. D'autre part, il est fort probable que les moyens informatiques disponibles soient sous-dimensionnés pour un tel surcroît de travail. Il sera alors souvent nécessaire de travailler de nuit, les moyens de restauration n'étant pas disponibles durant la journée. Cela demande par ailleurs de prévoir des moyens supplémentaires.

Réduire la durée maximale d'indisponibilité tolérable (MTD) demandera donc d'abaisser le RTO (et par conséquent le RPO), ainsi que de diminuer le temps de récupération du travail (WRT).

Bien évidemment, tous ces chiffres RPO, RTO, WRT et MTD varient en fonction du type d'activités de l'entreprise et des moyens techniques employés lors de la survenue d'un sinistre.

Cadrage de l'analyse

Une fois le décor planté, il s'agit de mener une analyse d'impact des sinistres sur les activités. La première chose à faire est de définir le cadre dans lequel celle-ci est réalisée. Il faut en particulier déterminer son périmètre, ses objectifs et certaines hypothèses à prendre en compte.

- **Le périmètre** : considère-t-on l'ensemble de la société ou bien un site, une activité ou un service en particulier ? Comment l'étude sera-t-elle découpée en fonction de cela ? Comment délimite-t-on les activités ?
- **Les éventuelles études déjà menées sur ce sujet ou d'autres études connexes** que l'on pourra prendre comme point de départ (analyses de processus, par exemple).
- **Les éléments techniques** : considère-t-on le système informatique seul ou aussi les locaux ? Inclut-on dans l'étude le domicile des employés, leur ordinateur personnel (en secours), ou des sites de prestataires externes ?
- **Les objectifs de l'étude** : que cherche-t-on exactement ? Vise-t-on à déterminer les activités les plus exposées ou plutôt à chiffrer des pertes potentielles, ou encore à déterminer des priorités ? Veut-on simplement mesurer les écarts entre ce que l'on imagine et la réalité ?
- **Les méthodes employées** : procédera-t-on par groupes de travail, par interviews de responsables ou par analyse technique des moyens existants ?
- **Les aspects financiers** : veut-on estimer les coûts du plan de continuité à venir ou fixer un coût à ne pas dépasser ? Préfère-t-on imaginer plusieurs scénarios avec différents niveaux de coûts ?
- **Les éventuelles exclusions de l'étude**.
- **Toute hypothèse jugée intéressante à étudier**, telle que la non-existence d'un site de secours ou le fait que les pics d'activité doivent être rendus possibles même par les moyens de secours, ou encore que les données ne peuvent sortir du site, etc.

Cette étape aboutira à une meilleure compréhension, partagée avec la direction générale, de ce que l'analyse d'impact sur les activités peut et doit produire. Elle est formalisée dans un document intitulé « note de cadrage » (voir en fin de chapitre).

Déterminer les activités critiques

Les activités critiques sont celles dont la disparition endommage le plus l'entreprise, car elles en constituent le fondement. Ces activités critiques feront l'objet d'une attention renforcée en cas de sinistre. Elles bénéficieront de moyens plus résilients et seront privilégiées dans les actions de reprise et de redémarrage.

Un exercice difficile

Cette étude des activités de l'entreprise est un exercice difficile. Toute la difficulté consiste à obtenir une vision partagée de ce que sont ces activités jugées critiques. En effet, chaque responsable aura probablement tendance à citer son activité comme étant critique, alors qu'il existe certainement des activités plus critiques que les autres : comment choisir ?

Une autre difficulté provient du fait que l'entreprise n'a pas forcément réalisé au préalable une description de ses activités. Avant de savoir laquelle est critique, il faut obtenir une liste des activités suffisamment descriptive.

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 11) 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.

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.

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

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.

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 « 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

		Impact de la perte : 0 (nul) à 5 (très fort)				Note finale
Fonction	**Processus**	**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**
	Coefficient retenu	**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.

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.

Tableau 2-5 : Évaluation des processus critiques sélectionnés

		Impact de la perte : 0 (nul) à 5 (très fort)				Note finale
Fonction	**Processus**	**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**
	Coefficient	**2**	**1**	**2**	**1**	

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

		Gravité : 0 (nulle) à 30 (très forte)		
Fonction	**Processus**	**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

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.

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.

Systèmes 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.

Tableau 2-7 : Exemples de systèmes et applications critiques

Fonction	Processus	Applications et systèmes critiques
Vente	Prise de commandes	Téléphonie Application *Vador* sur Unix, site de Lyon
Marketing	Gestion du catalogue	Serveurs web de gestion du catalogue, site de Lyon et hébergeur
	Gestion des partenaires	Application *Agépar* 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

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 applica-

tions 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.

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).

Autres ressources critiques

Pour terminer, il convient de lister également les autres ressources nécessaires au bon fonctionnement des processus critiques. 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.

Tableau 2-8 : 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

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.

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

Rappellons 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 2-9 : Détermination des RTO et WRT

Fonction	Processus	Applications et sytèmes 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 au maximum.

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 2-10 : 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 abréger 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 maximum.

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 *batch*) ;
- 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).

Tableau 2-11 : Exemples de RPO

Fonction	Processus	Applications et systèmes critiques	RPO
Vente	Prise de commandes	Téléphonie Application *Vador* 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 *Agépar* 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

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).

Procédures de secours

Les procédures de secours 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.

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 13).

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

Chapitre 3

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 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 maximum 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.

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 12) 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

Sites informatiques de secours		
Catégorie	**Option**	**Description**
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 ci-après).

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

Sites informatiques de secours		
Catégorie	**Option**	**Description**
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).

3. Données et enregistrements critiques

En ce qui concerne les données et enregistrements critiques, une attention particulière doit être portée à la capacité à reconstruire les données opérationnelles. Pour plus de précision sur les aspects techniques, on se reportera à la Partie III de cet ouvrage.

Tableau 3-5 : Options pour les données critiques

Données critiques		
Catégorie	**Option**	**Description (voir Partie III)**
Fréquence des sauvegardes	Continu	Sauvegarde en continu par réplication à distance
	Quelques minutes	Cliché (*snapshot*) toutes les 3 minutes, par exemple (stockage en réseau NAS)
	Jour	Sauvegarde une fois par jour
	Semaine	Sauvegarde une fois par semaine
	Mois	Sauvegarde une fois par mois
Type de sauvegarde	Complète	Complète, sur tous les fichiers
	Incrémentielle	Uniquement ce qui a été modifié depuis la sauvegarde précédente
	Différentielle	Uniquement ce qui a changé depuis la dernière sauvegarde complète
Technologie de sauvegarde	Miroir distant (*remote mirroring*)	Copie de disque à disque, par contrôleur, par exemple
	Propagation de log de SGBD	Le système de gestion de base de données propage son journal sur un site distant
	Bandes	Copie sur bandes stockées hors site

Afin de faciliter la prise de décision, il est également possible de mentionner les avantages et les inconvénients de chaque option. On se reportera au chapitre 8 pour plus de précision sur ces points.

Enfin, cette analyse ne doit pas omettre les dossiers non informatiques que l'on peut dupliquer, mettre dans des armoires ignifuges ou conserver en double sur deux sites, par exemple.

4. Production industrielle et fabrication

Pour la production et la fabrication industrielles, là encore, de nombreuses solutions sont susceptibles d'être proposées à l'étude.

Tableau 3-6 : Options pour les équipements de production

Équipements et ressources critiques de production		
Catégorie	**Option**	**Description**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	L'équipement est acquis lorsque le sinistre a lieu.
	Acquisition des pièces détachées	Acquisition des pièces en fonction des besoins après le sinistre
Préétabli	Contrat de service pour le sauvetage et la restauration	Contrat pour sauver et restaurer tous les équipements endommagés, souscrit, avant le sinistre, auprès d'un fournisseur externe.
	Maintien d'un stock de secours pour les pièces critiques sur un site distant	Le stock de pièces critiques est maintenu sur un site de secours à distance avant le sinistre.
	Maintien d'équipements de secours pour les équipements critiques, sur un site distant	Les équipements critiques sont maintenus sur un site de secours à distance avant le sinistre.
Stock de secours de matières premières	Maintien dans un entrepôt de secours des stocks de matières premières ou produits intermédiaires nécessaires durant la reprise	Ces matériels et produits sont stockés à l'avance sur un site distant.
Site de production alternatif	Utilisation d'un site distant de la société, vide	Site équipé de certains moyens : alimentations électriques, chauffage, sprinklers, air conditionné, etc.
	Réparation, reconstruction du site sinistré	Le site endommagé est reconstruit ou réparé, totalement ou partiellement.

Comme dans les autres analyses, un compromis est établi entre ce qui est souhaitable et ce qui est réalisable.

Phase 3 – Confrontation des options aux exigences métier

Une fois toutes les options possibles passées en revue, celles-ci devront être confrontées aux exigences de chaque activité, telles qu'elles ont été définies dans l'analyse d'impact (BIA). En éliminant les options non compatibles avec les besoins exprimés, notamment en termes de délais, cette phase permet de pro-

céder à une première sélection, avant d'effectuer une évaluation multicritère (coût/faisabilité).

Cette confrontation se fait en deux étapes.

1. Les options listées précédemment sont passées en revue pour déterminer leur rapidité de mise en œuvre ou « délai d'activation » en cas de sinistre.
2. Ce délai de mise en œuvre est alors comparé aux besoins émis par les métiers sur leurs activités critiques, permettant ainsi de retenir les options donnant satisfaction.

Définition des délais d'activation

Cet aspect est fondamental car, en cas de sinistre et d'activation de l'option considérée, il convient de se conformer aux exigences de délai imposées alors que le chronomètre court.

Les options listées précédemment sont étudiées afin de mettre à jour les diverses préoccupations ou problèmes de réalisation potentiels, ce qui permet d'aboutir, pour chacune d'entre elles, à l'évaluation de leur EAT (*Expected Availability Time*) ou « délai moyen d'activation ».

En effet, si ce délai moyen d'activation est supérieur aux exigences métier, cela nécessitera de revoir l'option, en l'éliminant ou en l'améliorant.

Par souci de cohérence, la même segmentation que lors des autres phases est retenue pour étudier les différents paramètres d'activation des options.

1. Bureaux et locaux de travail

Le tableau ci-après présente, pour les options citées en exemple, les obstacles principaux à une mise à disposition rapide.

Tableau 3-7 : Difficultés prévisibles pour chaque option envisagée

Locaux et bureaux		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Solution contractuelle avec fournisseur externe	Site mobile	Distance à parcourir, conditions de circulation (météo, trafic), encombrements pour un convoi exceptionnel.
	Salles de réunion d'hôtel	Si le sinistre est régional, tous les hôtels sont pris ou sinistrés.
	Site fixe	Distance, conditions de circulation et d'accès.
Solution interne à l'entreprise	Autre site de l'entreprise	Idem, en ajoutant les causes communes (par exemple, les grèves).
Recours à l'employé	Travail à la maison	Difficultés de mise en place de la solution technique pour les employés et la sécurité.

Il est aussi intéressant d'étudier d'autres aspects, tels que ceux liés au degré de préparation opérationnelle ou à l'ouverture des locaux et bureaux de secours, ainsi que du centre de crise (voir le chapitre 4).

Tableau 3-8 : Difficultés à envisager pour la préparation des locaux, bureaux et centre de crise

Locaux, bureaux et centre de crise		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Niveau de préparation opérationnelle	Site froid	Préparer le site, le configurer, installer, connecter, etc. Les tâches peuvent s'avérer très longues.
	Site tiède	Les compléments, les paramétrages et les connexions peuvent prendre du temps (1 jour ?).
	Site chaud	Normalement disponible rapidement si c'est bien géré (quelques heures).

Remarque : disponibilité des sites

Le centre de crise (voir le chapitre 4) est encore plus sensible que les autres types de locaux. Il doit être ouvert le premier.

Tableau 3-9 : Préoccupations lors du déclenchement

Locaux, bureaux et centre de crise		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Méthode de recours	Préétabli	Normalement c'est une solution préparée donc rapide. Attention aux évolutions non reportées. Il faudra faire des tests.
	Préarrangé	Bien, si les engagements sont tenus. Prévoir du temps et des ressources humaines aguerries pour les installations, configurations, paramétrages, etc.
	Cas par cas	Selon les circonstances et types de besoins, les ressources peuvent mettre du temps à se mettre en place. À réserver au matériel standard ?

2. Systèmes, infrastructures et locaux informatiques

Pour les options concernant les sites informatiques de secours, plus ou moins équipés des matériels et systèmes nécessaires, on s'attachera à des préoccupations telles que celles présentées dans les tableaux ci-après. Les difficultés mentionnées doivent permettre rapidement de retenir ou d'éliminer une option.

Tableau 3-10 : Difficultés prévisibles pour chaque option envisagée

Matériel sur les sites informatiques de secours		
Catégorie	**Option**	**Préoccupations et délais**
En toute propriété	Site distant appartenant à la société	La distance du site, l'état des routes, le temps pour y aller peuvent avoir un effet sur les délais.
	Site mobile	Idem, en ajoutant les connexions réseau à effectuer.
Accord avec un tiers	Accord de réciprocité avec un confrère	Les délais dépendent ici de la préparation ou non du site, de la réaction du partenaire (qui peut, dans les cas extrêmes, avoir lui-même subi un sinistre), de la distance et de l'état des routes, etc.
Offre commerciale	Site dédié (offre du marché)	La distance, le besoin de personnel sur place influencent les délais.
	Site partagé (offre du marché)	Site utilisé en totalité ou en partie, conséquences de l'occupation par d'autres clients, éloignement et facilité d'accès.

Tableau 3-11 : Difficultés à considérer pour la préparation des sites de secours

Matériels sur le site de secours		
Catégorie	**Option**	**Préoccupations et délais**
Niveau de préparation opérationnelle	Site froid	Il faut équiper le site : problèmes d'acquisition d'équipements, de démarrage, d'installations diverses, de paramétrages, qui peuvent aller jusqu'à 7 jours.
	Site tiède	Les équipements supplémentaires et les installations puis les paramétrages peuvent prendre de 1 jour à 5 jours.
	Site chaud	Normalement disponible rapidement (de 15 minutes à quelques heures).

3. Données et enregistrements critiques

En ce qui concerne les données et enregistrements critiques, une attention particulière sera portée à la rapidité de reconstruction des données opérationnelles. Rappelons que les moyens techniques utilisés sont expliqués plus en détail dans la partie III.

Tableau 3-12 : Caractéristiques et délais pour chaque option concernant les données critiques

Données critiques		
Catégorie	**Option**	**Problématique et délais**
Fréquence des sauvegardes	Continu	Convient aux RPO courts (quelques heures).
	Quelques minutes	RPO de quelques minutes.
	Jour	RPO = 1 jour.
	Semaine	RPO = une semaine.
	Mois	RPO = un mois.
Type de sauvegarde	Complète	Demande peu de bandes et peu de temps pour restaurer.
	Incrémentielle	Demande le plus de bandes et de temps pour restaurer.
	Différentielle	Entre les deux précédents.
Technologie de sauvegarde	Miroir distant (*remote mirroring*)	Peut permettre des RTO et RPO voisins de zéro, si complet.
	Routage de transactions	Idem, avec retour en arrière possible.
	Grappe (*cluster*) à distance campus et SAN	Typiquement : RTO < 30 minutes et RPO < 8 heures.
	Propagation de log de SGBD	Dépend du traitement de la log sur site distant ; dans les meilleurs cas : RPO et RTO < 30 minutes.
	Bandes	Bandes proches ou non du lieu de restauration ; selon le temps d'acheminement, RPO et RTO se comptent en jours.
Site de stockage distant	Site commercial	Considérer la distance et l'accessibilité, le rangement des bandes, la facilité à les regrouper et à les retrouver rapidement, délais pour prévenir le fournisseur.
	Site interne	Idem, en ajoutant les compétences en local ou à déplacer.

Sur tous ces points, le chiffrage devra être précis et validé par les hommes de l'art. L'enjeu consiste ici à détecter les points à problèmes, qui peuvent se révéler bloquants ou, au contraire, à susciter une amélioration.

Il faut aussi noter que la plupart du temps plusieurs solutions cohabiteront et que, pour une activité donnée de l'entreprise, c'est la plus pénalisante qui sera ressentie au final par les usagers.

Là encore, les données papier ou enregistrées sur disque optique numérique (DON) feront l'objet d'une considération particulière.

4. Production industrielle et fabrication

Enfin, voici un exemple de préoccupations concernant les solutions envisageables pour les moyens de production de l'entreprise.

Tableau 3-13 : Difficultés prévisibles pour chaque option envisagée

Équipements et ressources critiques de production		
Catégorie	**Option**	**Préoccupations et délais**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	Si l'équipement n'est pas disponible et pas standard, il faudra attendre (des mois) ou sinon l'acquérir à l'avance et l'entreposer.
	Acquisition des pièces détachées	Les pièces de rechange ont-elles été réservées par le fabricant pour la maintenance ? Sont-elles accessibles ? Sinon : refabrication, donc délais élevés.
Pré-établi	Contrat de service pour le sauvetage et la restauration	Difficultés de mise en œuvre du contrat dues à des effets collatéraux du sinistre (incendie rendant les locaux inaccessibles, émanations toxiques).
	Maintien d'un stock de secours pour les pièces critiques sur un site distant	Le temps de récupération dépend de la distance, de l'état des transports, de l'emballage des pièces et de la logistique.
	Maintien d'équipements de secours pour les équipements critiques, sur un site distant	Idem, en ajoutant les compétences nécessaires pour maintenir ces équipements en état et redémarrer.
Stock de secours de matières premières	Maintien dans un entrepôt de secours des stocks de matières premières ou produits intermédiaires nécessaires durant la reprise	Le temps de récupération dépend de la distance, de l'état des transports, de l'emballage des matières et de la logistique. Les produits finis stockés peuvent-ils être expédiés au client depuis le site de secours sans impact pour les clients ?
Site de production alternatif	Utilisation d'un site distant de la société, vide	Attention au degré de préparation du site.
	Réparation, reconstruction du site sinistré sur place	Délais dépendant du temps à évaluer les dommages, à monter le dossier assurance, à évaluer les réparations et à les déclencher avec les contrats adéquats, tout en respectant les consignes de sécurité.

Les défauts ou faiblesses constatés peuvent conduire à rechercher l'amélioration des offres dont l'entreprise dispose sur le marché. Ils nécessitent souvent des ajustements dans les options, qui se traduisent par une révision des contrats.

Comparaison aux exigences et sélection des options

Une fois le délai moyen d'activation déterminé, celui-ci est comparé aux besoins chiffrés précédemment par les différents paramètres de reprise : MTD, RTO, RPO et WRT. Cette comparaison permet de sélectionner les options les mieux adaptées ; les options non convenables sont alors éliminées. Notons que, dans certains cas, les options sont réétudiées dans le but d'accélérer ou de faciliter leur activation. Les autres options, elles, sont retenues et passées au crible de l'étude de faisabilité et coût faisant l'objet de la phase 4.

Le tableau suivant donne, à titre d'exemple, la liste des options précédentes qui sont ici éliminées, en précisant la raison de cette élimination.

Tableau 3-14 : Options éliminées pour les locaux et bureaux (1)

Locaux et bureaux		
Catégorie	**Option**	**Raison de non-sélection**
Solution contractuelle avec fournisseur externe	Site mobile	La distance à parcourir, les conditions de circulation (météo, trafic), les encombrements pour un convoi exceptionnel sont rédhibitoires.
Activation	Cas par cas	Selon les circonstances et le type de besoins, les ressources peuvent prendre trop de temps à être mises en place.
Niveau de préparation	Site froid	Les tâches de préparation du site, de configuration, d'installation, de connexion, etc.,peuvent être très longues.

Tableau 3-15 : Options éliminées pour les sites informatiques de secours (2)

Sites informatiques de secours		
Catégorie	**Option**	**Raison de non-sélection**
En toute propriété	Site mobile	Sur routes surchargées, cette solution est impossible à réaliser, sans parler des difficultés de connexions réseaux à effectuer.
Offre commerciale	Site partagé (offre du marché)	Le site peut être utilisé en totalité ou en partie, l'occupation par d'autres clients, l'éloignement et la difficulté d'accès rendent cette option trop incertaine.
Niveau de préparation	Site froid	Il faut équiper le site : problèmes d'acquisition d'équipements, de démarrage, d'installations diverses, de paramétrages ; cela peut aller jusqu'à 7 jours voire plus.

Tableau 1-16 : Options éliminées pour les données critiques (3)

Données critiques		
Catégorie	**Option**	**Raison de non-sélection**
Fréquence des sauvegardes	Mois	RPO = un mois. Délai trop long, même pour les applications peu exigeantes.
Type de sauvegarde	Incrémentielle	Demande le plus de bandes et de temps pour restaurer.
Technologie de sauvegarde	Routage de transactions	Technologie non maîtrisée en interne.
	Grappe (*cluster*) à distance campus et SAN	Technologie non conforme à l'architecture choisie.

Tableau 3-17 : Options éliminées pour les équipements de production (4)

Équipements et ressources critiques de production		
Catégorie	**Option**	**Raison de non-sélection**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	Si l'équipement n'est pas disponible et pas standard, il faudra attendre (des mois) sinon l'acquérir à l'avance et l'entreposer.
Préétabli	Contrat de service pour le sauvetage et la restauration	Difficultés de mise en œuvre du contrat dues à des effets collatéraux du sinistre (incendie rendant les locaux inaccessibles, émanations toxiques...).
Site de production alternatif	Réparation, reconstruction du site sinistré sur place	Délais trop longs en raison du temps nécessaire à évaluer les dommages, à monter le dossier assurance, à évaluer les réparations et à les déclencher avec les contrats adéquats, tout en respectant les consignes de sécurité.

Phase 4 – Étude de coût et faisabilité

Certaines options ont été éliminées en phase précédente. Les autres, après quelques aménagements, ont été retenues et font maintenant l'objet d'une étude d'évaluation. Elle se déroule classiquement en trois étapes :

1. la détermination des critères pour l'évaluation ;
2. le chiffrage des options selon les critères ;
3. les pondérations et choix d'options.

Enfin, une proposition de choix est réalisée pour la phase 5.

Critères d'évaluation

Ces critères doivent être appropriés au problème abordé. Concrètement, on aura souvent besoin d'évaluer les options sur les points suivants :

- **la facilité ou difficulté de mise en place** de l'option, en fonction des efforts de réalisation et des investissements demandés ;
- **la facilité ou difficulté d'activation** de l'option (une fois en place) – en effet, l'effort d'activation (au moment du sinistre ou au moment des tests) peut être important et dissuasif ;
- **le coût de la mise en place** (une fois, puis récurrent), en tenant compte des divers paramètres ;
- **le coût de l'activation** (là encore, pour une activation réelle ou lors des tests) ;
- **le niveau de qualité** permis par l'option – certaines options de type « mode dégradé » peuvent en effet être acceptables lors d'un sinistre pour certaines activités, mais pas pour d'autres ;
- **la sécurité** inhérente à l'option – l'option ne doit pas représenter une brèche béante en sécurité ; tout risque sur ce point doit être documenté afin de fixer les limites acceptables ;
- **la maîtrise ou le contrôle opérationnels** sur l'option – il est possible qu'une dépendance de tiers trop forte sur certaines applications sensibles soit inacceptable ;
- **la maîtrise technique** sur l'option – là encore, l'absence de compétences en interne ou la dépendance trop forte de compétences externes peuvent être considérées comme rédhibitoires.

Pour une bonne lisibilité et afin de faciliter la décision, on se fixera un nombre limité de critères (pas plus de cinq, par exemple).

Chiffrage des options

Une fois les critères définis, ils sont évalués pour chaque option retenue. Cela peut se faire par une note de 0 (mauvais) à 3 (très bon), comme l'illustre le tableau ci-après.

Tableau 3-18 : Évaluation des options sur des critères d'effort, de qualité, de maîtrise, de coûts et de sécurité

Matériels sur site de secours (0 = défavorable à 3 = très favorable)						
Catégorie	**Option**	**Effort**	**Qualité**	**Maîtrise**	**Coûts**	**Sécurité**
En toute propriété	Site distant	1	3	3	2	3
Accord avec un tiers	Accord de réciprocité avec confrère	2	2	1	3	1
Offre commerciale	Site dédié	3	3	2	1	3
Niveau de préparation	Site tiède	2	2	2	2	2
	Site chaud	3	3	2	1	3

Ce travail de chiffrage est à effectuer sur toutes les options qui ont été retenues jusque-là. Il peut être demandé à plusieurs personnes responsables dans des services différents et fera l'objet de discussions et d'itérations jusqu'à obtention d'une vision partagée. En général, ce chiffrage s'appuie sur des données factuelles et ne devrait pas provoquer trop de divergences de point de vue.

On peut ne pas discuter à ce stade de l'importance des différents critères. Cela permet de scinder l'approche en deux parties : une qui se concentre sur le choix des critères, et l'autre qui se focalise sur leur évaluation.

Sélection d'options

Les différents critères sont alors pondérés et les options les mieux notées retenues.

Considérons l'exemple précédent concernant le site de secours informatique :

- Dans l'hypothèse où seuls comptent l'effort et la sécurité (et donc pas le coût, ni la maîtrise, ni la qualité), alors le choix se portera sur les deux options suivantes :
  - Offre Commerciale / Site dédié
  - Niveau de préparation / Site chaud
- Si, en revanche, le coût et la maîtrise sont mis en avant, alors le choix se fera sur le site distant en toute propriété.

Toute pondération de l'ensemble des critères est bien évidemment possible et on obtient, à la fin de cette étape, une liste d'options retenues.

Phase 5 – Mise au point de la stratégie de continuité

Une réunion de validation peut être organisée pour avaliser les décisions ou pour les cibler d'avantage lorsque le nombre d'options ouvertes est élevé.

L'ensemble de la stratégie de continuité peut alors être documenté dans un rapport d'étude, qui peut se structurer comme suit :

Stratégie de continuité

1. Besoins de reprise
   - 1.1. Introduction, rappel du contexte BIA, cadrage
   - 1.2. Exigences des processus critiques
   - 1.3. Besoins pour la reprise
     - a. Segmentation (bureaux, locaux IT, données, autre)
     - b. Besoins en fonction de cette segmentation
     - c. Besoins communs
2. Options possibles
   - 2.1. Catégories d'options à étudier (internes, contractuelles, etc.)
   - 2.2. Options envisagées, en fonction de la segmentation
   - 2.3. Options éliminées et raisons de l'élimination
3. Confrontation aux exigences métier
   - 3.1. Délais d'activation
   - 3.2. Comparaison avec les besoins des métiers
   - 3.3. Options retenues avec argumentation
4. Étude de coût et faisabilité
   - 4.1. Critères retenus
   - 4.2. Chiffrage des options en fonction des critères
   - 4.3. Pondération et sélection des options
5. Compte rendu de la réunion de décision

L'ensemble de ces éléments, élaborés tout au long de l'étude décrite dans ce chapitre, est conservé dans un système documentaire. On pourra ainsi s'y reporter pour comprendre les décisions stratégiques qui ont été entérinées, en consultant le détail des attendus ou hypothèses qui ont conduit à ces décisions. Cela permet par ailleurs de vérifier si ces hypothèses sont encore valables ou non. Enfin, les auditeurs pourront facilement le consulter (voir le chapitre 13).

PARTIE II

L'entreprise élabore son plan de continuité

Le plan de continuité d'activité (PCA) fixe les directives à suivre par l'entreprise en cas de sinistre dans le but d'en minimiser les impacts sur son activité.

La réalisation d'un PCA s'inscrit dans le contexte décrit dans la première partie. Dans un premier temps, l'entreprise réalise une analyse des risques encourus et détermine différentes options pour y faire face (chapitre 1), puis elle en évalue les impacts résiduels sur ses activités critiques (chapitre 2) pour définir enfin une stratégie de réponse en cas de sinistre (chapitre 3). La réalisation du PCA s'inscrit logiquement dans cette démarche.

- Pour qu'un plan de continuité soit efficace, l'entreprise doit tout d'abord organiser la réponse apportée au sinistre en définissant les responsabilités de réaction en son sein, c'est l'objet du chapitre 4.
- Elle doit ensuite prévoir le déroulement des activités et travaux à mener en fonction de sa stratégie et réaliser à cet effet un planning guide, comme indiqué dans le chapitre 5.
- Enfin, pour assurer la viabilité du PCA, elle doit assurer sa maintenance en le testant régulièrement : les tests sont développés dans le chapitre 6.

Chapitre 4

PCA : définir les missions et les responsables

Cruciale dans toute activité humaine organisée, la définition des missions et de leurs responsables revêt une importance accrue dans un contexte de sinistre et de risque. Certains spécialistes américains de la continuité d'activité vont même jusqu'à considérer que, une fois les missions et les responsabilités définies, l'essentiel du PCA est en place, le reste n'étant alors plus que de l'intendance. Aujourd'hui, l'approche la plus pragmatique et efficace que l'on puisse adopter consiste à aborder le problème sous deux angles : d'une part, les missions et les objectifs à atteindre et, d'autre part, les activités à mener pas à pas.

Les missions et leurs responsables sont présentés dans ce chapitre, tandis que les activités sont détaillées dans le chapitre suivant.

Cadrage du plan de continuité

Pour toute action d'envergure, il est essentiel de bien spécifier le contexte des activités à mener. N'oublions pas la finalité première du plan de continuité : il est destiné avant tout aux personnes chargées de réagir en cas de sinistre. Il doit donc être lisible pour permettre très rapidement de situer les choses, de comprendre le rôle de chaque intervenant et de prendre les bonnes décisions.

Définition du sinistre

Une définition claire du sinistre permet à ce stade de décider s'il faut ou non déclencher le plan de continuité. En effet, des actions plus simples, telles que le recours à une procédure de gestion d'incidents, ou l'appel à un service d'assistance (*help desk*) ou un support technique, sont également envisageables avant de recourir au PCA.

Pour cela, l'entreprise doit mettre au point sa propre classification des sinistres. En général, on a recours à un classement en plusieurs niveaux. En voici un exemple, définissant trois niveaux de sinistre.

Sinistre mineur

En termes de probabilités, le sinistre mineur est l'événement le plus fréquent, tout en ne concernant qu'un sous-ensemble réduit de processus critiques de l'entreprise. Ainsi, il ne bloque pas complètement les entités métier ayant besoin de ces processus et celles-ci peuvent continuer à travailler pendant un certain temps.

Ce type de sinistre est causé le plus souvent par une défaillance simple d'un constituant : pannes de disques sur des serveurs de données, coupures de courant limitées à certains bâtiments, etc.

La tendance actuelle montre une diminution des situations dans lesquelles un tel sinistre se présente ; autrement dit, les actions à mener en cas de sinistre mineur sont quasi banalisées, amoindrissant son impact réel. Le chapitre 7 précise ces aspects.

Sinistre intermédiaire ou moyen

Ce type de sinistre est plus rare, mais il a un impact plus conséquent sur les activités critiques de la société. En effet, cet événement arrête l'activité normale de quelques entités métier jugées critiques dans l'entreprise, sans pour autant mettre à mal toutes les entités critiques.

La cause de ce sinistre est souvent une combinaison de plusieurs pannes ou une panne générale (voir le chapitre 7) entraînant l'arrêt de plusieurs systèmes ou équipements. Il s'agit par exemple d'une fuite d'eau en salle des machines, d'un écroulement partiel de bâtiment abritant des machines importantes, etc.

Les évolutions actuelles ont tendance à considérer que c'est ce type de sinistre qui doit être testé en premier lors de simulations en situation réelle (voir le chapitre 6).

Sinistre grave ou majeur

Ce type de sinistre est moins fréquent, mais ses conséquences sont d'autant plus néfastes. En effet, le sinistre grave ou majeur cause l'arrêt de pratiquement tous les processus métier critiques.

Il a pour origine la disparition ou la panne de la majorité des équipements et systèmes, ou tout événement susceptible de rendre les locaux inaccessibles (incendies importants, tremblements de terre, tempêtes, attentats, fuites de gaz, etc.). Le plus souvent, lorsque ce type de sinistre se produit, l'entreprise n'est pas la seule victime.

Objectifs du plan

L'objectif du plan de continuité est de réduire à un niveau acceptable les conséquences d'un sinistre en mettant en œuvre des procédures prédéfinies.

Ces procédures, manuelles ou automatisées, concernent aussi bien la mise en sécurité des personnes et des biens, la récupération (de moyens, de capacité, de données, de personnel) que la continuité pure et simple (passage sur un site de

secours). Les processus métier critiques de l'entreprise identifiés lors de l'analyse d'impact (voir le chapitre 2) sont concernés en priorité.

Ainsi, lors d'un sinistre, il doit être facile – tout du moins c'est un objectif – de savoir quels sont les processus métier touchés et où sont les procédures de récupération et de continuité ; les équipes d'intervention vont en effet en avoir besoin.

Dans ce sens, il se développe actuellement sur le marché des offres de services permettant d'accéder via le réseau à un site web stockant ces documents, à partir d'un portable ou d'un Smartphone. Cela peut se révéler utile dans les cas où la documentation papier du plan de continuité se trouve sous les gravats, les serveurs de l'entreprise perdus, tandis que le réseau mobile est demeuré intact.

Périmètre et exclusions

Il est primordial de délimiter le champ d'action du plan et d'en prévoir un découpage adapté à son exécution. En général, chaque site important possède son propre plan.

Le lecteur de ce plan doit y trouver aisément les données concernant son site, et uniquement cela, afin de ne pas parasiter la lecture. Au sujet des autres sites, seules les informations ayant des similitudes ou des relations importantes avec le site sinistré seront retenues.

Le périmètre doit déterminer en priorité :

- le centre de gestion de crise où transmettre l'information ;
- les sites de la société (couverts ou non) ;
- les entités métier concernées ;
- les partenaires métier (prestataires, clients et fournisseurs) ;
- les sites de secours pour les bureaux, l'informatique ou les machines ;
- les sites d'archivage ou de stockage distants ;
- les fournisseurs à impliquer en cas de sinistre (pour les mesures de secours informatique) ;
- les autorités locales (pompiers, sécurité civile, hôpital, Samu, etc.).

En outre, il doit fournir une liste de tout élément permettant de délimiter le champ d'action à l'intérieur comme à l'extérieur de l'entreprise, notamment les paramètres de réaction :

- la durée maximale attendue pour les opérations de récupération et de redémarrage ;
- les événements types susceptibles de déclencher le plan de continuité ;
- les personnes habilitées à invoquer le plan de continuité.

Il peut être également intéressant de lister les exclusions, afin de ne pas chercher trop longtemps ces informations :

- les sites ne devant pas être considérés ;
- les éléments techniques hors du champ d'action (par exemple, la téléphonie vocale) ;
- les actions qui ne sont pas du ressort de l'équipe intervenant sur le site (par exemple, la communication peut être confiée à un porte-parole) ;
- les éléments traités par d'autres équipes ;
- les éléments totalement secondaires, qui seront pris en compte en dernier.

Contexte général du plan

À ce stade, l'objectif n'est pas de connaître ce qui s'est produit et pourquoi, mais de sortir de l'état de sinistre. On peut donc rappeler très succinctement, et à titre purement indicatif, les travaux qui ont précédé l'établissement du plan, afin de cibler au mieux les actions à mettre en œuvre.

Rappel concernant la gestion des risques

Un court rapport de type *management summary* est nécessaire pour rappeler les risques encourus par l'organisation et les solutions entreprises pour y remédier (voir le chapitre 1). Voici les points qui y sont mentionnés :

- la liste des risques et des menaces qui pèsent sur l'organisation ;
- la liste des biens (ou actifs) exposés aux menaces ;
- la description synthétique des actions de mise sous contrôle employées et du risque résiduel qui en résulte.

Des références à d'autres rapports peuvent également y figurer, en particulier les analyses de risques.

Rappel concernant l'impact sur les activités

Les résultats de l'analyse d'impact sur les activités (BIA) sont consignés dans un rapport dans lequel sont listés notamment les processus critiques (voir le chapitre 2). Pour chacun de ces processus, les aspects suivants seront brièvement décrits dans le plan de continuité :

- la désignation du responsable, interlocuteur privilégié dont le nom est actualisé dans la liste de contacts (voir plus loin) ;
- la MTD ou durée d'interruption maximale admissible ;
- les systèmes informatiques et applications utilisés par ce processus ;
- les ressources critiques non informatiques ;
- les divers temps de reprise : RTO, RPO, WRT des applications et ressources critiques (voir le chapitre 2 pour plus de détail).

Rappel concernant la stratégie de continuité

Ce dernier rappel concerne le troisième aspect du processus de continuité d'activité, à savoir les choix stratégiques réalisés en termes d'options de continuité (voir le chapitre 3) :

1. les locaux et bureaux de secours qu'il est prévu d'utiliser suite à un sinistre, en particulier le centre de gestion de crise destiné à l'équipe de gestion de crise ;
2. les systèmes, infrastructures et locaux informatiques jugés critiques et ceux prévus pour les remplacer en cas de sinistre ;
3. les dossiers et données critiques, ainsi que les lieux ou sites où sont stockés les sauvegardes et duplicata des documents critiques ;
4. pour la production industrielle, une indication précise des équipements et produits critiques, ainsi que des sites où l'on peut trouver ou rétablir ces éléments ou ceux prévus pour les remplacer.

Structure du plan de continuité

Le plan de continuité doit être formalisé par un document lisible, mis à jour régulièrement et accessible par ceux qui devront l'appliquer. Ce plan doit être complet et facile à mettre en œuvre.

Voici à quoi peut ressembler un plan de continuité type.

Plan de continuité d'activité

1. Objectif et périmètre
   - 1.1. Objectif du plan
   - 1.2. Périmètre concerné
   - 1.3. Exclusions
2. Définition du sinistre
   - 2.1. Sinistre mineur
   - 2.2. Sinistre moyen
   - 2.3. Sinistre majeur
3. Rappel de l'étude sur la gestion des risques
4. Rappel de l'analyse des impacts sur les activités
5. Rappel de la stratégie de continuité de l'activité
6. Équipes et missions
   - 6.1. Groupe de gestion de crise
   - 6.2. Groupe de redémarrage des activités
   - 6.3. Groupe de récupération technique et opérationnelle
7. Informations utiles sur les contacts
   - 7.1. Listes par entités et/ou compétences
   - 7.2. Membres des différents groupes et remplaçants
   - 7.3. Aspects confidentiels et « vie privée »
8. Centre de gestion de crise
   - 8.1. Localisation

8.2. Activation
8.3. Occupants
9. Planning en sept étapes
9.1. Première intervention et notification
9.2. Évaluation et escalade
9.3. Déclaration de sinistre
9.4. Planification de la logistique d'intervention
9.5. Récupération et reprise
9.6. Retour à la normale
9.7. Bilan
10. Affectation des ressources techniques à chacune des étapes
10.1. Listes et responsables
10.2. Méthode de mise à jour
11. Affectation des ressources humaines à chacune des étapes
11.1. Lien entre groupe et étape
11.2. Évaluation des charges
12. Contrôle des changements éventuels du plan
12.1. Responsable
12.2. Méthode
13. Liste des destinataires du plan
13.1. Liste nominative et par fonction
13.2. Mise à jour

Annexes (documents complémentaires fournis)

A. Plan de secours
B. Plan de communication de crise
C. Contacts externes
D. Ressources critiques
1. Bureaux et équipements
2. Systèmes informatiques et infrastructures
3. Machines et équipements de production
4. Stocks divers de production
E. Dossiers critiques et enregistrements sensibles
F. Informations sur les sites de secours
1. Sites de secours informatiques
2. Sites de secours de production
3. Bureaux ou locaux de secours
4. Centre de gestion de crise
G. Procédures de stockage et de récupération des dossiers et enregistrements vitaux

H. Informations sur les polices d'assurance
I. Conventions de service
J. Guides et normes
K. Formulaires de travail manuel
L. Rapports sur les études réalisées
    1. Évaluations de risque
    2. Impacts sur les affaires
    3. Stratégie de continuité
M. Glossaire

Planning des activités

Le PCA : un projet à part

Le planning des activités doit être conçu par l'entreprise de façon à être adapté au mieux au contexte de ses activités. Il n'existe donc pas de plan universellement valable et chaque entreprise possède son propre plan. Néanmoins, il y a tout avantage à ce que le plan soit basé sur un modèle type de planning permettant de répondre à toutes les questions importantes dans un ordre raisonné.

Comme tout projet, le PCA fait appel à des ressources spécifiques et des groupes d'intervention particuliers, dont il est important de définir au préalable la composition et les responsabilités dans des listes. Lors d'un sinistre, ces listes de contacts jouent un rôle primordial, car il est bien évidemment impossible de prévoir à l'avance les compétences à mobiliser et disponibles à ce moment-là : « nul ne connaît le jour ni l'heure » du déclenchement du plan, et encore moins le nom des responsables qui seront en position de décider. Il faudra alors réagir avec les ressources disponibles. Sur ces points, le PCA se distingue d'un projet normal. (Pour plus de détails sur le projet de PCA, se référer au chapitre 12.)

Planning en sept étapes

On retient le plus souvent un planning en sept étapes, qui sera vu plus en détail dans le chapitre 5.

- **Étape 1 – Première intervention et notification.** Il s'agit de prendre en compte le sinistre, d'en évaluer très vite les dégâts et d'alerter les groupes d'intervention.
- **Étape 2 – Évaluation et escalade.** Une inspection plus complète des dégâts sur le site touché est réalisée, produisant rapidement un rapport. À partir de ces évaluations, les équipes nécessaires sont dépêchées sur le site.
- **Étape 3 – Déclaration de sinistre.** Selon les constatations faites, l'état de sinistre est déclaré ou non. Les étapes suivantes ne sont réalisées que dans le cas où l'état de sinistre est déclaré.

- **Étape 4 – Planification de la logistique d'intervention.** Les procédures de préparation logistique sont exécutées pour préparer l'environnement de reprise et les équipes d'intervention aux deux étapes suivantes.
- **Étape 5 – Récupération et reprise.** Les ressources critiques, informatiques ou non, sont récupérées selon les options prévues. Les sites de secours sont mis en état, investis et opérationnels ; les processus critiques peuvent ainsi reprendre.
- **Étape 6 – Retour à la normale.** Les activités opèrent une transition vers l'état précédant le sinistre. Les ressources et sites sont alors ceux d'origine ou d'autres à caractère définitif.
- **Étape 7 – Bilan.** Toutes les étapes précédentes sont analysées afin d'améliorer et/ou modifier le plan de continuité en conséquence.

> **Attention ! Plan de continuité vs plan d'intervention d'urgence**
>
> Notons qu'il est fortement possible que l'étape 1 soit réalisée en parallèle d'un plan d'intervention d'urgence (médical, pompiers) s'occupant de la sécurité du personnel, de la sauvegarde des biens et de la préservation de l'environnement. Le plan de continuité, quant à lui, s'attache uniquement à la continuité des activités de l'entreprise.
>
> Cette différence d'objectif est importante et doit rester à l'esprit des personnes qui exécutent le plan, car elle peut amener des divergences de comportement. Par exemple, en cas d'incendie, les pompiers vont arroser un bâtiment pour éviter la reprise ou la propagation du feu, alors que les équipes chargées de la continuité souhaiteront protéger les ordinateurs de toute humidité.

Le centre de gestion de crise

Point central de commandement, le centre de gestion de crise est le lieu à partir duquel sont décidées, planifiées et pilotées les actions des différents groupes d'intervention. C'est aussi le numéro de téléphone à appeler pour proposer ses services et demander une affectation à une tâche du plan de continuité. Enfin, c'est là que l'on rend compte de toute exécution d'actions planifiées ou de tout événement nouveau.

Une analogie militaire présenterait le centre de gestion de crise comme une salle d'état-major ou une *war room* de film de guerre américain, avec sur les murs des tableaux et listes d'intervenants affectés dans les groupes d'intervention. On y tient à jour l'état d'avancement des actions lancées et la liste de celles à venir.

C'est également un lieu où sont présents les décideurs. Ainsi, en cas de doute ou de nécessité d'arbitrage, les opérationnels sur le terrain savent qu'en appelant ce centre, ils obtiendront une décision ou une consigne à appliquer et à faire appliquer.

Un rôle clé

Il est primordial que ce rôle de centralisation soit assuré de manière claire et reconnue. De nombreux exemples de pannes relativement simples prouvent que

l'absence de centre de gestion de crise, et donc de prise de décision centralisée, complique une situation de crise et ralentit les actions de reprise.

> **Exemple : Panne d'électricité dans une usine de circuits imprimés sans centre de gestion de crise**
>
> La société CT fabrique des circuits imprimés pour la téléphonie. Vers 16 h 30, en plein hiver, une panne d'électricité survient. Les machines s'arrêtent et l'usine est quasi plongée dans le noir, hormis dans les endroits où un éclairage de secours a pris le relais.
>
> Le centre informatique qui se trouve dans le même bâtiment n'a également plus d'électricité. Certains serveurs s'arrêtent, d'autres basculent sur une alimentation de secours. En tout cas, les personnes présentes sur le site supposent qu'il en est ainsi.
>
> Au bout de cinq minutes, tous les employés ont quitté leur poste et discutent en groupes dans les zones encore éclairées. En réalité, personne ne sait trop quoi faire. Certains s'enquièrent auprès de leur chef de la conduite à tenir. Certains responsables téléphonent, sans trop savoir à qui. Les ordinateurs ne fonctionnent plus, la messagerie est inaccessible. Le *help desk* informatique présent sur le site reçoit des appels, mais il ne peut que confirmer qu'il est lui aussi dans le noir.
>
> Des ingénieurs systèmes se rendent dans la salle des ordinateurs et constatent que certains serveurs critiques fonctionnent toujours, mais ils ne savent pas durant combien de temps encore les réserves des batteries tiendront. Certains décident d'eux-mêmes d'arrêter certains serveurs en suivant des procédures de sécurité, d'autres se contentent d'espérer que le courant reviendra sous peu. Mais on ne peut rien faire, car les procédures de sécurité sont enfermées dans le bureau d'un chef d'équipe absent.
>
> Monsieur X., chef de service, rentre de déplacement vers 17 h. Étant sur place le plus haut placé dans la hiérarchie, tout le monde se tourne vers lui, son bureau devenant alors une salle des pas perdus où se rassemblent des employés impuissants. Monsieur X. demande alors à certaines équipes de rentrer à leur domicile pour libérer un peu de place et ainsi se concentrer sur le problème. Il part ensuite en salle informatique pour se renseigner sur les batteries alimentant les serveurs critiques. En son absence, son téléphone continue de sonner, mais personne ne décroche.

La société citée en exemple s'en est sortie ; cet événement lui a permis de tirer certaines leçons, en faisant apparaître les besoins suivants.

- **Mise en place d'un centre de gestion de crise connu de tous** – Le *help desk* a été choisi car son numéro de téléphone est connu de tous les employés. Un bureau, doté de plusieurs lignes de téléphone, lui est attribué.
- **Désignation d'un responsable** – Monsieur X. est désigné responsable de crise sur ce site et, lorsqu'il s'absente, son adjoint le remplace.
- **Permanence au centre** – En cas de crise, Monsieur X. se rend au centre de crise et n'en bouge pas. S'il a besoin d'une information, il demande à un employé d'aller se renseigner.
- **Liste de contacts** – Des numéros de téléphone de personnels utiles en cas de crise sont notés dans une liste dont une copie est gardée au centre de crise.
- **Doubles des clés** – Des clés d'accès pour la salle informatique et pour certains bureaux sont dupliquées et conservées au centre de crise.

- **Liste des ressources critiques** – Une liste des serveurs les plus critiques est établie, dont une copie est conservée au centre ; le *help desk* est par ailleurs très content d'en disposer. Une pastille colorée de priorité d'arrêt est également collée sur les serveurs critiques.
- **Matériel nécessaire** – Des lampes de poche, un tableau de conférence avec des marqueurs sont stockés dans une armoire du bureau de gestion crise.

Ces quelques actions de bon sens permettent d'améliorer la réactivité des intervenants en cas de sinistre. Le fait de désigner un centre de gestion de crise et de réfléchir à ce qu'il serait bon d'y trouver a permis de progresser dans la prise en compte et la résolution de sinistres.

Emplacement stratégique du centre de gestion de crise

Malheureusement, il est impossible de connaître à l'avance le lieu où se produira le sinistre. Il faut donc étudier différentes situations pour évaluer les sites candidats. Les critères qui suivent permettent ensuite de les comparer.

- **Reconversion de locaux existants équipés** – Peu de sociétés peuvent s'allouer une salle entièrement dédiée à la gestion de la crise. En général, c'est un local d'un autre usage habituel qui est utilisé en cas de sinistre. Il faut donc chercher dans les locaux existants les salles qui peuvent facilement être reconverties en centre de gestion de crise et qui disposent déjà de téléphones, d'un câblage réseau, de tables et chaises et éventuellement d'ordinateurs connectés. Très souvent, les salles de cours s'avèrent de bonnes candidates.
- **Éloignement des zones à risque** – Le centre ne doit pas être soumis au même sinistre que le site touché. Ainsi, on évitera de le placer en zone inondable, si l'inondation est le risque principal. Il faut penser également que les ascenseurs peuvent être en panne et ne pas le placer trop haut dans les étages.
- **Accessibilité** – Le centre doit être facile d'accès (gare, sortie d'autoroute), proche de commodités (hôtels, restaurants), avec des facilités de chargement et de déchargement de matériels.

Centre de gestion de crise de secours

Pour des raisons de fiabilité, un centre de gestion de crise doit aussi disposer d'un site de secours, dans le cas où le centre principal serait inutilisable.

Pour un tel choix, il convient de rester pragmatique. Si l'entreprise dispose de plusieurs sites relativement proches, il est facile de trouver des bureaux adaptés que l'on puisse aménager en cas de sinistre. Chaque site possède son centre de gestion de crise et le centre d'un site peut venir au secours d'un autre. Il est également possible d'utiliser les locaux d'un confrère peu éloigné. Dans ce cas, il faudra gérer la cohabitation, en particulier si le bureau utilisé sert aussi de centre de gestion de secours pour le confrère. Ce type d'accord peut bien évidemment être réciproque. Enfin, il est également envisageable d'utiliser des bureaux mobiles aménagés dans un conteneur que l'on fait venir sur le site ; un centre précaire vaut mieux que pas de centre du tout. En cas de sinistre, il s'avère donc

utile de prévoir ces trois alternatives : le centre de gestion de crise principal, le centre de secours et le centre mobile.

Concrètement, il est possible d'utiliser en premier recours un centre de secours éloigné parce que l'on ne dispose d'aucune autre solution. Ensuite, il est toujours temps de déménager, pour des raisons pratiques, dans un lieu plus proche du sinistre ; on utilise alors un site mobile ou le centre site sinistré lui-même.

Une dernière solution consiste à louer une salle dans un hôtel, demandant une moindre préparation. Toutefois, si le sinistre est d'ampleur régionale, cette solution n'est pas forcément viable, d'autres entreprises pouvant également avoir réquisitionné les salles de ce même hôtel.

Fonctions du centre de gestion de crise

Le centre de gestion de crise est le lieu d'où sont exécutées trois fonctions essentielles : le commandement, le contrôle et la communication – points essentiels dans l'organisation de ce centre et la planification de ses besoins.

Attention, cependant : le centre est souvent fortement associé dans les esprits avec la coordination générale du PCA. À ce sujet, les Américains ont coutume de dire qu'un général sans centre d'opération n'est pas un vrai général.

Commandement

Très souvent, les décisions doivent être prises dans l'urgence à partir d'informations incomplètes. Le sinistre a provoqué des dégâts et il est fortement probable qu'il en provoquera d'autres. Il faut donc le circonscrire et sauver ce qui peut encore l'être. Dans ce but, un dispositif de prise de décisions doit être mis en place rapidement – ceci afin que tous les intervenants prennent le réflexe de rendre des comptes au centre de gestion de crise tout en suscitant une attitude d'écoute et de respect des instructions émanant du centre.

Un cercle vertueux « rendre compte » puis « exécuter » doit impérativement se mettre en place rapidement. Si ce n'est pas le cas, les équipes sur le site risquent d'agir inutilement, de façon dangereuse voire nuisible, sans pour autant avoir effectué les actions de première importance. Pour éviter cela, il faut que l'opérationnel puisse contacter le centre et y trouver des réponses immédiates. Sinon, il considérera qu'il doit « se débrouiller tout seul » et que les comptes rendus sont « une perte de temps ».

Un commandement efficace collecte les informations, met en place des plans d'actions réalistes en fonction des moyens mis à disposition et affecte les rares ressources disponibles là où leur efficacité sera maximale. Il est donc nécessaire que le responsable soit un bon décisionnaire et qu'il ait à disposition un minimum d'infrastructures.

Contrôle

Le contrôle consiste à suivre l'exécution des opérations et à réajuster les actions en fonction des événements et des résultats obtenus.

Toutes les informations collectées sont regroupées et rapportées aux responsables. C'est pourquoi, il est utile de disposer de tableaux de conférence avec du papier blanc et des marqueurs : cela permet de noter les informations par groupes d'intervention et de les avoir toujours sous les yeux. Détail anodin en apparence, l'utilisation de papier plutôt que de surfaces effaçables a l'avantage de permettre un débriefing ultérieur et la reconstitution de la chronologie des événements.

C'est encore au centre de gestion de crise que les réaffectations de ressources sont décidées, transmises et consignées. On y reçoit également les nouvelles informations sur le sinistre, qui sont classées et horodatées.

Des actions centralisées, telles que des commandes de matériels (pompes, bâches, serveurs, etc.) ou les déclarations diverses auprès des autorités ou assureurs, sont menées depuis le centre, où elles sont documentées. L'outil principal dans ces actions est alors le téléphone.

Communication

Le centre de gestion de crise est le point névralgique de la communication : c'est l'endroit où toutes les nouvelles informations doivent converger et d'où proviennent toutes les informations fiables. On distingue deux types de communication, en fonction de son objectif : la communication pour action et la communication pour information. L'information entrante provient des groupes d'intervention sur le terrain tandis que la communication sortante est à destination des médias, des partenaires et clients, des salariés et du grand public.

Un plan de communication type est donné en fin de chapitre.

> **Exemple : Quand les télécommunications ne fonctionnent pas**
>
> Suite à un incendie ayant provoqué une coupure de courant et de nombreux dégâts, la téléphonie interne de la société SLO, société de leasing, ne fonctionne plus.
>
> Constatant le problème, les responsables de l'entreprise se rendent les uns après les autres dans le bureau du chef du service des télécommunications, Monsieur Y. Après vingt minutes, ce bureau s'est quasi transformé en centre de gestion de crise. Il en présente en effet bien des caractéristiques : Monsieur Y. y a réuni ses experts qui tracent un plan de résolution au tableau blanc tandis que deux d'entre eux se rendent dans la salle de l'autocom pour en revenir au bout de cinq minutes avec des propositions d'actions. Monsieur Y. et d'autres chefs d'équipes ont planifié sur un tableau de conférence diverses interventions et ont revu ensemble les activités du soir pour tenir compte surtout de l'absence de téléphonie. Les plannings ainsi modifiés sont fixés au mur avec du ruban adhésif, les employés viennent s'y informer.
>
> Dans cet exemple, il est évident que le bureau du chef de service des télécommunications est le lieu le plus approprié pour implanter un centre de gestion de crise, tant que la téléphonie n'est pas opérationnelle et le local initialement prévu sans aucun moyen de communiquer. Dans le bureau de Monsieur Y., toute communication est de forme orale et le reporting réalisé grâce au réflexe des experts se déplaçant pour rendre compte à leur chef et s'aviser des instructions. Des informations opérationnelles sont également affichées au mur.

En général, il est préconisé de disposer au centre d'au moins trois lignes téléphoniques : une ligne pour les appels entrants (à limiter en durée), une autre pour les appels sortants et une dernière disponible pour les appels de secours.

En cas de défaillance des moyens habituels de communication (téléphonie fixe et mobile), il est nécessaire de disposer de moyens radio (talkie-walkie) pour relier le centre de gestion de crise aux opérationnels envoyés sur le terrain.

Équipement du centre de gestion de crise

Le centre de gestion de crise prévu doit être doté de moyens lui permettant de remplir parfaitement sa mission sur toute la durée nécessaire. Il faut donc prévoir, dans le centre, même ou à proximité, des moyens facilement accessibles tels que :

- un générateur électrique ou des batteries avec onduleurs ;
- un éclairage de secours ;
- des lampes de poche avec provision de piles électriques en état de fonctionner ;
- des sanitaires, si le centre est isolé ;
- des trousses à pharmacie ;
- des fournitures – blocs-notes, papiers, crayons, stylos bille, marqueurs, tableaux de conférence, tableaux blancs, agrafeuses, papier adhésif, etc. ;
- des ordinateurs et des imprimantes connectés au réseau ;
- des tables, chaises, armoires à dossiers, corbeilles à papier et poubelles ;
- un ou plusieurs photocopieurs, télécopieurs, avec les recharges de papier et les cartouches d'encre adaptées ;
- des exemplaires du plan de continuité, des listes téléphoniques, des organigrammes et des listes de contacts ;
- des plans des bâtiments, du site, de la ville et des environs ;
- des formulaires spécifiques à certains processus manuels de l'entreprise ;
- des talkies-walkies avec batteries et chargeurs.

Il est indispensable de vérifier régulièrement le bon fonctionnement des divers matériels ; les batteries doivent être chargées, les piles utilisables et tout ce qui possède une date de péremption renouvelé dans les délais. Les tests décrits au chapitre 6 traitent plus précisément de ces aspects.

Missions, équipes et responsabilités

Lors de l'exécution d'un plan de continuité, rien n'est plus terrible qu'une situation où les employés ne savent pas quoi faire, agissent isolément et sans rendre de comptes ou, simplement, les rassemblements de curieux qui entravent la

liberté d'action des intervenants voire, pire, augmentent le niveau d'exposition et de risque. Il est donc essentiel de cadrer clairement les équipes opérationnelles, en définissant précisément le profil des intervenants ainsi que leurs responsabilités.

Il faut distinguer plusieurs missions et responsabilités. Toutes sont indispensables. L'organisation peut varier : on peut prévoir une seule équipe polyvalente qui assume l'ensemble des missions ou, à l'inverse, répartir ces missions entre plusieurs équipes spécialisées. Le découpage doit être guidé par des préoccupations de facilité de mise en œuvre et de capacité à coordonner.

D'autre part, il faut garder à l'esprit qu'un spécialiste prévu dans l'une des équipes d'intervention peut se trouver indisponible le jour du sinistre. Un compromis doit donc être trouvé : à compétence égale, il est préférable de choisir un employé sédentaire plutôt qu'une personne toujours en déplacement. À l'inverse, un employé qui ne travaille pas en temps normal sur le site considéré ne sera pas touché si le site est sinistré ; il sera alors plus disponible pour intervenir.

Dans ce domaine encore plus qu'ailleurs, il existe une différence entre la théorie et la pratique. En cas de sinistre, il faut avant tout rechercher l'efficacité : un ingénieur système sera probablement plus utile en donnant ses instructions par téléphone (s'il fonctionne) à un opérateur de la salle informatique, plutôt qu'à essayer de se rendre sur le site sinistré au risque de perdre deux heures dans les embouteillages.

Le groupe de gestion de crise

Le groupe de gestion de crise dirige l'exécution du plan de continuité et coordonne la communication ainsi que les diverses interventions connexes.

Ce groupe est placé sous la responsabilité d'un chef de groupe choisi parmi les cadres dirigeants seniors de l'entreprise. C'est lui qui, lors d'un sinistre, a le pouvoir de décider d'activer ou non le plan de continuité. En effet, grâce à sa connaissance de l'entreprise et ses nombreux contacts sur le site et à l'extérieur (siège, filiales, étranger, hors entreprise, etc.), il est en mesure de comprendre rapidement les enjeux et de décider en connaissance de cause.

Le groupe de gestion de crise se voit confier notamment les sept missions suivantes, qui peuvent faire l'objet d'équipes distinctes ou de responsables seniors attitrés.

Coordination de la continuité d'activité

La coordination consiste à mener à bien les diverses étapes du plan de continuité, aussi bien en interne qu'entre les différentes équipes. Il peut également être intéressant d'y associer la responsabilité de la maintenance et des tests du plan de continuité.

Cette mission fondamentale doit être confiée à une personne dotée d'une grande résistance au stress et d'une force de décision conséquente – trop

d'hésitations se révélant inefficaces en cas de crise. Un responsable senior ou, dans de plus petites structures, le chef du groupe « continuité » peuvent parfaitement assumer cette fonction.

Évaluation des dommages

Cette mission s'effectue immédiatement après la prise de connaissance du sinistre. Elle s'appuie sur l'intervention de spécialistes locaux, qui sont immédiatement envoyés sur les lieux pour évaluer au mieux l'étendue des dégâts et estimer le temps nécessaire pour une remise en état et un redémarrage des activités – informations consignées dans un rapport. Ainsi, il est préférable de prévoir sur place des intervenants pour cette mission.

Afin de déterminer au mieux tous ces éléments clés pour la suite des opérations, il est bon de s'appuyer sur des listes ou des guides de recommandations préétablis (listes de contrôles).

Déclaration d'activation du plan

Cette mission consiste à avertir l'ensemble des employés et des dispositifs impliqués dans le plan de continuité. Elle doit donc être confiée à une équipe connaissant bien l'organisation de l'entreprise et des clients. En effet, il est souvent nécessaire, en cas de sinistre, de trouver et de contacter les personnes disponibles, qui ne sont pas forcément celles prévues à l'origine.

Pour cela, il existe des listes préétablies de responsables et de personnels, organisées en fonction des compétences de chacun (voir ci-après).

Interventions d'urgence ou de premiers secours

En cas d'urgence ou de premiers secours, il est impératif de protéger en priorité les personnes, les biens et l'environnement. Ainsi, différentes équipes peuvent être dépêchées sur les lieux du sinistre :

- équipes de premiers secours envoyées par et dépendant du groupe de gestion de crise ;
- équipes rattachées à une autre responsabilité (sécurité civile, préfet…) ; c'est le cas le plus fréquent, et la mission consiste alors à se coordonner avec ces équipes.

Pour définir cette coordination, un « plan de secours », consistant en une liste de points qui devront être pris en considération par les premiers secours, doit être mis en place. Un exemple en est donné à la fin de ce chapitre.

Communication

C'est un aspect important, mais trop souvent négligé, de la gestion de crise. Il s'agit de fournir des informations cohérentes, actualisées et précises sur le sinistre subi (nature, évolution, actions à mener et temps de rétablissement prévu) à toutes les personnes concernées (le personnel, la hiérarchie, les partenaires d'affaire externes, les clients mais aussi le public).

Il faut distinguer la communication pour information de la communication pour action. Ce rôle d'information sera confié préférablement à une personne travaillant en appels sortants, afin d'éviter les saturations d'appels téléphoniques inutiles vers les responsables opérationnels. Cela veut dire que la personne prend les devants et appelle vers l'extérieur plutôt que d'attendre des appels entrants pouvant perturber les responsables opérationnels.

Un guide préétabli de la communication de crise peut être réalisé avec profit : un exemple de plan de ce type est donné en fin de chapitre.

Activation de la logistique et de l'approvisionnement des moyens de secours

Il s'agit ici de réaliser concrètement les actions prévues par la stratégie de continuité (voir le chapitre 3), à savoir :

- activer les contrats de secours de sites, les livraisons des moyens informatiques et autres, l'ouverture des droits de licence, des connexions réseaux de secours, etc., prévus dans le plan ;
- effectuer des déménagements et les déplacements des employés vers les sites secondaires.

En général, cette mission est confiée à une équipe travaillant en parallèle des autres, ayant une parfaite connaissance des fournisseurs, des contrats de secours et de leurs conditions. Ses membres ne se trouvent pas nécessairement sur place, mais doivent interrompre leur activité habituelle pour s'y consacrer à plein temps.

Évaluation des risques

Préoccupation majeure du groupe de gestion de crise, cette mission consiste à évaluer en continu les risques pris lors de l'activation du plan de continuité, afin de les contrôler au mieux. Ces risques concernent notamment :

- avant tout, bien sûr, les personnes, les biens et l'environnement ;
- ensuite, la préservation des droits et des intérêts de l'entreprise (vis-à-vis des assurances ou de recours divers), ainsi que le respect des obligations légales, de la sécurité et de la confidentialité.

Cette mission est le plus souvent confiée à un technicien généraliste reconnu qui aura, éventuellement, à s'opposer à certaines actions qu'il jugera trop risquées. Ainsi, des arbitrages inévitables seront à faire avec et par le chef du groupe de gestion de crise. Ces arbitrages devront nécessairement être documentés.

Le groupe de redémarrage des activités

Ce groupe est très important, car tourné vers les métiers et les activités de l'entreprise. Il représente les intérêts des responsables des différentes activités de l'entreprise (entités métier ou *business units*) et porte leurs exigences en termes de continuité d'activité.

Le groupe de redémarrage des activités se subdivise en trois équipes, reportant chacune au chef du groupe de gestion de crise : l'équipe métier, les utilisateurs courants et le groupe chargé des relations internationales, quand il y a lieu. Toutefois, sa constitution est volontairement différente de celle du groupe qui précède, car il se peut que les priorités divergent.

*L'équipe métier (***business unit***)*

Son objectif est de répondre aux préoccupations et de défendre les intérêts des différents départements de l'entreprise qui ont besoin de retrouver des moyens pour fonctionner.

Plusieurs organisations sont possibles pour constituer cette équipe :

- chaque département a son propre groupe constitué d'utilisateurs clés ;
- une seule équipe regroupe les représentants ou correspondants informatiques des principaux départements ;
- les départements intervenant sur des activités critiques sont représentés par une seule équipe, les autres unités par une seule personne ou ne sont pas représentées ;
- un rôle est souvent attribué à une maîtrise d'ouvrage interne proche des *business units*, focalisée sur les processus dits critiques de l'entreprise.

Le groupe des utilisateurs courants

Ce groupe détermine les besoins immédiats et souvent d'ordre général (bureautique, réseau local, poste de travail) des utilisateurs, suit le processus de redémarrage des activités et sert de relais entre les utilisateurs et le groupe de récupération technique (voir plus loin).

À la demande du responsable de la gestion de crise, ses membres peuvent être amenés à choisir entre deux solutions. Il est en effet possible d'imaginer des solutions de reprise en mode dégradé, demandant de choisir entre une solution incomplète mais rapide et une solution complète mais beaucoup plus longue à mettre en œuvre.

D'autre part, on peut imaginer des entités métier qui, devant l'étendue des dégâts, vont mener leurs propres actions à l'aide de moyens hors du champ du plan de continuité, comme utiliser des boîtes mails de grands fournisseurs Internet en attendant que la messagerie interne soit rétablie. Ces actions ne concernant qu'un nombre restreint d'utilisateurs peuvent être menées en dehors du plan de continuité. Ce type de situation se rencontre lorsque la mutualisation des moyens informatiques n'est ni très forte ni centralisée. Le responsable de la gestion de crise doit malgré tout en être averti. Dans ce cas, le département « autonome » rejoint le plan en étape 6 (retour à la normale). Avec l'apparition des offres de services sur Internet ou l'utilisation de logiciels en mode SaaS (*Software as a Service* ou logiciel proposé comme un service), ces situations, encore rares, deviennent de plus en plus courantes.

Ainsi, l'élaboration du plan de continuité ne doit pas négliger ces solutions externes, sous peine de se trouver débordé le jour du sinistre par des opérationnels qui iront chercher des solutions partielles et non coordonnées en dehors de celles prévues par le plan. Avant de ne recourir qu'aux solutions internes, il est indispensable d'envisager la viabilité des offres externes du marché et de les intégrer au plan si elles conviennent.

Le groupe des relations internationales

Pour les entreprises disposant de filiales ou de partenaires importants à l'étranger, il convient d'être vigilant quant aux impacts que le sinistre peut avoir sur ces relations. Ainsi, en raison des problèmes de langues et de décalages horaires, il est souvent préférable de confier à une personne ou à un petit groupe la mission suivante, consistant à :

- prévenir les contacts ou responsables étrangers de l'occurrence du sinistre ;
- les avertir de l'impact du sinistre sur leurs activités ;
- les informer des évolutions et des actions mises en œuvre ;
- leur transmettre des messages à diffuser localement ;
- déclencher, éventuellement, en local les parties du plan de continuité qui les concernent ;
- assurer un suivi des actions menées localement et la coordination avec la maison mère ;
- recueillir les éventuelles suggestions d'amélioration du dispositif.

Le groupe de récupération technique et opérationnelle

Les membres de ce groupe sont envoyés sur le terrain pour récupérer tout ce qui peut l'être et remettre en ordre de fonctionnement ce qui doit l'être.

Selon le contexte du sinistre et son ampleur, sa constitution ainsi que sa localisation géographique peuvent varier. En effet, certaines personnes peuvent être envoyées sur le site sinistré et d'autres sur un site de secours plus ou moins éloigné.

Ses compétences doivent permettre la réalisation des missions décrites ci-après.

Remise en route de l'informatique

Effectuée par des spécialistes, cette mission consiste à remettre en état ou à faire redémarrer « à neuf » les moyens informatiques : plates-formes et systèmes d'exploitation, réseaux et télécommunications, systèmes de bases de données et fichiers, applications prévues dans le plan, restaurations système, systèmes de sécurité conformes au niveau convenu, environnements divers (tests, intégration), câblage, alimentations électriques et refroidissement.

Ces spécialistes connaissent parfaitement les procédures d'installation et les contraintes de configuration, tout en disposant des autorités et autorisations nécessaires.

Récupération et mise en route des moyens de production industrielle

Cette mission est confiée à différents corps de métiers : mécaniciens, électriciens, spécialistes de commandes numériques, dépanneurs, chargés de maintenance, électroniciens, etc. Cette équipe prend en charge la récupération, la remise en état et l'activation des équipements conservés en secours ou apportés sur le site du sinistre :

- équipements endommagés à évaluer et à remettre en état ;
- équipements à tester ;
- alimentations électriques ou autres énergies ;
- stocks de matières et biens intermédiaires ;
- tout équipement assurant la sécurité d'exploitation.

Manipulation des matières dangereuses

Il est nécessaire de manipuler correctement certaines matières qui, selon le contexte, peuvent s'avérer dangereuses pour l'environnement comme pour l'homme. Les intervenants sur cette mission doivent donc identifier les matières ou conditions à risques, détecter les contaminations ou pollutions diverses, afin de mettre en œuvre les actions de protection ou d'évacuation.

Il est donc primordial que ces intervenants soient des spécialistes du domaine, voire des intervenants extérieurs (pompiers, fournisseurs d'électricité ou de gaz, services municipaux). Parfois, ils peuvent être amenés à prendre des décisions allant à l'encontre des intérêts immédiats des acteurs, rendant là encore un arbitrage nécessaire.

Les évolutions récentes en matière de protection de l'environnement et de développement durable font de la manipulation des matières dangereuses un sujet de réflexion désormais incontournable.

Récupération et restauration des dossiers vitaux

Certaines industries sont tenues de conserver des dossiers durant de très longues périodes : l'industrie pharmaceutique, par exemple, doit garder ses tests de médicaments pendant au moins trente ans, sans parler des cabinets d'experts comptables ou d'avocats qui archivent également un nombre considérable de pièces justificatives sous forme papier.

Cette quatrième mission technique consiste donc à récupérer les dossiers endommagés (dossiers papiers ou microfiches) en leur apportant un soin et une protection immédiate, en stoppant toute poursuite de dégradation et tout dommage ultérieur et en appliquant des procédures permettant de les reconstituer dans leur état initial. Seulement dans certains cas, encore rares, ces dossiers

papiers ont été copiés sur CD-Rom ou sur DON (disque optique numérique). Les supports à rechercher et à restaurer sont donc d'une grande diversité.

Récupération des sauvegardes critiques

Cette récupération concerne les sauvegardes informatiques traditionnelles, qui ont normalement été déposées « en lieu sûr ». Les intervenants sur cette mission doivent donc :

- récupérer les sauvegardes là où elles sont stockées (coffre-fort ignifugé proche du site sinistré ou sur un autre site de dépôt) ;
- récupérer tous les éléments nécessaires, sans en oublier, dans le bon état et à la bonne date (applications, bases de données, fichiers, systèmes, etc.) ;
- assurer la sécurité des sauvegardes classées confidentielles.

Cette mission délicate doit être menée avec le plus grand soin. En effet, tout oubli (une valise de cassettes non récupérée, par exemple) peut « torpiller » l'ensemble du processus de restauration des données.

L'équipe habilitée doit donc parfaitement connaître le lieu où sont entreposées les sauvegardes. Très souvent, elle sera constituée des employés chargés du transport (par navette, en général) des cassettes de sauvegarde en temps normal. En outre, les cassettes de sauvegarde doivent être stockées par lots cohérents, reconnaissables sans ambiguïté. Enfin, les responsables des applications critiques doivent s'assurer que les données qu'ils donnent à sauvegarder sont effectivement les données nécessaires à la restauration de leurs applications.

Les technologies de stockage étant en pleine évolution, une partie des données à récupérer ne se trouve plus actuellement sur des bandes en cassettes ou cartouches. En effet, des systèmes de copie miroir à distance rendent les données disponibles directement sur les systèmes de disques du site de secours. Ces techniques, encore minoritaires, se développent et sont décrites dans les grandes lignes au chapitre 8.

Coordination des moyens généraux

Assurée généralement par des assistantes de direction ou des administratifs maîtrisant l'environnement des sites concernés, cette mission consiste à assurer l'intendance en liaison avec les fournisseurs, le site de secours, les bureaux alternatifs, etc. – à savoir :

- gérer les déclarations et les demandes auprès des fournisseurs pour se procurer, par exemple, des tables, des chaises ou des ordinateurs, déménager certains biens, etc., conformément au plan ;
- prévoir le gîte et le couvert des équipes déplacées, ainsi que leur transport (réservations d'hôtel, de taxi, de trains, d'avion, etc.) ;
- procéder à l'identification et assurer le suivi des coûts engagés.

Retour à la normale

En général, une fois cette étape atteinte, le stress lié au sinistre a baissé d'un cran et la rapidité d'action cède le pas à la qualité d'exécution, afin de ne pas perturber les processus critiques. Si cette mission se trouve sous une contrainte de délai forte, cela peut signifier que les moyens de secours choisis n'étaient pas les plus adaptés.

Toutefois, cette mission est loin d'être négligeable, car son impact sur les activités reprises doit être le plus faible possible. Ainsi, il est primordial de planifier avec attention le retour vers le site primaire ou un nouveau site en cas de destruction totale du site primaire ou d'abandon.

Les tâches incombant à cette mission sont confiées à une équipe qui lui est entièrement consacrée.

Les listes de contacts

En temps normal, il est déjà souvent difficile de joindre quelqu'un ; que dire alors en cas de sinistre ! La liste des contacts a donc pour fonction d'établir précisément le rôle de chaque employé, en donnant ses coordonnées ainsi que la personne devant le remplacer en cas d'absence ou de non-disponibilité.

Véritable outil entre les mains des responsables du plan de continuité, ces listes demandent d'être établies avec le plus grand soin, dans le respect des contraintes dues à leur usage.

Listes par entité

Chaque entité potentiellement impliquée dans des actions de réaction face à un sinistre (départements en support opérationnel, départements métier) doit tenir à jour une liste des employés qui seront sollicités pour mener à bien ces actions. Ces listes doivent être faciles à trouver, lisibles et mises à jour régulièrement. Elles comportent :

- la dénomination de l'équipe ;
- les nom et prénom des membres ;
- le rôle de chacun (domaine, spécialité technique) ;
- les numéros de téléphone professionnel, personnel et portable de chacun ;
- le nom d'un éventuel remplaçant ou de la personne à appeler en priorité en cas d'absence ou de non-disponibilité.

Le tableau 4-1 montre un exemple d'une telle liste (les noms utilisés sont fictifs).

Tableau 4-1 : Liste de contacts – Service support production (SP)

Nom	Prénom	Domaine	Téléphone fixe	Téléphone portable	Téléphone privé
André	Jean-Luc	réseaux locaux	01-44-41-...	06-61-...	01-78-04-...
Bardeau	Jacques	responsable SP	01-44-41-...	06-66-...	01-67-61-...
Charles	Pierre	expert exploitation	01-44-41-...	06-82-...	01-44-41-...
Drumont	Albert	support MVS & zOS	01-44-41-...	06-03-...	01-92-66-...
Evenin	Emma	support Unix (1)	01-44-41-...	06-61-...	01-67-61-...
Figeac	Greg	support Windows	01-44-41-...	06-84-...	01-53-25-...
Gal	Loïc	support CICS, DB2	01-44-41-...	06-66-...	01-54-65-...
Judon	Alfred	support réseau	01-44-41-...	06-61-...	01-78-03-...
Klein	Helmut	support Unix (2)	01-44-41-...		01-44-41-...
Lamarre	Pierre	support Unix (3)	01-44-41-...	06-09-...	01-77-92-...
Marche	Louis	sécurité	01-44-41-...	06-86-...	01-75-26-...

Pour les listes de contacts, on privilégiera un classement alphabétique pour les noms propres ainsi qu'un libellé simple et universel pour les domaines.

Le tableau 4-1 indique, par exemple, que pour un problème concernant Unix et la sécurité, il faut tout d'abord appeler Emma Evenin (Unix 1) pour le support Unix, et Louis Marche pour la sécurité. Si Emma Evenin n'est pas joignable, il faut alors appeler Helmut Klein (Unix 2). Si Louis Marche est absent, il faut contacter le responsable SP, Jacques Bardeau. En effet, c'est la règle, lorsque aucun remplaçant n'est indiqué, il faut transférer la demande au responsable hiérarchique.

Certaines sociétés indiquent également si la personne est membre ou non d'un groupe intervenant dans le plan de continuité. En outre, cette information est aussi bien gérable dans des listes spécifiques aux groupes. Enfin, il est parfois mentionné le type d'information que la personne peut recevoir (rapport de sinistre préliminaire ou détaillé, par exemple), afin de désigner un destinataire au groupe de notification chargé d'envoyer les rapports.

Listes de constitution des groupes

Les différents groupes mentionnés plus haut sont constitués de membres désignés à l'avance, recensés dans des listes du même type. Ces listes devront plus que toute autre porter une forte attention à ce que leurs membres soient effectivement joignables ainsi qu'à la notion de remplaçant (ou d'adjoint).

Selon la taille des effectifs et du site à traiter, les groupes peuvent varier en importance ; la gravité du sinistre joue également un rôle majeur dans la constitution des groupes. Certaines personnes peuvent aussi appartenir à plusieurs

groupes. Tous ces aspects sont à décider en amont, afin d'être immédiatement opérationnel lors du sinistre. Certaines sociétés établissent à cet effet des listes indicatives de groupes et de membres. Désignant un chef de crise pour prendre en main les opérations, c'est lui qui se chargera en temps voulu de la constitution des groupes à partir de ces listes indicatives et de sa propre connaissance de l'entreprise.

Confidentialité et informations privées

Par respect de la vie privée, le fait que les numéros de téléphone personnel figurent sur les listes rend ces dernières confidentielles. Cela pose d'ailleurs un problème classique en cas de crise, puisque les données devant être accessibles en urgence sont davantage protégées que les données habituelles. Cette question de confidentialité, récurrente au cours des interventions d'urgence, doit être traitée spécifiquement (voir le chapitre 5).

Dans ces listes, il peut être également spécifié si l'employé a accès ou non à des outils de suivi d'incidents ou s'il dispose d'autorités spécifiques, cela pouvant s'avérer utile dans les actions de reprise.

Toutefois, il faut veiller à ce que les listes ne contiennent pas trop d'informations. En effet, plus il y en a, plus les listes sont difficiles à gérer et à mettre à jour – ce qui peut s'avérer problématique en cas de sinistre. N'oublions pas que nombre d'informations utiles peuvent être relayées par la suite par les responsables via le téléphone. Pour une gestion plus facile des listes, il existe sur le marché des outils permettant à chaque employé membre des listes de contacts, via de simples e-mails sur serveurs web, d'actualiser régulièrement son profil.

Constituer les groupes d'intervention

Pour élaborer son plan de continuité ou PCA, l'entreprise doit constituer les groupes d'intervention en fonction des compétences et du personnel disponible, sans oublier l'importance primordiale d'avoir « un pilote dans l'avion ».

La constitution des groupes mis en action en cas de sinistre s'appuie sur la structuration des missions décrite précédemment et sur la liste des missions à remplir. De la même manière, un responsable est nommé pour prendre les choses en main, ainsi qu'un suppléant en cas d'absence.

Affectation des missions

Dans l'exemple d'affectation suivant, les groupes envoyés en mission sont calqués sur l'organisation de l'entreprise.

Tableau 4-2 : Affectation des missions aux groupes d'intervention

Mission	Groupe responsable	Commentaire
Coordination du PCA	Gestion de crise	Responsable du groupe
Évaluation des dommages	Gestion de crise	Peut être déléguée localement
Déclaration d'activation	Gestion de crise	Responsable du groupe
Intervention des premiers secours	Secours locaux	Vérifier l'activation
Communication	Service de communication	Liste de contacts
Logistique et approvisionnement	Service logistique	Liste de contacts
Évaluation des risques	Gestion de crise	Mission permanente
Redémarrage métiers	MOA du site	Liste de contacts
Redémarrage utilisateurs courants	Groupe service PC	Liste de contacts
Remise en route informatique	Service IT	Liste de contacts
Récupération de moyens industriels	Service industriel	Liste de contacts
Récupération de bureaux	Service IT	Traite aussi les ordinateurs
Manipulation de matières dangereuses	Gestion de crise	Peut éventuellement être déléguée
Récupération des dossiers vitaux	Service archivage	Liste de contacts
Récupération des sauvegardes critiques	Service logistique	Liste de contacts
Coordination des moyens généraux	Service logistique	Liste de contacts
Retour à la normale	Gestion de crise	Pourra être déléguée ultérieurement

Ce tableau mérite certains commentaires.

- Parmi les groupes en charge des différentes missions, seul le groupe de gestion de crise est constitué lors du sinistre, les autres groupes étant des sous-ensembles de services préexistants au sein de l'entreprise. Ces groupes doivent avoir été formés à cette nouvelle mission.
- La mention « liste de contacts » signifie qu'il existe une liste, tenue à jour, avec un nom et des coordonnées.

- La mention « peut être déléguée » signifie que le groupe en charge de la mission peut en confier la réalisation à un autre, tout en suivant sa bonne exécution.
- Un service de communication n'est pas toujours présent sur le site sinistré. Il est donc primordial d'y envoyer des représentants attitrés, d'autant plus que si l'entreprise est connue, les chaînes de télévision seront sur place pour filmer et interroger les employés.
- La MOA du site désigne la maîtrise d'ouvrage informatique : dans le cas présent, c'est l'entité qui maîtrise le mieux les applications informatiques et les processus critiques.
- Le service IT (informatique) s'occupe ici de remettre en ordre de bon fonctionnement l'informatique et les bureaux, mais ce n'est pas toujours le cas. Dans notre exemple, l'entreprise a probablement un service informatique qui maîtrise bien les aspects d'infrastructure et de bâtiment.
- Le service « archivage » figure dans ce tableau, car il a la responsabilité des archives et de leur conservation. Ainsi, il est le plus qualifié pour récupérer ce qui doit l'être.

En fonction de ce qui précède, le responsable du groupe de gestion de crise peut constituer les différents groupes et décider du lieu où ils vont intervenir ainsi que des comptes qu'ils devront lui rendre (actions de reporting).

Ainsi, les groupes décrits plus haut peuvent être à géométrie variable d'une entreprise à une autre, tant que les missions restent assumées.

Former et sensibiliser les différents acteurs

Tout plan, quel qu'il soit, n'a pas lieu d'être si les personnes censées le mettre en œuvre ne savent pas ce qu'elles doivent faire, d'autant plus que les conditions de travail en cas de sinistre ne sont pas celles auxquelles le personnel est habitué. Une sensibilisation et une formation des acteurs s'imposent alors.

C'est pourquoi la notion de sensibilisation (*awareness*) est extrêmement importante dans la littérature anglo-saxonne comme pour les groupes de travail sur les normes britanniques (B*ritish* S*tandard* I*nstitute*), qui y accordent une importance accrue.

Ainsi, il est recommandé de mettre en place un programme de sensibilisation et de formation. L'engagement de la direction générale sur ce point est fondamental et des crédits doivent être débloqués pour ce programme. Par ailleurs, la DRH doit assurer le suivi des listes de personnel formé et à former.

Formation

On procède généralement en quatre temps.

1. Établir, dans les services, la liste des besoins en sensibilisation et en formation. Pour cela, il faut lister les employés impliqués dans les différents groupes ou recourir à une évaluation par la hiérarchie.

2. Faire une évaluation d'écart entre ce que les employés doivent connaître et ce qu'ils connaissent déjà.
3. Sélectionner, selon les budgets, les programmes de formation à mettre en place pour combler les écarts – il se développe actuellement sur le marché français une offre dans ce domaine.
4. Planifier les formations et contrôler les personnes formées et restant à former.

Sensibilisation

Par ailleurs, l'entreprise dispose de divers moyens de sensibilisation :

- les règlements intérieurs ou les manuels d'utilisation liés à l'informatique abordent – trop peu, hélas – les aspects de continuité d'activité (continuité de service, secours, restaurations, etc.) ; il est possible, et même recommandé, de développer les points principaux dans ces documents ;
- les affiches ou cartons à poser sur son bureau de type « conduite à tenir en cas de sinistre » avec indication des numéros de téléphone à appeler, par exemple, peuvent se révéler très utiles ;
- des séminaires ou autres événements d'entreprise peuvent régulièrement aborder le sujet ;
- la littérature sur la continuité d'activité se développe, y compris en langue française ;
- la participation à des campagnes de tests peut avoir un effet pédagogique, même si cela n'est pas l'objectif premier des tests (voir le chapitre 6) ;
- les divers audits et leurs rapports subséquents peuvent être l'occasion d'un rappel intéressant (voir le chapitre 13).

Comme dans les approches qualité ou sécurité, l'implication de la direction générale, qui indique ses orientations et ses choix en matière de continuité d'activité, s'avère primordiale. Celle-ci doit communiquer régulièrement, via la parution de notes ou autres, au sujet de la « politique de continuité » de l'entreprise. Le mot « politique » étant une traduction un peu biaisée de l'anglais *policy*, les mots « volonté d'orientation de la direction » conviendraient mieux. (Voir le chapitre 11 et les suivants sur ces aspects de gouvernance.)

Mettre à jour la constitution des groupes

Pour la pérennité du plan de continuité, il est indispensable d'actualiser régulièrement les groupes constitués pour réaliser les missions. Cette remarque est valable également pour les listes de contacts et pour les tableaux de missions et groupes décrits plus haut.

En matière de maintenance des listes de personnels à jour, la recette miracle n'existe pas. On limitera les risques d'obsolescence en procédant par deux approches concurrentes mais complémentaires.

- **Mise à jour par la hiérarchie** – Les responsables des équipes ou services conservent la liste des employés « réquisitionnés » en cas de sinistre, maintenue à jour au niveau de leur entité. En cas de modification, ils préviennent le responsable de la continuité d'activité.
- **Mise à jour par le responsable de la continuité** – Ce responsable (le chef du groupe de gestion de crise en général) maintient à son niveau une matrice de correspondance entre les groupes et les noms des personnes qui les constituent. Il est normalement averti des changements par les responsables métier. Pour éviter les erreurs, il révise régulièrement les listes en les faisant valider par les responsables.

De cette manière, les risques d'erreurs dans les listes sont limités, sans toutefois être éliminés.

Documents types

Plan de communication

Voici à quoi un plan de communication peut ressembler.

Plan de communication de crise

1. Objectifs de la communication de crise
2. Responsable et coordinateur
3. Conditions de déclenchement de ce plan
4. Message à transmettre
   - 4.1. Information générale
     - a. Événement
     - b. Impacts identifiés
     - c. Situation (à actualiser)
   - 4.2. Demandes particulières
     - a. Aux employés
     - b. Aux partenaires d'affaires
     - c. Aux clients
     - d. Au public
     - e. Aux parents, familles
   - 4.3. Qui contacter et comment ?
     - a. Pour en savoir plus
     - b. Pour signaler une information
5. Moyens de communication
   - 5.1. Presse, TV, radio
   - 5.2. Téléphone
   - 5.3. Internet, Web, e-mails

6. Informations générales de référence
   6.1. Sur l'entreprise
   6.2. Sur le site
7. Fréquence
   7.1. Selon le média
   7.2. Prochain communiqué
8. Validation et autorisation
   8.1. Qui valide ?
   8.2. Qui est habilité à communiquer ?
9. Trace de ce qui est communiqué (notes, enregistrements)

Plan de secours

Voici un modèle de plan de secours, mis en œuvre par le groupe d'intervention de secours (qui dépend ou pas, selon les cas, du PCA).

Ce plan, comme le plan de communication de crise, peut être joint aux documents annexes du plan de continuité.

Plan de secours

1. Cadrage
2. Responsabilités et périmètre
3. Personnel sur site et visiteurs
4. Équipe de secours : missions et responsabilités
5. Employés : responsabilités et comportements
6. Déclenchement de la procédure de secours
   6.1. Activation de l'équipe de secours
   6.2. Avertissement des autorités
   6.3. Alerte et évacuation du personnel
7. Procédures d'évacuation
   7.1. Signal d'alarme
   7.2. Systèmes automatiques (exemple : fermeture de portes)
   7.3. Voies d'évacuation
   7.4. Personnel responsable de zone et d'évacuation
   7.5. Lieux de rassemblement
   7.6. Décompte des personnes
8. Procédures de recherche et d'évacuation
9. Procédures spécifiques à un risque en particulier (tremblement de terre, nucléaire, produits spéciaux à risque)
10. Procédures spéciales de mise en protection pour certains matériels

Annexes : cartes, listes de personnels, numéros de téléphone, etc.

Chapitre 5

PCA : planifier les activités

Le chapitre précédent a permis de déterminer les missions à remplir et leurs groupes responsables. La planification proposée dans le présent chapitre permet de structurer les activités menées par chaque groupe dans le but d'accomplir au mieux leurs missions.

Le déroulement du plan de continuité est en effet conditionné par les impératifs du compte à rebours : déclenché au moment du sinistre, il égrène les minutes implacablement. La durée maximale d'interruption admissible (MTD) à ne pas dépasser ayant été déterminée pour chaque processus critique de l'entreprise, le PCA doit permettre d'ordonnancer au mieux les travaux dans le temps imparti. C'est le but de la planification présentée dans ce chapitre.

L'ensemble des activités décrites ici porte aussi le nom de PRA (plan de reprise d'activité).

Planning général en sept étapes

Le modèle de planning généralement retenu propose un déroulement en sept étapes. Si toutes ces étapes sont nécessaires, en réalité, leur importance relative pourra varier d'une situation à l'autre : certaines étapes prendront une heure et d'autres plusieurs jours ; selon l'impact du sinistre, certaines seront plus ou moins utiles. Décrites ici dans leurs grandes lignes, chaque entreprise devra ensuite les adapter à sa propre situation.

L'entreprise aura aussi tout intérêt à formaliser ce planning avec ses propres méthodes de gestion de projet. Par exemple, elle peut procéder à un découpage du projet en deux ou trois niveaux de structuration : chacune des étapes (premier niveau) pourra être structurée en plusieurs activités (deuxième niveau), qui elles-mêmes pourront contenir plusieurs tâches (troisième niveau). Ce sont ensuite chacune de ces tâches ou activités qui seront affectées à une personne ou à un groupe d'intervention décrit au chapitre précédent.

Le découpage présenté ci-après présente une structure en deux niveaux : les étapes et les activités.

Étape 1 – Première intervention et notification du sinistre

Le déclenchement de cette première étape ne va pas de soi. Lorsqu'un sinistre s'est produit, l'entité responsable de cette première mission doit en être avertie. Or l'expérience prouve que les personnes les plus proches du lieu du sinistre n'ont pas nécessairement le bon réflexe d'appeler immédiatement la personne ou le service adéquats. Le plus souvent, les employés préviennent leur supérieur hiérarchique et c'est lui qui enclenche la procédure d'avertissement des personnes en charge de l'étape 1 du plan de continuité.

Première intervention

Le coordonnateur du plan de continuité est alerté et déclenche le plan de continuité. Les dégâts et leurs conséquences sont rapidement évalués. Les activités à prévoir sont les suivantes :

1. recevoir l'alerte initiale à partir d'un centre d'appels, d'un *help desk*, d'un responsable sur site ou des autorités locales ;
2. avertir les secours locaux, ou vérifier qu'ils ont bien été avertis (pompiers, SAMU, police ou gendarmerie, etc.), afin d'assurer la mission de sauvegarde des personnes ;
3. accéder aux documents et informations concernant le plan de continuité ;
4. dans la mesure du possible, se rendre sur les lieux ; sinon, joindre un intervenant local désigné dans les listes de contacts ;
5. collecter un minimum d'informations sur le site sinistré : est-il accessible ? Est-il joignable par téléphone ? Le centre de gestion de crise est-il intact ?
6. activer le groupe d'évaluation des dommages (voir le chapitre 4) ;
7. réaliser une première évaluation rapide des conséquences du sinistre ;
8. détecter rapidement les causes des dégâts (utile si on peut y pallier, sinon ne pas y passer trop de temps) ;
9. conduire une évaluation rapide des impacts sur les activités de l'entreprise et lister ce qui ne fonctionne plus ;
10. établir un rapport préliminaire de sinistre.

Ces activités sont présentées dans leur ordre logique d'exécution, et doivent être affectées à divers intervenants. Cependant, le contexte réel du sinistre imposera souvent de faire avec les moyens du bord.

Rapport de notification

Cela consiste alors à alerter la direction générale et le centre de gestion de crise afin d'activer les équipes prévues dans le PCA (groupe de gestion de crise, etc.), comme cela a été présenté dans le chapitre 4.

Bien évidemment, le groupe de gestion de crise peut se réduire à quelques personnes, voire une seule au tout début. Cela dépend beaucoup de la taille du site sinistré. On ne travaillera pas de la même manière sur un site de 5 000 personnes avec 3 000 serveurs et sur un site de 20 personnes sans aucun matériel informatique. Le nombre de personnes et les compétences à prévoir doivent être en rapport avec le problème posé. Constituer le groupe peut prendre un certain temps et il faut commencer à agir avant que tout le monde soit là.

Le rapport produit à l'issue de cette première étape est capital, car il s'agit de la première information disponible sur le sinistre. De sa qualité dépendra l'adéquation des premières actions mises en œuvre.

Afin de ne pas perdre de vue les impératifs de rapidité et d'efficacité, ce rapport pourra être mis en ligne sur l'intranet et ainsi être accessible aux groupes d'intervention prévus. À cette étape, certaines sociétés insistent sur la confidentialité des événements et la nécessité de garder tout rapport secret. Il est alors important de rappeler par la même occasion qui est habilité à parler à la presse à ce moment.

Le rapport lui-même est un constat sommairement détaillé. En général, on y trouve une première évaluation des dégâts et des impacts sur l'entreprise, avec si possible une classification provisoire du sinistre selon les trois catégories retenues (sinistre mineur, moyen ou majeur). Il contient aussi tout ce qui concerne les risques résiduels sur les personnes, les biens et l'environnement. Enfin, il est utile d'y mentionner les moyens et équipements/services qui subsistent sur place pour intervenir.

Étape 2 – Évaluation et escalade

L'objectif de cette étape est d'affiner l'évaluation des dégâts afin de décider si, oui ou non, on lance les étapes ultérieures. Les activités suivantes peuvent être réalisées :

1. reprendre le rapport préliminaire de sinistre pour prendre connaissance des points en suspens ;
2. inspecter le site sinistré pour évaluer plus précisément l'impact du sinistre ;
3. évaluer les risques résiduels sur la santé et la sécurité des personnes et des biens ;
4. lister les dégâts touchant aux bâtiments, aux machines, aux ordinateurs ou à tout autre moyen de production ;
5. estimer les pertes matérielles, même grossièrement ;
6. déterminer les processus métier touchés, en les considérant selon leur degré de criticité ;
7. classer le sinistre en fonction de sa gravité (mineur, moyen, majeur, par exemple : voir le chapitre 4) ;
8. si aucun processus critique n'est touché, n'effectuer l'intervention que jusqu'au point 9 et continuer à surveiller la situation et son évolution ;

9. établir un rapport plus détaillé ;
10. activer les groupes de redémarrage des activités et de récupération technique et opérationnelle.

Le rapport détaillé donne les éléments nécessaires à la décision sur la suite des actions à entreprendre. Il peut être structuré selon le plan type ci-dessous.

Rapport détaillé de sinistre

1. Description rapide
2. Niveau du sinistre (selon échelle)
3. Processus critiques touchés
4. Pertes estimées
5. Origine des dégâts (feu, inondation, séisme, attentat, etc.)
6. Degré de détérioration
   a) des bâtiments et structures
   b) des processus de l'entreprise
   c) des matériels informatiques
   d) des moyens de production
7. État d'usage du site touché
8. Éléments à risque sur le site touché
9. Délai(s) estimé(s) de remise en état

Souvent, ce plan est déjà utilisé dans le rapport préliminaire établi à l'issue de l'étape 1, qui est alors un rapport détaillé partiellement rempli. Certaines sociétés fusionnent d'ailleurs les étapes 1 et 2 en une seule opération produisant un rapport intermédiaire.

Ce formalisme peut paraître un peu lourd dans une situation où il faut agir vite. L'objectif n'est pas ici de remplir des centaines de pages, mais de décrire vite et bien la situation. Réaliser et communiquer rapidement un bon descriptif évite d'être sans arrêt interrompu par des demandes de renseignements téléphoniques qui encombrent les lignes et surchargent les opérationnels. Le temps passé à rédiger le rapport représente donc une économie de temps.

Enfin, si l'entreprise a des clients ou des partenaires touchés par les événements, ce rapport est une pièce importante à produire, car il sera étudié en cas d'audit ultérieur.

Étape 3 – Déclaration de sinistre

Si le rapport en constate la nécessité, la société décide d'activer l'état de sinistre. Cette décision concerne tout d'abord les actions de reprise à lancer, en référence à la stratégie de continuité de l'entreprise (voir le chapitre 3), puis l'activation des ressources nécessaires à leur réalisation.

Communiqué

Le communiqué de déclaration de sinistre émis à cette occasion peut être structuré à partir des activités suivantes :

1. reprendre les éléments du rapport détaillé ;
2. parmi les options déterminées dans la stratégie de continuité de l'entreprise (vues dans le chapitre 3), sélectionner les plus adaptées à la situation : que fait-on sur le site principal ? Active-t-on le site de secours ; si oui qu'y fait-on ? Où place-t-on le centre de gestion de crise ? etc. ; cette opération peut être scindée en autant de parties qu'il existe de sites (principal, de secours, mobile, etc.) ;
4. réaliser un communiqué d'état de sinistre (voir le plan ci-après) ;
5. diffuser ce communiqué via le groupe prévu à cet effet ;
6. avertir le groupe de communication de crise.

Le communiqué d'état de sinistre peut avoir la structure type suivante.

Communiqué d'état de sinistre

1. Description rapide du sinistre
2. Lieu et heure de l'événement
3. Niveau du sinistre (sur l'échelle à rappeler)
4. Options de reprise choisies
5. Informations sur les sites de reprise
6. Estimation du temps de reprise nécessaire pour chaque processus
7. Nom de l'entité en charge du communiqué
8. Contacts, moyens de s'informer

Cette étape est cruciale et n'est pas facile à vivre. La communication a lieu au sujet du sinistre *et* des moyens d'y faire face. Il faut, de plus, prendre des décisions à partir d'informations en général incomplètes et y impliquer la direction générale de l'entreprise.

L'évaluation des temps de remise en état, par exemple, est souvent un piège. Pour décider vite et bien, on est en effet amené parfois à caricaturer la situation ou, à l'inverse, la sous-estimer.

> **Sous-estimation des dégâts : un risque supplémentaire**
>
> La société ITF possède des bureaux dans un bâtiment situé près d'un fleuve. Ce bâtiment héberge aussi un centre informatique (pour serveurs Unix et Intel). Un peu plus haut se situe l'ancien centre informatique où des mainframes IBM sont encore en activité.
>
> Une inondation touche le bâtiment de bureaux mais épargne l'ancien centre. À ce stade, la déclaration de sinistre prévoit de reloger les employés et d'activer un centre de secours pour les serveurs Unix et Intel. Les informaticiens pensent que le site des mainframes ne sera pas touché, aucune mesure importante n'est donc prise le concernant : il suffit sim-

> plement de rétablir les connexions entre les deux salles qui s'échangeaient des fichiers régulièrement, opération ne demandant pas plus de vingt-quatre heures.
>
> Malheureusement, l'eau continue de monter et l'alimentation électrique du centre IBM doit être coupée un peu plus tard pour des raisons de sécurité. Les mainframes, bien qu'au sec, ne fonctionnent plus... En catastrophe, IFT doit employer des mainframes de secours chez un autre prestataire, ce qui lui coûte beaucoup plus cher que si elle avait envisagé dès le début la perte complète de son système informatique sur les deux sites – sans compter la perte de temps en hésitations et travaux inutiles.
>
> **Moralité :** il vaut mieux parfois simplifier le problème pour travailler au plus tôt à une solution externe plutôt que chercher à sauver ce qui sera finalement perdu.

Les situations de panne franche ou de catastrophe provoquant des dommages matériels évidents sont, de ce point de vue, plus faciles à gérer : on ne se raccroche pas à l'espoir de redémarrer dans cinq minutes. Si l'on tarde à décider de passer sur un site de secours, c'est généralement que l'on fait le pari d'un redémarrage du site principal dans un délai raisonnable. Si ce pari échoue, le temps d'attente est finalement du temps perdu.

Activation du plan

Le communiqué est accompagné par le déclenchement concret du plan de continuité. Le groupe de gestion de crise a normalement été activé en fin d'étape 1, même si, en pratique, il se limite à ce stade à un responsable senior de l'entreprise, qui, bien souvent, n'est pas encore sur place, et à quelques responsables locaux du site concerné.

Il faut maintenant activer les groupes d'intervention prévus dans le plan (voir le chapitre 4). Bien évidemment, en fonction du problème posé et dans un objectif d'efficacité, l'équipe sera de taille différente : cinq à sept personnes peuvent très bien assumer les diverses missions suite à un sinistre mineur, tandis que si celui-ci est plus complexe (plusieurs sites touchés, avec des implications contractuelles graves en termes de continuité de service ou de sécurité), la taille de l'équipe sera d'autant plus conséquente.

Dans les entreprises les mieux organisées, il existe aussi des consignes de délégation de pouvoirs entre responsables nationaux et locaux, selon la gravité du sinistre. Cela peut être crucial dans les cas où le site sinistré est isolé du reste du monde ou s'il se trouve à l'étranger.

L'activation du PCA se découpe donc en quatre activités principales :

1. déterminer les personnels qui vont constituer les groupes pour mener les actions à venir ;
2. rappeler le niveau de gravité du sinistre et ce qu'il signifie ;
3. rappeler ou établir les circuits de décision et de reporting ;
4. indiquer les moyens de reporting et de suivi des actions.

Cette étape implique souvent de faire un choix, en vue de la constitution des équipes, entre les personnes idéalement pressenties pour gérer la crise mais pas

disponibles dans l'immédiat, et les personnes disponibles dont le profil diffère quelque peu de ce qui est souhaité. Pour remédier à ce type d'inconvénients, le point 2 ci-dessus permet, dans certaines entreprises, de libérer immédiatement des responsables en cas de gravité maximale, par exemple.

Étape 4 – Planifier la logistique d'intervention

À ce stade, un embryon d'équipe est en place et les options de reprise ont été sélectionnées au cours des étapes précédentes. Il s'agit maintenant, à partir de la documentation produite, même succincte, de mettre en œuvre les moyens techniques et humains pour les réaliser.

Désormais, les opérations vont se concentrer sur trois sites : le site sinistré, le site de secours et le centre de gestion de crise. Il faut donc planifier la logistique ainsi que les moyens humains et techniques nécessaires aux interventions sur ces trois types de sites.

Logistique

Gérer la logistique implique les activités suivantes :

1. activer les contrats concernant les sites de secours choisis chez des prestataires ; si les sites sont internes, commencer leur préparation ;
2. s'assurer que les sites ont les moyens de communication appropriés ; en cas de besoin, compléter ce qui existe ;
3. décider rapidement du meilleur emplacement pour le centre de gestion de crise et, selon le contexte, en prévoir éventuellement deux (un mobile, puis un fixe) ;
4. passer commande ou déménager les divers matériels nécessaires pour équiper les sites (PC, imprimantes, fax, papier, etc.) ;
5. lancer les éventuels déménagements prévus pour meubler les sites de secours ;
6. s'assurer que les sites de secours possèdent les dernières versions des documents (plan de continuité, listes de contacts) ou formulaires concernant les procédures manuelles ;
7. prévenir les sites de secours de l'arrivée d'éléments sensibles tels que des sauvegardes, dossiers importants ou éléments confidentiels ; déterminer à cet effet un contact sur place.

Moyens humains

En ce qui concerne les employés, il faut constituer les différents groupes et prévoir leurs déplacements sur les divers sites. Cela consiste à :

1. déterminer, en fonction des groupes à activer, les employés disponibles, procéder aux affectations puis avertir les intéressés ;
2. prévoir les déplacements et l'intendance (voiture, train, hôtel) ;

3. prévenir le responsable de la sécurité informatique pour que les droits d'accès en situation de crise soient attribués correctement et sous son contrôle.

Comme le montre l'exemple ci-après, ce dernier point, qu'il importe d'aborder sereinement, est souvent difficile à gérer. Il faut donc prévoir des procédures spéciales pour les situations de crise.

> **Importance des droits d'accès en situation de sinistre**
>
> La société CDE teste son plan de reprise : elle simule la perte d'un site et l'activation d'environnements mainframe éloignés de 200 km.
>
> Au bout de quatre heures, les machines sont en état de marche sur le site de secours et les connexions réseau sont réalisées. Malgré tout, les ingénieurs systèmes de CDE ne peuvent s'y connecter pour faire leur travail : ils n'ont ni les droits, ni les mots de passe !
>
> Insistant pour obtenir des droits d'accès, ils sont contraints par la hiérarchie à remplir les demandes officielles, traitées en urgence. Deux jours plus tard, les droits sont ouverts et les ingénieurs système peuvent enfin paramétrer les environnements techniques. Le test a finalement duré trois jours au lieu d'un seul prévu initialement.
>
> **Moralité :** ces tests ont amené CDE à modifier les procédures d'attribution des droits en cas de sinistre. On remarquera que les procédures en place ont été correctement respectées au cours de cet exercice, ce qui a permis de découvrir le problème. Rien n'aurait été plus simple, en effet, de passer outre.

L'ensemble de ces activités fait partie de la responsabilité du groupe de gestion de crise.

Étape 5 – Récupération et reprise

L'étape précédente a préparé les activités qui vont être réalisées dans l'étape 5. Cette dernière se déploie sur tous les sites concernés, qui peuvent être :

- le site original sinistré ;
- un site de secours informatique ;
- un site de secours pour les bureaux ;
- un site de secours pour la production ;
- le centre de gestion de crise ;
- le domicile de certains employés.

Présentons maintenant, site par site, la liste des activités.

Activités sur le site sinistré

Sur ce site, il faut avant tout arrêter la propagation des dommages, sécuriser la situation et enfin récupérer ce qui peut l'être. Souvent, il arrive aussi qu'on puisse y retrouver des lots de sauvegarde ou des documents importants sous diverses formes.

On peut distinguer quatre catégories d'activités, selon qu'elles touchent à la préparation, l'évaluation des dégâts, la sauvegarde et la récupération ou le transport des divers équipements récupérés.

Préparer

Toutes ces activités sont un préalable aux actions sur site :

1. s'assurer que le personnel prévu se trouve sur place et a les moyens d'agir (droits d'accès, protections diverses, etc.) ;
2. s'assurer que les configurations informatiques critiques sont localisées et connues : serveurs, système de stockage, réseau, etc. ;
3. s'il existe des schémas d'infrastructure et de réseau, les communiquer au personnel sur place ;
4. prendre connaissance des rapports déjà émis sur le sinistre, des consignes de sécurité, etc.

Évaluer, expertiser

Il s'agit maintenant d'évaluer plus précisément l'ampleur des dégâts dans le but de savoir comment y faire face :

1. inspecter l'état des bâtiments, des alimentations en électricité, gaz et eau ; évaluer les risques résiduels ;
2. identifier les dossiers critiques, leur état et les risques qu'ils encourent (eau, moisissure, feu, etc.) ;
3. localiser et identifier les matériels critiques (informatiques ou non), leur état et les risques qu'ils encourent ;
4. rechercher et évacuer les sauvegardes critiques, si elles sont sur le site, afin de les garder sous surveillance ;
5. évaluer le risque de dégradations pouvant encore survenir (écroulements, montée des eaux, etc.) ;
6. déterminer les options de protection et de récupération qui semblent les plus appropriées, en chiffrer les délais et coûts si possible ;
7. documenter rapidement tout ce qui précède, que ce soit par une prise de notes, une liste avec points de contrôle, un formulaire, un enregistrement audio, etc.

Sauvegarder et récupérer

On entreprend ici les premières actions de récupération du site, afin d'éviter que celui-ci ne se dégrade davantage :

1. se procurer et mettre en fonctionnement les divers équipements nécessaires (pompes à eau, générateurs électriques, systèmes de chauffage, déshumidificateurs d'air, bennes à ordures, pelleteuses, camionnettes, etc.) ;
2. éliminer les diverses substances à risques ou trop dégradées (carburants, papier imbibé d'eau, etc.) ;
3. évacuer et mettre en lieu sûr les équipements en bon état qui sont menacés s'ils restent sur le site ;
4. mettre dans un état sécurisé les équipements encore en fonctionnement mais inutiles ;

5. vérifier la situation des équipements en bon état et utiles puis les restaurer dans l'état souhaité ;
6. documenter ce qui est fait.

Transporter

Ces activités ont pour objectif de déménager sur le ou les sites de secours ce qui a été récupéré et doit encore servir :

1. pour chaque élément (matériels, documents, sauvegardes, meubles, etc.), déterminer le site de destination parmi les sites prévus ;
2. accompagner chaque transport de matériel de consignes spécifiques sur la prise en charge, la manutention, les précautions d'emploi, l'usage à destination et le nom du réceptionnaire ;
3. effectuer ou faire effectuer le transport ;
4. pour les sauvegardes ou documents ayant un niveau de sécurité élevé, respecter scrupuleusement les consignes ou, à défaut, les faire accompagner par un membre de l'entreprise.

Toutes ces activités doivent tenir compte du fait que certains processus sont critiques et nécessitent une remise en route plus rapide que d'autres. La priorité devant être donnée aux processus les plus urgents, il faudra donc, dans certaines situations, prendre une décision privilégiant les moyens techniques nécessaires aux processus critiques de l'entreprise. C'est pourquoi il est important que l'équipe sur place connaisse précisément les processus critiques et identifie rapidement les moyens qui leur sont liés.

Tout problème rencontré doit être décrit succinctement par écrit, car cela servira à améliorer le plan par la suite.

Activités sur le site de secours informatique

Le site de secours informatique doit être prêt à accueillir ou activer des matériels nouveaux. Il faut donc préparer le cadre, installer les matériels et logiciels, puis démarrer et restaurer les applications critiques dotées de données convenables.

Les besoins en termes de délais (MTD, RTO, RPO et WRT, expliqués dans le chapitre 2) ont été spécifiés ; il en va de même des configurations matérielles et logicielles nécessaires.

Préparer

Les activités suivantes visent à s'assurer que tout est prêt pour redémarrer le système d'information :

1. s'assurer que le groupe d'intervention est arrivé sur place et est bien opérationnel ;
2. vérifier que les différents délais (MTD, RTO, RPO et WRT) et priorités sont connus du groupe ;

3. vérifier que les listes d'inventaires et les configurations matérielles et logicielles nécessaires sur le site de secours ont bien été communiquées au groupe ;
4. s'assurer que les méthodes de redémarrage, les instructions de paramétrage et les éventuels outils (scripts, etc.) sont en la possession du groupe, ou connus de lui ;
5. vérifier que l'infrastructure (racks, câbles, fourniture électrique, plateaux, refroidissement) est convenablement préparée ;
6. recevoir les matériels et logiciels divers qui ont été envoyés sur le site en s'assurant de leur conformité ;
7. prendre connaissance des consignes associées aux matériels ;
8. recevoir et sécuriser les médias de secours : les cartouches de sauvegardes, les valises de bandes, etc ; les inspecter et les mettre en lieu sûr ;
9. faire un bilan général en comparant ressources prévues et ressources présentes ;
10. planifier la suite des opérations en fonction de ce bilan et des priorités des processus ;
11. s'assurer que les droits d'accès nécessaires aux travaux ont bien été attribués.

Arrivé à ce stade, il est malheureusement courant de constater des écarts entre ce qui est prévu et ce qui est réellement disponible. Il faut alors documenter ces écarts pour effectuer des réclamations auprès des prestataires et améliorer les listes d'inventaire et le plan de continuité.

Les points 2 à 11 peuvent être exécutés en parallèle par des équipes dédiées chacune à une catégorie de matériels (réseau d'un côté, serveurs de l'autre, par exemple) ou bien à une catégorie de processus ou d'applications.

Rappelons que les droits d'accès sont un point sensible. Des procédures assez simples, avec des identifiants et mots de passe utilisables en cas d'activation de plan de secours et conservés sous enveloppe cachetée, peuvent faire l'affaire. Tout ceci doit avoir été fait sous le contrôle du responsable de la sécurité du système d'information (RSSI).

Mettre en route l'informatique et le réseau

Il ne sert à rien de démarrer un serveur de secours s'il reste inaccessible via le réseau. Il est donc indispensable de remettre en fonctionnement ensemble informatique et réseau, en suivant la procédure indiquée ci-dessous :

1. étudier le plan d'implantation en salle des serveurs des machines de stockage et de leurs connexions ;
2. étudier les plans et cheminements des réseaux ;
3. effectuer les connexions physiques et brassages nécessaires ;

4. initialiser les serveurs qui ont besoin de l'être, démarrer les systèmes d'exploitation, exécuter les diverses procédures d'installation, de paramétrage ou de création d'images disques (*imaging*) ;
5. effectuer le paramétrage réseau des divers routeurs ou commutateurs ;
6. réaliser les connexions du réseau de stockage SAN (S*torage* A*rea* N*etwork*) ou nécessaires au stockage en réseau NAS (N*etwork*-A*ttached* S*torage*) pour les serveurs qui en sont pourvus ;
7. configurer les sous-systèmes (systèmes de gestion de bases de données, systèmes de fichiers, serveurs d'applications, moniteurs transactionnels, etc.), en utilisant au besoin les scripts ou procédures préparées à cet usage ;
8. mettre en place les protections de sécurité (pare-feu, anti-virus, etc.) ;
9. activer les liens avec les bureaux de secours ou les divers sites à couvrir ;
10. tester l'ensemble des opérations précédentes.

Ces tâches sont pour la plupart bien connues des ingénieurs système, à la différence qu'ici, les travaux sont menés avec un niveau de stress inhabituel. Par ailleurs, il se peut que les matériels ne soient pas ceux auxquels les ingénieurs système sont accoutumés. Tout cela accroît les risques d'erreur et le travail en binôme, s'il est possible, est donc vivement recommandé.

En cas de tâches hautement répétitives (lignes de commande à passer à l'identique sur des dizaines de serveurs, par exemple), on aura recours à des scripts de commandes. Encore faut-il les avoir prévus suffisamment longtemps à l'avance et pouvoir y accéder. Les scripts permettent aussi de réduire les erreurs de frappe.

Restaurer les applications critiques

L'infrastructure étant en place, il faut maintenant restaurer les applications en commençant par les plus critiques :

1. revoir la liste des priorités de restauration des applications ;
2. étudier la ou les procédures d'installation, de lancement de l'application et de récupération des données ;
3. vérifier les droits d'accès administrateur et système ;
4. vérifier la manière dont les utilisateurs et leurs droits sont gérés ;
5. restaurer ou installer les applications critiques et paramétrer l'environnement en conséquence ;
6. restaurer les données à partir du point de reprise prévu puis procéder aux vérifications de cohérence et d'intégrité prévues dans le plan ;
7. appliquer, si cela est prévu et réalisable, les traitements complémentaires pour remettre les données dans un état proche de celui où elles se trouvaient au moment de la panne ;
8. à partir d'un identifiant d'utilisateur de test, vérifier que le fonctionnement des applications est correct ;

9. à partir du site où se trouvent les utilisateurs, vérifier le fonctionnement à distance ;
10. prévenir les utilisateurs que l'application est accessible et leur indiquer les restrictions éventuelles.

Dans le cas d'un système de miroir distant, de routage d'entrée/sortie ou de tout autre mécanisme assurant une bonne disponibilité (voir le chapitre 8), les activités précédentes sont simplifiées de façon significative.

Là encore, les difficultés rencontrées seront documentées par écrit. Parmi les anomalies, il est courant de constater que seule une partie de l'infrastructure peut être rétablie : cela nécessite alors une analyse supplémentaire pour déterminer ce qui, malgré tout, peut être remis en marche.

Activités sur le site de secours de bureaux

Le site de secours de bureaux doit être prêt à accueillir des employés privés de leur site habituel. Les activités consistent à organiser les lieux, installer des matériels qui sont livrés et mettre le tout en état de marche.

Les besoins en termes de délais (MTD, RTO, RPO et WRT, voir le chapitre 2), ainsi que les besoins matériels (PC, bureau, formulaires, etc.), ont été spécifiés auparavant.

Préparer

Il s'agit d'assurer la préparation des intervenants qui inspecteront et organiseront les locaux :

1. s'assurer que le groupe d'intervention est arrivé sur place et est bien opérationnel ;
2. vérifier que les différents délais (MTD, RTO, RPO et WRT) sont connus du groupe ;
3. vérifier que les inventaires matériels des besoins sur le site de secours ont été communiqués au groupe.

Une fois tous les éléments entre les mains du groupe d'intervention, celui-ci peut s'acquitter des tâches suivantes :

4. inspecter ce qui existe sur place et détecter les manques ;
5. recevoir les envois (en provenance du site sinistré) et prendre connaissance des consignes associées ;
6. recevoir les nouveaux matériels prévus (PC, commutateurs réseau, serveurs bureautiques, etc.) ;
7. en fonction des manques, commander le nécessaire ou chercher une alternative dans l'entreprise.

Le groupe, désormais en connaissance de ce dont il dispose, ce qu'il va recevoir et quand, peut alors commencer à agir.

Installer les matériels de bureau et les moyens informatiques

Il faut commencer tout d'abord par les activités d'installation suivantes :

1. consulter les plans d'aménagement des bureaux pour les meubles, les PC et le réseau local, puis étudier les plans de câblage ;
2. installer les meubles dans les bureaux, avec les fournitures, puis y affecter les employés ;
3. installer et paramétrer le réseau local et les PC ;
4. établir les connexions au réseau général de l'entreprise ;
5. démarrer les PC, éventuellement en mode client léger (voir le chapitre 9) et non en mode habituel ;
6. paramétrer la téléphonie pour accueillir les nouveaux venus ;
7. si possible, router les appels entrants de l'ancien site vers le nouveau site de secours ;
8. mettre à disposition les dossiers critiques ou les CD/DVD-Rom importants provenant des sites où ils étaient conservés ;
9. indiquer aux nouveaux venus un numéro à appeler ou un lieu où se rendre, en cas de demande ou problème.

Au cours de ces activités, on veillera à respecter les priorités des processus critiques, en commençant par traiter les quelques utilisateurs prioritaires, par exemple.

D'un point de vue technique, si le degré de préparation du site est insuffisant pour un équipement parfait, il est possible de recourir à des solutions provisoires, telles que celles utilisées pour les câblages notamment (collés à l'adhésif sur les plinthes au lieu d'être logés en goulotte par exemple). Il est essentiel que les schémas de câblage disponibles soient à jour et de bonne qualité.

> **Importance de la validité des plans de câblage**
>
> La société EBU active son plan de secours et aménage rapidement un immeuble de bureaux en partie désaffecté pour y installer les employés d'un site sinistré.
>
> Le technicien en charge du câblage intervient, plan en main, dans les sous-répartiteurs, pour modifier les connexions afin d'y ajouter les nouveaux venus. Très vite, certains employés travaillant sur le site depuis longtemps se plaignent de l'impossibilité de se connecter au réseau. La pagaille se généralise.
>
> Le technicien constate vite que son plan de connexion est faux. Il arrive tout de même à revenir en arrière pour rétablir les connexions initiales. Les nouveaux venus, eux, devront se contenter quelques jours de câbles volants courant sur la moquette et de connexions lentes.
>
> **Moralité :** l'utilisation d'un plan non valide s'avère néfaste et empêche de câbler en fonction de l'existant. Il est donc primordial de maintenir à jour les plans de câblage.

Mettre en marche le système

Les opérations suivantes consistent à restituer à l'utilisateur son environnement de travail, même incomplet pendant un certain temps :

1. restaurer les postes de travail (PC, en général) avec les applications, données, identifiants et mots de passe prévus ;
2. mettre à disposition les dossiers critiques sous la forme prévue (papier, CD-Rom, DON, etc.) ;
3. mettre à disposition les procédures, formulaires ou documents nécessaires à un travail en mode déconnecté, tant que le réseau ou les serveurs ne sont pas prêts ;
4. traiter les demandes ou les transactions à la main, comme cela est prévu en cas d'indisponibilité du système informatique ;
5. conserver ce qui sera nécessaire à une saisie informatique lorsque le système général sera de nouveau disponible ;
6. lorsque le système informatique est de nouveau fonctionnel, en tester les points essentiels selon la procédure métier, puis vérifier ce qui a été ou non pris en compte ;
7. une fois que c'est possible, saisir les données manquantes dans le système informatique, en fonction de ce qui a été réalisé aux points 4 et 5 ;
8. Passer en mode de travail normal une fois la situation complètement récupérée.

En résultat de cette séquence d'actions, il arrive souvent que le système fonctionne un peu différemment de l'habitude : plus lent, moins ergonomique et encore incomplet, puisque bien que non perdues, certaines données ne sont pas encore disponibles. Il existe deux raisons à ce phénomène :

- le poste de travail fonctionne souvent en mode dégradé avec un PC plus ancien, avec des applicatifs en mode dit « client léger », ce qui dégrade le temps de réponse et le confort graphique ;
- il n'est pas toujours évident de pouvoir entrer dans le système les données traitées à la main – plus précisément, cela ne peut souvent pas être effectué par un utilisateur standard, car cela nécessite des autorisations d'un niveau plus élevé qui ne pourront être attribuées que plus tard.

Tout événement marquant, ou fait ayant posé problème, devra une fois encore être consigné par écrit.

Activités sur le site de secours de production industrielle

Une certaine analogie existe entre le site de secours de production industrielle et le centre informatique : dans les deux cas, il faut préparer les intervenants et les lieux, réactiver ou déménager du matériel et enfin le mettre en marche, le tester et le transmettre aux utilisateurs.

Préparer

Réalisées pour la plupart par le groupe d'intervention, les activités suivantes consistent à mettre le site en état de production :

1. s'assurer que le groupe d'intervention est arrivé sur place et est bien opérationnel ;
2. vérifier que les différentes contraintes de délais (MTD, RTO, RPO et WRT, expliqués dans le chapitre 2) sont connues du groupe ;
3. contrôler que le site de secours répond aux normes et aux diverses exigences en vigueur dans l'entreprise pour une production de la qualité voulue ;
4. s'assurer que les zones de stockage sont convenables, en particulier pour les matières à risque ;
5. s'assurer que les dispositifs de sécurité sont appropriés ;
6. vérifier l'infrastructure, l'approvisionnement en électricité et la présence des sources d'énergie prévues ;
7. vérifier que les listes faisant l'inventaire des besoins matériels sur le site de production de secours ont bien été communiquées au groupe ;
8. inspecter le matériel sur place et vérifier qu'il convient : quantité, caractéristiques… – penser aux moyens de manutention, très sollicités au début ;
9. détecter les éventuels écarts et manques, et en établir une liste en vue d'une action ultérieure ;
10. réceptionner les équipements, vérifier les contenus, lire les procédures et conduites à tenir ;
11. réceptionner les pièces, outils et tout autre matériel nécessaire ;
12. détecter et noter tout écart entre ce qui était prévu et ce qui a été reçu.

L'absence de certains équipements ou matériels peut avoir des conséquences paralysantes graves ; par exemple, l'insuffisance de moyens de manutention peut ralentir voire arrêter les opérations. À ce stade, ce problème peut être partiellement résolu en faisant appel à des fournisseurs locaux. Il est préférable, cependant, d'avoir prévu dès l'établissement du plan de continuité une quantité suffisante d'équipements critiques.

Mettre en marche

Les activités réalisées au cours de la phase de mise en marche permettent de rendre le site de production opérationnel :

1. étudier le plan d'occupation au sol et attribuer les emplacements ;
2. installer et mettre en état de fonctionnement les machines et outillages ;
3. répartir les stocks de matière première, les pièces et autres ressources indispensables ;
4. récupérer les procédures, consignes et descriptions des gammes de produits à partir des copies conservées en secours ;
5. installer et rendre opérationnels les téléphones, fax, télécopieurs, etc., puis router les communications ;
6. mettre en place les éventuels ordinateurs, imprimantes et connexions de réseaux locaux ou longue distance.

Tester et démarrer

Ces activités permettent de tester l'installation du site pour lui permettre de démarrer dans les meilleures conditions :

1. tester les différents équipements ;
2. tester les produits obtenus via ces équipements ;
3. agencer la logistique du site, retirer ce qui ne sert plus ;
4. tester les moyens de télécommunication, le système informatique et la bureautique ;
5. démarrer la production sur le site de secours.

Afin d'alimenter un bilan ultérieur, il est une fois encore bon de tenir une main courante des événements.

Activités au centre de gestion de crise

Le centre de gestion de crise doit être aménagé de façon à tenir son rôle de quartier général. Il est conseillé d'y avoir prévu l'essentiel à l'avance. Les premières activités consistent à tout mettre en place, tandis que les activités suivantes se répartissent sur divers pôles de préoccupation comme :

- le pilotage des interventions sur les divers sites ;
- la communication ;
- le pilotage des moyens humains ;
- le suivi financier, le suivi des assurances, ainsi que les aspects juridiques et légaux ;
- l'amélioration du plan de continuité en soi.

Ces activités sont à mener dans les tout premiers temps après l'occurrence du sinistre.

Mise en état du centre de gestion de crise

L'étape 4 a permis de décider de l'emplacement du centre de gestion de crise, qu'il s'agisse d'un local déjà prévu à cet effet, d'un conteneur de bureaux mobile ou bien d'un hôtel. Il s'agit désormais de le préparer, via les actions suivantes, pour le rendre opérationnel :

1. activer la mise à disposition du centre, c'est-à-dire ressortir les éléments importants normalement conservés sur place de leur lieu de conservation pour les rendre fonctionnels ;
2. avertir les employés attendus sur place ;
3. une fois sur place, vérifier que les équipements sont corrects ;
4. si besoin, faire établir l'électricité par le réseau ou par des générateurs ;
5. au besoin, mettre en place les meubles, équipements et fournitures diverses : bureaux, PC, tableaux, téléphones sur trois lignes (entrante, sortante et de secours), etc. ;

6. préparer les documents et matériels spécifiques à la gestion de sinistre : procédures, plan de continuité (papiers, classeurs), projecteur, listes de contacts et éventuellement des moyens radio ;
7. récupérer, depuis les sites de conservation, les dossiers critiques et les procédures spéciales en vigueur ;
8. prévoir le déplacement du centre, si ce site n'est que provisoire.

Pilotage des interventions

Piloter les diverses interventions est un rôle important – sinon vital – que le centre doit permettre d'assurer (voir le chapitre 4). Cela implique d'accomplir les actions suivantes :

1. garder comme objectifs les durées d'interruption maximale admissibles (MTD) : pour chaque processus critique, ces MTD doivent être connus et le temps écoulé doit être mesuré ;
2. constituer les groupes (voir le chapitre 4) et lancer les actions qu'ils doivent réaliser en donnant objectifs et priorités ;
3. suivre les actions réalisées par les différents groupes sur les différents sites, en sollicitant des comptes rendus des groupes à intervalles réguliers ;
4. évaluer et réévaluer les risques ; en garder une trace écrite pour chaque groupe ;
5. tenir un tableau d'avancement des actions sur chaque site, y compris le site sinistré ;
6. répondre aux demandes des groupes : décider en cas de demandes d'orientation, de choix de priorité ; conseiller en cas d'incertitude et de demande de vérification ;
7. réorienter les actions, redistribuer les ressources en fonction de la réalité du terrain et des évolutions constatées ;
8. tenir à jour l'évaluation des dégâts par rapport aux chiffrages initiaux : au fur et à mesure que les groupes travaillent, l'étendue exacte du sinistre se révèle ; certaines estimations se confirment, d'autres sont à revoir ;
9. obtenir certains documents (plans, inventaires, etc.) manquant aux groupes en action sur les sites, puis leur transmettre.

Communication

Situé aux premières loges, le centre de gestion de crise est le lieu où converge l'information correcte et où elle est actualisée. Il est donc naturel qu'il soit à la source des actions de communication sur le sinistre et son traitement et doit :

1. lancer le plan de communication de crise ; s'assurer de son exécution (voir le plan type en fin de chapitre 4) ;
2. maintenir à jour le tableau de suivi avec les moyens à disposition (tableau physique dans le couloir, site web, communiqués par e-mails) ; cela permet d'éviter un certain nombre d'appels au centre, coûteux en temps ;

3. tenir le comité exécutif ou la direction générale régulièrement au courant des événements ;
4. tenir informés les responsables clés des différents sites ou services concernés, en particulier ceux ayant connu des victimes ou ayant fourni des membres aux groupes d'intervention.

Suivi des moyens humains

Les groupes d'intervention sont actifs sur le terrain et accomplissent les activités et tâches déjà décrites par ailleurs. Au centre de gestion de crise, il reste à réaliser les activités complémentaires suivantes portant sur l'ensemble du personnel :

1. maintenir à jour la liste des employés indisponibles (blessés, décédés, en vacances, renvoyés chez eux, etc.) ;
2. fournir un soutien aux victimes et à leur famille (psychologique, médical, juridique, financier, etc.) ;
3. maintenir à jour la liste des effectifs opérationnels ;
4. recourir à des tiers (sociétés de services ou d'intérim) pour combler les manques en personnel ;
5. comptabiliser le temps passé par les prestataires et les employés en heures normales et supplémentaires ;
6. s'assurer des changements d'équipes et du respect du droit du travail ;
7. impliquer éventuellement des fournisseurs et des clients qui peuvent, en cas de coup dur, prêter main forte ; il peut éventuellement s'agir d'entreprises voisines ou de partenaires commerciaux.

> **Du bon usage d'un fournisseur**
>
> La société Métal-X subit une panne importante de son système informatique. Par conséquent, sa gestion de stock et sa facturation sont inopérantes pour une durée estimée à une semaine. Or, Métal-X connaît des problèmes de trésorerie et aimerait bien pouvoir envoyer au moins les factures du mois.
>
> Client de la société ITM qui fabrique des ordinateurs et des imprimantes, Métal-X a par ailleurs prévu de renouveler bientôt un parc d'imprimantes. Son vice-président appelle donc le directeur commercial d'ITM, lui explique le sinistre subi et demande conseil.
>
> Le directeur commercial d'ITM propose alors de prêter une machine à Métal-X et de réaliser chez lui l'impression des factures, de même qu'il est parfois amené à le faire pour certains gros prospects à titre de démonstration de ses nouveaux matériels. Quant à Métal-X, cela lui retire une belle épine du pied.
>
> **Moralité :** face à l'adversité, les fournisseurs aiment bien conserver des clients en forme. On a donc là une démonstration d'intérêt réciproque bien compris.

Suivi financier, juridique et des assurances

Il s'agit d'une part de garder un œil sur les dépenses spéciales générées par le sinistre et les actions de reprise, tout en défendant et préservant les intérêts de la société. Dans une situation difficile de sinistre, il faut conserver des preuves

pour les assurances et les divers recours possibles. Cette phase d'opérations implique notamment de :

1. suivre les engagements de dépenses effectués par les canaux non habituels ;
2. garder la trace des dépenses effectuées, éventuellement ventilées selon divers critères ;
3. estimer les coûts de réparation, de remplacement, de remise en état ;
4. effectuer une estimation financière pour la direction générale ;
5. prendre connaissance, avec les services concernés, des contrats d'assurance et de ce qu'ils prévoient en cas de sinistre ;
6. faire les déclarations en temps et en heure auprès des compagnies d'assurance ;
7. commencer à monter les dossiers pour les assurances (prendre des photos, chiffrer les pertes d'exploitation, éventuellement faire dresser des constats d'huissier, etc.) ;
8. détecter, si nécessaire, les écarts ou risques d'écarts entre les évaluations de l'entreprise et celles des assurances ;
9. impliquer le service juridique en leur faisant inspecter les différents contrats avec les clients et fournisseurs pour activer les démarches contractuellement ou juridiquement nécessaires.

> **Cas particulier : les sociétés de service informatique**
>
> Dans le cas de sociétés de prestation de service informatique, le sinistre a normalement déjà déclenché, auprès des gestionnaires de clientèle, des actions visant à avertir les clients et les utilisateurs dans les délais convenus. Ces sociétés se sont en effet contractuellement engagées à des temps de disponibilité et ont mis en place des procédures d'escalade auprès des clients et des responsables internes pour remonter les incidents graves. Le sinistre présente toutefois la caractéristique d'être un incident très grave et très long à réparer. C'est cet aspect exceptionnel qui doit être communiqué au client pour qu'il prenne ses dispositions.

Pour les sociétés plus traditionnelles, les perturbations concerneront davantage des aspects comme les délais de livraisons ou les dates d'expédition. Avertir les clients et fournisseurs dans ce cas n'est pas forcément un réflexe immédiat et il vaut donc mieux spécifier ce point dans le plan de continuité.

Amélioration du plan de continuité

Le centre de gestion de crise héberge les responsables qui exécutent le plan de continuité. Ils sont donc à même d'y détecter les défauts, carences, erreurs et limites. L'objectif est ici d'améliorer le plan.

Tout au long des sept étapes, il est bon de noter en marge les améliorations pouvant être apportées au plan ; celles-ci peuvent concerner :

1. des écarts dans la documentation ;
2. des différences entre ce qui était attendu et ce que l'on a trouvé sur site (en termes de matériels, logiciels, etc.) ;

3. des aspects non couverts qu'il aurait été bon d'inscrire dans le plan ;
4. des points insuffisamment détaillés ou, à l'inverse, des détails inutiles ou incorrects ;
5. des aspects matériels bloquants imprévus (par exemple, des matériels de secours sous clé alors que les clés sont introuvables) ;
6. toute autre suggestion d'amélioration.

Activités concernant les employés à domicile

Il est de plus en plus fréquent que les plans de continuité d'activité prévoient qu'une partie du personnel travaille depuis son domicile. Il s'agit en général de cadres qui, à l'aide d'un PC ou d'un terminal, sont autorisés à se connecter à des réseaux de l'entreprise ou à des services de partenaires divers.

Plusieurs situations se présentent selon que l'employé dispose d'un portable de l'entreprise qu'il emmène chez lui ou bien qu'il recourt à un PC fixe lui appartenant en propre ou prêté par l'entreprise. Dans tous les cas, les activités à prévoir sont :

1. déterminer les moyens techniques de l'entreprise mis à disposition de l'employé à son domicile ;
2. assurer que la configuration est gérée à long terme et permet un accès suffisamment sécurisé ;
3. rendre le contrat de travail de l'employé compatible avec cet usage ;
4. déterminer les moyens d'accès au réseau de l'employé (ADSL à son nom, au nom de l'entreprise, etc.) ;
5. protéger correctement le réseau de l'entreprise pour les usages prévus ;
6. doter la configuration de moyens de protection et de sécurité convenables ;
7. déterminer les applications utilisables de cette manière ;
8. attribuer et gérer les divers mots de passe ;
9. prévoir des accès de secours au réseau hors de l'entreprise ;
10. gérer la liste des sites web (URL) accessibles en cas d'activation du plan de continuité et la communiquer à tous les employés concernés ;
11. conserver et tenir à jour la liste des employés concernés.

Bien évidemment, il faudra prévoir ces cas de figure dans les consignes d'utilisation de l'informatique, en notant bien que les PC portables présentent un risque supplémentaire en raison de leur vulnérabilité au vol.

Si ce type des dispositifs permet à des employés de travailler depuis leur domicile, rien ne dit cependant que le réseau de l'entreprise pourra les accueillir s'il a été sinistré. En revanche, en cas de perte de locaux de bureaux, cette solution présente bien des avantages – d'autant qu'avec certains produits actuels, il est de plus en plus possible de travailler sur un PC en mode déconnecté et de se reconnecter, une fois le réseau à nouveau opérationnel, pour envoyer le travail

réalisé à l'entreprise. Ce mode de fonctionnement doit donc être considéré avec grand intérêt.

Étape 6 – Retour à la normale

À ce stade, le personnel a retrouvé des locaux et des moyens informatiques et industriels pour travailler, tandis que les processus les plus critiques de l'entreprise ont redémarré. Cependant, les moyens mis en œuvre n'étant pas les mêmes qu'avant le sinistre, les données en ligne ne sont peut-être pas totalement à jour. En effet, certaines informations qui ont été notées à la main dans des formulaires ne sont pas encore insérées dans le système d'information, de même que certaines données qui n'ont pas encore été collectées dans leur totalité.

L'entreprise fonctionnant en partie sur des moyens provisoires, le but est maintenant de revenir à la situation d'avant le sinistre. De plus, les processus non critiques n'ayant pas été traités en priorité, ceux-ci ne fonctionnent peut-être pas encore et nécessitent donc d'être redémarrés. C'est tout l'objet de cette étape de retour à la normale, qui va couvrir des activités pouvant être regroupées en trois objectifs :

- déterminer la cible définitive (site, matériel) ;
- réparer et préparer ;
- opérer la transition finale.

On notera que certaines activités ont pu démarrer en parallèle lors des étapes précédentes.

Déterminer les moyens définitifs

Pour toutes les conditions provisoires d'exploitation (moyens et sites de secours), il s'agit de déterminer les conditions cibles définitives : quelles conditions permanentes veut-on obtenir pour un retour de l'entreprise dans une situation équivalente à celle d'avant le sinistre ?

Cela concerne tous les éléments qui ont été sinistrés : le site informatique, le site de production industrielle et les bureaux. Dans une moindre mesure, cela vise aussi les données informatiques et les dossiers vitaux qui se trouvent peut-être encore dans un état de dégradation pouvant être amélioré. Voici une liste des activités à entreprendre dans ce but de cibler les besoins :

1. étudier les rapports d'inspection réalisés par le groupe de récupération technique et opérationnelle durant la phase précédente, contenant notamment une évaluation des dégâts ;
2. déterminer les hypothèses réalisables : retour sur le site d'origine ? déplacement sur un autre site ? rester sur le site secondaire et créer un nouveau site de secours ?

3. pour le système informatique : déterminer les configurations cibles à mettre en place en termes de serveurs, stockage et réseaux – au vu des évolutions du marché, les configurations diffèrent souvent de celles d'origine ;
4. pour les données : élaborer les plans de traitements ou de transactions nécessaires pour remettre entièrement les données à niveau – si ces traitements sont consommateurs de temps de calcul, étudier de quelle façon obtenir le surcroît de puissance nécessaire. Valider les droits d'accès spéciaux aux applications, aux données et systèmes ;
5. pour la production industrielle : déterminer les réparations à effectuer et les éventuels équipements supplémentaires à acquérir ;
6. envisager la meilleure façon de récupérer rapidement des moyens de secours : en effet, en situation de sinistre, le droit à l'erreur ou à l'accident est très faible. Prévoir éventuellement des contrats de secours provisoires de courte durée ;
7. prendre en compte les aspects financiers : apport des contrats d'assurance en valeur de remplacement, en pertes d'exploitation, etc. ;
8. à partir de tous ces éléments, élaborer un planning des travaux et actions à mener.

Si ces activités se limitent bien évidemment d'abord à ce qui a été sinistré, il est rare que tous les aspects soient à couvrir en même temps.

En général, il « suffit » de remettre en état le site primaire et d'évacuer le site secondaire. Cependant, certaines entreprises en profitent pour repenser leur implantation en cherchant à diminuer les risques à l'avenir. L'entreprise doit aussi se préoccuper de la récupération de sa capacité à résister et donc de ses moyens de secours.

> **Réorganisation d'un centre informatique après un incendie**
>
> La société SL2 possède un centre informatique bien isolé à la campagne. Sur ce site cohabitent les ordinateurs centraux, des serveurs divers et une cinquantaine de personnes (ingénieurs système) travaillant dans des bureaux très proches des machines, dans la zone à faux plancher pour certains.
>
> Un incendie se déclare. Il se propage rapidement et oblige à évacuer les lieux ; des câbles sont endommagés et certains serveurs touchés. La remise en état se révèle assez difficile car il faut décâbler puis recâbler la salle. Après enquête, il s'avère que l'origine du feu est un mégot jeté dans une poubelle...
>
> Le retour à la normale est accompagné alors d'une décision : le personnel travaillera désormais dans un autre bâtiment, situé au centre-ville. En effet, les techniques de pilotage à distance n'imposent plus de se trouver à proximité des machines ; les opérateurs de salle sont ainsi réduits au minimum et les risques sur place diminués.

Réparer et préparer

Les actions planifiées et décidées en phase précédente sont exécutées. Cela concerne :

1. la réparation des dommages dans les locaux et la préparation des salles et des bureaux en vue du réinvestissement des lieux ;
2. la remise en état des données et des dossiers sensibles ;
3. le suivi de toute activité sous-traitée, tel que cela a été décidé ;
4. la commande et l'acquisition des matériels et logiciels nécessaires ;
5. la réception, le contrôle, l'installation et le démarrage de tout ce qui est livré ;
6. le réapprovisionnement en consommables divers (papiers, cartouches, supports, etc.) ;
7. les câblages en salles et dans les répartiteurs, avec mise à jour des schémas ;
8. la mise à jour générale de toutes les configurations et des bases de données de configuration ;
9. le paramétrage et l'administration des droits d'accès, avec mise à jour ;
10. la remise à niveau des diverses protections de sécurité qui ont pu être modifiées durant la phase de fonctionnement en mode de secours.

Réussir la transition

Afin de ne pas trop perturber l'activité ayant désormais repris son cours, le retour sur des sites et des matériels stables et définitifs s'effectuera de préférence lorsque les employés sont absents – souvent, le week-end. Concernant l'informatique, les conditions de transition sont contraintes encore davantage, l'objectif étant de ne pas interrompre les processus critiques.

Souvent, face à cette opération délicate, les entreprises trouvent judicieux de suivre, en particulier pour tout ce qui concerne l'informatique, une procédure de gestion des changements de type ITIL.

Plusieurs cas de figure se présentent, éventuellement combinés : les systèmes qui opéraient sur le site de secours sont déménagés sur le site principal et/ou le site principal est doté de nouveaux matériels vers lesquels il faut basculer.

La transition pourra donc être réalisée via les activités suivantes :

1. planifier la transition, en prévoyant éventuellement un retour arrière en cas de difficulté ;
2. préparer à la fois le site cédant et le site recevant ;
3. installer, s'il y a lieu, les systèmes nouveaux sur le site principal et les initialiser ;
4. figer les données à un point de sauvegarde propre, réaliser les copies de sauvegarde et arrêter les systèmes qui vont déménager du site de secours ;
5. déménager les systèmes anciens sur le site principal s'il y a lieu, puis transférer les sauvegardes ;
6. installer les systèmes sur le site principal, les initialiser, puis mettre le réseau en fonctionnement ;

7. restaurer les sous-systèmes et les données sur les systèmes cibles ;
8. vérifier le bon fonctionnement des applications avec des représentants des utilisateurs ou des responsables applicatifs ;
9. attribuer les identifiants et les mots de passe correctement ;
10. rétablir les connexions téléphoniques ;
11. compléter les dossiers critiques en vue de les finaliser, puis les entreposer à l'endroit prévu ;
12. reprendre les opérations courantes ;
13. redémarrer les diverses protections anti-sinistres (sauvegardes, copies miroirs locales et distantes, etc.) ;
14. débarrasser le site de secours et le rendre à sa mission originale, en suivant les indications contractuelles ou les procédures ;
15. détruire éventuellement les informations confidentielles et rétablir la confidentialité à son niveau nominal exigé en fonctionnement normal.

À la fin de cette étape, l'entreprise se retrouve dans une situation semblable ou équivalente à celle qu'elle connaissait avant le sinistre. Cela ne signifie pas qu'elle utilise les mêmes moyens à l'identique, mais qu'elle emploie des moyens adaptés à sa nouvelle situation et qu'elle dispose à nouveau de moyens de secours opérationnels.

Étape 7 – Bilan d'après sinistre

Cette étape finale ne doit pas être négligée, car elle est riche d'enseignements concernant le plan qui vient d'être exécuté face à un sinistre. Il s'agit là d'un test grandeur nature.

Normalement, comme cela a été préconisé tout au long des étapes précédentes, les anomalies constatées ont été notées par les membres des groupes d'intervention et les divers responsables. Si ce n'est pas le cas, il faut demander alors un bilan écrit aux différents chefs de groupes.

Les anomalies reportées sont couramment classées en trois niveaux de gravité.

- **Les anomalies bloquantes :** elles ont empêché que le plan soit exécuté comme prévu, sans possibilité de contournement. C'est le cas, par exemple, lorsqu'un site de secours prévu n'existe plus car le contrat de secours a été résilié, ou encore lorsque ce site a changé de destination suite à une fusion, sans que le plan de continuité ait été mis à jour.
- **Les anomalies gênantes :** elles ont empêché l'exécution du plan conformément à ce qui était prévu, mais il a été possible de trouver une solution de contournement. Cela se produit souvent lorsque les documents comportent des inexactitudes : les serveurs prévus ne sont pas exactement ceux qu'il faudrait, ou les quantités de postes de travail de secours, par exemple, ne répondent pas au besoin.

- **Les anomalies simples :** elles ont provoqué des pertes de temps ou des efforts supplémentaires. C'est l'histoire classique des clés absentes du tableau qu'il faut aller chercher chez le collaborateur.

Ces anomalies résultent souvent de défauts ou de laxisme dans l'actualisation des bases de données de configuration ou dans le respect des consignes.

En outre, il arrive aussi que des suggestions remontent pour améliorer le plan de continuité. Tous ces points d'amélioration peuvent faire l'objet de nouvelles actions à planifier et à réaliser, avec chiffrage du coût. L'effort à fournir devra alors venir des opérationnels eux-mêmes plutôt que des personnes en charge de la continuité.

Les actions de sensibilisation et de formation du personnel à l'intérêt de la continuité d'activité peuvent permettre d'éviter bon nombre de ces difficultés.

Comment affecter les tâches ?

La description d'activités qui précède, répartie selon un planning en sept étapes, permet à l'entreprise de sélectionner les actions qu'elle doit entreprendre, avec un déroulement adapté à son contexte. Il se pose alors le problème de l'affectation de ces activités – éventuellement subdivisées en tâches – à des employés en charge de leur exécution.

Cette affectation doit se faire en respectant les responsabilités des différents groupes définis dans le chapitre 4.

Spécificité du PCA

Dans une approche de planification de projet classique, une tâche est confiée à une personne donnée, assortie d'une charge et d'une durée. Dans certains cas, la tâche peut être accomplie deux fois plus vite si deux personnes y travaillent en parallèle. Dans d'autres cas, la durée est incompressible. Ce sont là des considérations habituelles en gestion de projet.

Dans le cas particulier de la continuité d'activité, la situation est plus problématique, car :

- on découvre l'ampleur du travail à effectuer au fur et à mesure qu'on l'effectue ;
- les personnes disponibles ne sont pas – elles non plus – connues à l'avance, ce qui rend illusoires les affectations précises planifiées.

La durée de l'activité apparaît donc comme la seule variable d'ajustement. Or c'est justement là que réside la difficulté, car cette durée est contrainte par les MTD (durées maximales d'indisponibilité admissibles). Tous les paramètres devront donc être ajustés en fonction des délais de MTD. Cela signifie que les équipes seront à géométrie variable aussi bien dans leurs effectifs que dans les compétences représentées.

Tableau 5-1 : Approche de projet classique, peu adaptée au PCA

Étape	Activité	Tâche	Personne	Charge	Durée
PCA N° 1	1.1.5 collecter des infos sur le site	b) vérifier l'accessibilité	Chef du centre informatique	2 heures/homme	2 heures
PCA N° 5	5.2.5 installer les serveurs	c) installer les 10 serveurs Unix/Oracle	2 ingénieurs système Unix	5 heures/homme	2,5 heures
		d) installer les 24 serveurs WinTel	4 ingénieurs système Windows	8 heures/homme	2 heures

Le tableau précédent décrit un idéal qui ne se présente pas forcément dans la réalité de l'après sinistre. Si au lieu des six ingénieurs prévus, il n'y en a que quatre et qu'ils ne sont pas spécialistes des technologies adéquates, les délais vont s'allonger. Il faudra donc choisir entre les serveurs à installer en premier ou bien trouver des ingénieurs supplémentaires. La seule indication intéressante et exploitable est ici la charge prévisionnelle. Elle permet au responsable de dimensionner ses équipes et les travaux en fonction du délai à tenir.

Charges et délais cibles

L'exemple qui précède explique pourquoi l'approche généralement retenue consiste à raisonner en charge prévisionnelle par unité de travail (par serveur, par exemple).

Dans tous les groupes, le responsable a donc deux paramètres en tête :

- la charge totale estimée pour le travail à faire ;
- le temps écoulé depuis l'interruption des activités.

Il en déduit donc les effectifs dont il a besoin en théorie pour réaliser, dans le délai maximal admissible d'interruption (MTD), les tâches nécessaires. Dans la réalité, les spécialistes savent à peu près en combien de temps telle ou telle action doit être accomplie et combien de personnes sont nécessaires idéalement pour la mener à bien dans les délais impartis. C'est le rôle du chef de groupe de trouver les profils les plus compétents parmi le personnel disponible, soit à l'extérieur du site, soit dans l'entreprise.

Du réalisme avant tout

Un planning prévisionnel précis et figé est irréaliste en situation de reprise après sinistre. L'affectation des personnes aux tâches par le chef de groupe se fait donc au coup par coup selon la réalité du sinistre. Ce qui importe ici, c'est d'affecter un ensemble d'activités à un groupe et à son responsable. Le plan doit donc

indiquer ces affectations et le responsable de groupe connaître ses missions (voir le chapitre 4).

Le plan peut, en plus, donner des indications de charge par type de travaux, ce qui permet d'évaluer la quantité totale de travail à produire. Souvent, les spécialistes (s'ils sont là…) sont capables d'effectuer des évaluations réalistes.

En fonction du chronomètre, qui court depuis l'arrêt des activités critiques de l'entreprise, le chef de groupe cherche à composer ses équipes avec des personnes efficaces et aptes à atteindre l'objectif du groupe. Il demande de l'aide au chef de groupe de gestion de crise, en cas de besoin et lui fait un rapport d'avancement régulier. Ce responsable central a donc un rôle d'arbitrage entre les diverses demandes qu'il reçoit des différents groupes.

Ces arbitrages sont multiples et complexes. On peut préférer privilégier les activités prioritaires afin d'en remettre quelques-unes en route. À charge égale et personnel identique, on aura souvent soit toutes les tâches avancées à 50 %, soit la moitié des tâches terminées. Mieux vaut alors choisir la deuxième situation, même si elle est plutôt complexe à réaliser : autant avoir quelques activités qui fonctionnent que rien du tout.

Chapitre 6

Tester le plan de continuité

À ce stade de son élaboration, le plan de continuité ne correspond qu'à une suite de travaux, de réflexions et de décisions synthétisés dans plusieurs documents. Après cette organisation théorique, il est maintenant indispensable de tester le plan de continuité afin de s'assurer de ses applications concrètes.

Cela permet de valider la stratégie, les hypothèses, l'attribution des missions, les plannings et les recommandations qui ont été mis au point lors des étapes précédentes. Il vaut mieux, en effet, que les difficultés potentielles soient rencontrées durant un exercice de test plutôt qu'au moment de l'exécution du plan, en situation réelle de sinistre.

Cadrage des tests

Il est indispensable de définir une politique de tests pluriannuelle. L'objectif général est divisé en objectifs tactiques respectant un calendrier précis et validé par les différentes parties prenantes. Ces aspects de gouvernance sont abordés dans le chapitre 11.

On devra également déterminer la méthode à suivre pour appliquer les différents types de tests afin d'atteindre les objectifs fixés. L'entreprise doit en effet mettre en œuvre une démarche qui lui permette de vérifier, d'assimiler et de se familiariser avec son plan de continuité, ayant recours aux tests pour l'améliorer.

Objectifs

Un exercice test peut avoir un ou plusieurs objectifs. Il est important de définir à l'avance cet objectif, car le déroulement et le suivi des tests en dépendent grandement.

Valider l'efficacité du plan

Les exercices de test du plan de continuité permettent de vérifier son bon fonctionnement. Les points suivants doivent être validés ou, le cas échéant, faire l'objet d'un plan d'action qui les rendra plus adaptés ou efficaces :

- les responsabilités définies dans le plan sont prises en charge par les bonnes personnes ;
- les activités sont convenablement définies et produisent les résultats attendus ;
- la synchronisation, les durées et les charges prévues dans le planning sont bonnes ;
- les étapes définies dans le planning se déroulent comme prévu ;
- les processus critiques sont redémarrés en temps voulu.

Identifier les points faibles

Aucun plan n'étant parfait, l'exercice de test est l'occasion de détecter certains points faibles, parmi lesquels on distingue :

- les difficultés d'accès à la documentation, aux listes de références, de noms, de configurations ;
- les délais pour constituer les groupes, en raison de l'indisponibilité immédiate des responsables ;
- le caractère irréaliste ou incomplet de la stratégie de continuité se révélant dans son application ;
- les erreurs dans les documents ou listes de contacts, de ressources, etc. ;
- les omissions de personnes ou de tâches nécessaires ;
- la différence entre la réalité et ce qui est prévu dans le plan : conditions du matériel informatique (tel serveur censé être sauvegardé régulièrement mais qui ne l'est pas, par exemple), ressources présentes sur le site de secours, etc. ;
- les soucis imprévus de dernière minute (tel logiciel ne peut être utilisé car la clé logique n'est pas attribuée, telle porte est fermée à clé et celle-ci est introuvable…).

> **Il n'y a pas de clé, hélas !**
>
> La société BCD doit interrompre son alimentation électrique sur toute sa salle informatique pour cause de travaux. Elle décide à cette occasion de simuler une panne de courant, tout en prévenant le personnel, afin d'observer comment se passe l'arrêt des serveurs en salle.
>
> Le jour *j* arrive : le courant est coupé, et on passe alors sur les onduleurs, qui assurent, prévoit-on, environ 50 minutes d'autonomie. Les opérateurs lancent les procédures d'arrêt des machines correctement. Pour certaines d'entre elles, il faut se rendre dans la salle informatique : tout se passe bien, les opérateurs prévus ont effectivement les droits.

> La plupart des machines en salle sont accessibles sans difficulté et peuvent donc être arrêtées. Mais certaines d'entre elles se trouvent dans une armoire fermée à clés, sans que cela ait été prévu. Cherchant alors les clés, on finit par les trouver mais elles ne sont pas clairement identifiées, ce qui fait perdre du temps pour les essayer une à une. Or, le chronomètre tourne !
>
> En fin de compte, il reste deux machines dont l'accès est impossible : la clé d'armoire est trouvée mais pas la deuxième nécessaire pour activer le clavier ! Ces deux machines finissent par s'arrêter, faute de courant, ce qui n'était pas prévu. Or il se trouve que ces machines sont justement jugées critiques.
>
> **Moralité** : un petit oubli a failli tout faire échouer ! Concernant les machines critiques, il vaut mieux analyser à l'avance et dans le détail les problèmes potentiels.

Vérifier la validité du plan

Le plan de continuité part d'une photographie de l'entreprise et de ses partenaires à un moment donné. En raison des évolutions qui ne manqueront pas de se produire, le plan ne sera donc pas toujours d'actualité et il faudra régulièrement procéder à une mise à jour. La liste des éléments à remettre à jour est longue. Une procédure particulière est normalement prévue pour cela (voir le chapitre 12), mais elle n'est pas toujours appliquée correctement. Parmi ces éléments, on peut citer :

- les organigrammes et les listes de contacts ;
- les informations concernant les partenaires (fournisseurs de sites de secours, dépanneurs, etc.) ;
- les caractéristiques des systèmes techniques de toute sorte, connaissant des modifications régulières qui doivent être suivies afin que leur secours soit de même niveau.

Aucun exercice de test ne se révèle sans surprise sur ces aspects. L'exercice permettra non seulement la mise à jour des listes, mais surtout l'amélioration de la procédure de tenue à jour elle-même, en détectant ses faiblesses. L'un des meilleurs résultats que l'on puisse obtenir est d'ailleurs la sensibilisation des responsables chargés de cette mise à jour.

Former les employés

Cet objectif est très souvent mis en avant par ceux qui pratiquent des tests réguliers. Pour les employés comme pour les responsables, le premier test est le plus difficile car « on ne sait pas ce que l'on a à faire ». Les tests suivants ressemblent davantage à des répétitions et des exercices de rodage.

Dans l'idéal, les employés devraient parvenir à :

- respecter les affectations aux groupes et attributions d'activités prévues par le plan ;
- réagir efficacement face à toute sorte d'imprévu (absence de personnel, allongement des délais, situations non conformes au plan, etc.) ;

- se familiariser avec les locaux de secours, le centre de gestion de crise, les trajets à effectuer, les lieux à visiter (pour récupérer des bandes, par exemple) de manière à parer à toute éventualité ;
- utiliser aisément les moyens de communication et avoir le réflexe de rendre des comptes (reporting).

L'exercice de test se révèle ainsi être un bon moyen de former les employés, qui peuvent eux-aussi proposer des améliorations du plan.

Pour les employés non directement impliqués dans les tests, la sensibilisation aux problèmes de continuité est un résultat intéressant de la campagne de tests.

Méthodes de test

Il existe plusieurs méthodes pour tester un plan, que celui-ci concerne la continuité ou pas d'ailleurs. Les principales méthodes en usage sont décrites ci-après. Le coût et le risque associés au test sont variables en fonction de la méthode choisie.

Test de vérification (check-list)

Ce type de test est peu onéreux et permet de préparer des tests plus approfondis. Il consiste à passer en revue le plan de continuité et les documents associés pour en vérifier l'exactitude et l'applicabilité, tout en inspectant la disponibilité des ressources prévues. En particulier, cela revient à vérifier :

- l'exactitude des listes de contacts et des numéros de téléphone ;
- la bonne documentation des applications critiques et des systèmes informatiques associés ;
- la bonne description des dossiers vitaux (existence, lieu de conservation, etc.) ;
- la présence effective des sauvegardes dans les lieux prévus, sous la forme attendue, aux dates voulues ;
- l'existence des formulaires nécessaires aux procédures dégradées, avec la bonne description desdites procédures ;
- la bonne tenue des manuels d'installation ou d'intervention prévues sur le site de secours ;
- la présence sur le site de secours du matériel et des documents qui sont censés s'y trouver ;
- la présence au centre de gestion de crise des matériels et équipements prévus, en bon état de fonctionnement.

Ces vérifications peuvent se faire régulièrement. L'implication des groupes d'intervention, même si elle est intéressante, n'est pas nécessaire.

Inspection de documents (walk-through)

Appelé parfois « test en chambre », l'inspection de documents consiste à lire les documents constituant le plan de continuité pour en dérouler, virtuellement ou à blanc, le scénario d'exécution.

Avant de réaliser ce type de test, il faut déterminer un scénario précis de sinistre. Par ailleurs, on doit avoir remis aux membres de l'équipe de test une description de leurs responsabilités, des activités à effectuer et des procédures à suivre. Le test consiste ensuite, pour les personnes impliquées, à jouer le rôle de leur responsabilité, en « déroulant » les activités à effectuer, tout en suivant les procédures avec leur équipe. Le but est de vérifier que l'ensemble est correctement conçu et opérationnel.

Le fait de rassembler des groupes avec des responsabilités diverses dans le même exercice se révèle très intéressant, car cela permet éventuellement de :

- détecter des recouvrements de missions (deux groupes voulant faire la même chose) ;
- découvrir des lacunes (personne pour certaines activités) ;
- constater des trous dans les procédures, ou encore des points inapplicables ou inutiles ;
- observer éventuellement des difficultés dans les activités ou réajuster le planning.

Ce genre de test a l'avantage de familiariser les équipes avec leurs collègues, les rôles de chacun, les sites de secours et leurs ressources, les circuits de décision et de reporting. Les personnes impliquées apprennent ainsi à vivre le plan de continuité. Afin de rendre les tests plus réalistes, les équipes peuvent d'ailleurs être dépêchées sur les lieux réels d'intervention.

Simulation

Ce test est plus élaboré et plus coûteux que les précédents. Il s'agit en effet de simuler une interruption d'activité due à un sinistre et d'exécuter la portion du plan de continuité correspondante.

La mise en œuvre de ces tests peut comporter plusieurs variantes, dont vont dépendre le degré de perturbation des activités de l'entreprise et le coût du test :

- simuler des activités (l'arrêt d'un serveur, par exemple) ou les effectuer réellement (arrêter effectivement le serveur) ;
- faire la simulation sur un site de production réel ou sur un site de secours ;
- demander aux employés concernés par les activités touchées d'arrêter effectivement de travailler ou les laisser continuer ;
- faire travailler une partie du personnel sur le site de secours ou employer les moyens de secours avec des procédures dégradées ;
- se limiter à certaines portions du plan, concernant une activité de l'entreprise en particulier ou une partie d'un site ;
- se concentrer uniquement sur certaines étapes du plan, comme les trois premières, qui peuvent nécessiter un rodage particulier.

En outre, ces tests de simulation peuvent être particulièrement intéressant pour vérifier certains points particuliers tels que :

- le degré de réactivité des prestataires impliqués ;
- l'efficacité de la sortie des sauvegardes de leur lieu de conservation ;
- la faisabilité de l'utilisation de tel ou tel site en secours pour les bureaux ;
- le temps à prévoir pour certains déplacements ;
- la durée nécessaire à la reconstitution des données sur le site de secours ;
- la viabilité des procédures manuelles ;
- l'efficacité du plan en cas d'absence de téléphonie ou de messagerie ;
- l'efficacité des circuits de décision en cas d'absence de certains responsables.

La simulation peut d'ailleurs être centrée sur des points particuliers pour lesquels des doutes subsistent. Dans ce cas, les résultats permettent d'apporter de réelles améliorations au plan.

Test parallèle

En informatique, le test parallèle s'emploie pour remplacer un système par un autre et ainsi vérifier qu'ils donnent le même résultat. Ce genre de test permet d'asseoir la confiance dans un système de secours et dans les procédures de restauration des données. Dans le cadre de la continuité d'activité, il s'agit de faire fonctionner le système de secours en parallèle du système principal, afin qu'il soit le plus ressemblant possible. Pour atteindre cet objectif, on procède comme suit :

1. le système principal fonctionne normalement sur son site ;
2. à un moment donné, on fait comme si un sinistre s'était produit : on commence à garder une trace manuelle des transactions saisies sur le système principal (en faisant comme s'il n'existait plus) ;
3. le système de secours prévu est mis en route sur le site de secours ;
4. les diverses sauvegardes disponibles sont récupérées et restaurées sur le système de secours, en appliquant au besoin les journaux ;
5. les transactions manuelles (du point 2) sont saisies sur le système de secours ;
6. on compare alors les deux systèmes, en notant tout écart concernant les données.

Les écarts de données sont dus aux périodes durant lesquelles l'enregistrement des transactions n'a pas été fait ou communiqué – par exemple, le laps de temps entre la dernière sauvegarde et le sinistre simulé. Les raisons peuvent être diverses et les solutions techniques proposées également. Dans tous les cas, cela doit donner lieu à un plan d'action.

Ce type de test est délicat et parfois coûteux ; on l'effectue en général quand les autres tests ont été menés avec succès. Le test parallèle peut être réalisé assez facilement sur certaines solutions techniques (telles que le SGBD, voir le chapitre 8).

Grâce à ce test, il est également possible de vérifier si les employés ont bien accès au système de secours. Enfin, il peut se révéler utile pour mesurer le temps nécessaire à chaque récupération. On pourra ainsi analyser la manière de réduire ces délais s'ils s'avèrent trop longs.

Test interruptif total

C'est le test complet. Tout se passe comme si un sinistre avait réellement eu lieu. Le plan est activé en grandeur nature et les activités qu'il prévoit sont réellement exécutées.

Si le test le permet, l'activité « normale » peut continuer. Il faut bien évidemment avertir les clients, fournisseurs et partenaires de cette interruption programmée. On cherchera pour cela à éviter les périodes de grande activité ou les pointes de transactions.

Comme il s'agit du test le plus onéreux, il ne sera réalisé que lorsque les autres tests auront été effectués et que les améliorations à apporter découvertes au cours de ceux-ci auront été intégrées. Ce genre de test est très rarement pratiqué.

Faut-il annoncer le test ?

Faut-il prévenir les employés et les partenaires de l'entreprise que le plan de continuité sera testé (en leur indiquant le site, le jour et l'heure précis) ? Ou vaut-il mieux, au contraire, garder le secret et le déclencher à l'improviste ? Les avis divergent, mais la façon de procéder dépendra aussi de chaque situation.

En effet, plusieurs éléments doivent être pris en considération pour déterminer la méthode à adopter, dont certaines prêchent en faveur d'une annonce :

- si le plan de continuité n'est pas encore tout à fait maîtrisé, rien ne sert de compliquer les choses en réalisant des tests à l'improviste ;
- si le plan comporte des défauts, que le test soit annoncé ou non, ils seront tout de même constatés ;
- si le test est annoncé, l'entreprise peut en réduire l'impact et donc le coût.

D'autres incitent plutôt à privilégier la surprise :

- seul le test non annoncé permet de vérifier la bonne réactivité des employés ;
- le sinistre réel ne prévenant pas, le test sera lui aussi réalisé à l'improviste, par souci de réalisme ;
- la surprise empêchera que certaines personnes soient tentées de rectifier à l'avance des situations dommageables à la continuité, que l'on ne découvrira donc pas.

En conclusion, les tests réalisés à l'improviste ne sont recommandés que si l'entreprise possède une bonne maîtrise de son plan de continuité, acquise à la suite de tests annoncés. Toujours dans une démarche de progression, les premiers tests non annoncés se feront sur un périmètre limité et viseront essentiel-

lement à évaluer la réactivité des personnes sur les premières étapes du planning.

Document de préparation

Pour réussir l'exercice du test, il est important de bien le préparer. Le manque de préparation peut générer des doutes quant au sérieux du plan et décrédibiliser toute action ultérieure. En effet, la direction générale accorde à ces tests un temps et une attention qui n'est conséquente que si les résultats sont à la hauteur des attentes. Enfin, pour être crédible, il est nécessaire d'être réaliste et pragmatique.

On devra donc décrire ce que l'on attend concrètement du test dans un document qui couvre les points suivants :

- le dispositif humain et technique pour mener le test ;
- les points du plan de continuité à tester ;
- la date, le lieu et la durée du test ;
- les ressources nécessaires ;
- les actions à mener avant, pendant et après ;
- la méthode d'évaluation des points qui ressortiront à travers ce test ;
- le dispositif de surveillance et de compte rendu des événements et constatations.

Avant de développer le plan de test proprement dit, les points de ce document devront être approuvés préalablement par la direction des services concernés.

Contraintes des tests

Un test peut perturber le déroulement habituel des activités des employés. Avant de le mettre en application, il est donc judicieux d'en définir les limites de concert avec les opérationnels concernés. En effet, pour obtenir leur accord sur un calendrier annuel et les perturbations acceptables, il faudra les convaincre de l'utilité des tests en leur montrant qu'ils ont tout à y gagner. Concrètement, on validera avec eux un certain nombre de points :

- les répercussions acceptables sur le service ;
- les contraintes financières, le budget alloué et surtout ce que le test coûtera à ceux qui en seront les « victimes » ;
- les niveaux de sécurité à respecter : certaines dérogations sont-elles possibles ? dans quelles conditions ?
- les limites de temps et de coûts pour la mise à disposition de moyens de secours, de sites et d'employés ;
- la disponibilité du support technique fourni par les opérationnels en phase de préparation et d'exécution du test, puis lors de la remise en état normal ;
- la détermination de toute autre contrainte ou limite aux actions de test (par exemple : exécution uniquement le week-end ou la nuit, etc.).

Élaborer un plan de test

Pour chaque test programmé, un plan est établi afin d'en préciser formellement le cadrage et de prévoir le planning de son déroulement. Ce plan se déroule selon sept phases, devant chacune produire des résultats tangibles (livrables) :

1. revue des tests antérieurs ;
2. description des objectifs, périmètre et contraintes ;
3. définition de la tactique du test ;
4. mise en place de la logistique du test ;
5. planning et calendrier du test ;
6. revue des risques éventuels avant exécution ;
7. documentation du test.

Phase 1 – Revue des tests antérieurs

Lors de cette première phase, les rapports de tests déjà effectués sont passés en revue pour établir un bilan et capitaliser sur leurs résultats. Ceux-ci contiennent en effet des renseignements utiles, aussi bien au sujet des points du PCA qui posent problème que de ceux qui ont été testés avec succès.

Cela permet également de dresser la liste des points qui n'ont pas encore été testés, le but étant d'améliorer les points défaillants et d'évaluer ceux qui n'ont pas encore été testés.

> **Quand tout va bien, il faut le dire !**
>
> La société Dugroup a racheté la société DBC et fusionné leurs moyens informatiques. Avant la fusion, DBC testait son plan de reprise (PRA) sur un site éloigné.
>
> Après restructuration technique, Dugroup souhaite organiser une campagne de tests et analyse dans ce but les rapports des tests antérieurs menés par DBC. Ces derniers sont très succincts et ne décrivent pas avec suffisamment de précision l'existant technique. Difficile donc de déterminer les éléments qui restent valables dans la nouvelle configuration. Par ailleurs, les rapports font surtout état de problèmes de télécommunications qui ne sont plus pertinents dans la nouvelle structure.
>
> Dugroup ne peut quasiment rien déduire des rapports de tests de DBC et réalise de nouveaux tests, qui recouvrent fort probablement des actions déjà accomplies par DBC et que l'on aurait pu éviter si leurs résultats avaient été rapportés plus précisément.
>
> **Moralité** : il est fréquent de trouver dans les rapports de tests uniquement la liste de ce qui ne va pas... les points positifs étant éludés. Sachez que, afin d'optimiser les tests suivants, il est également important de les indiquer !

Bien entendu, il faut également intégrer dans la revue les éventuelles modifications subies par l'entreprise qui rendent caducs certains tests réalisés antérieurement ou certaines actions correctives.

Par ailleurs, les documents des tests antérieurs peuvent être réutilisés comme modèle pour les nouveaux tests.

À l'issue de cette phase, un document de revue des tests antérieurs doit être produit.

Phase 2 – Description des objectifs, périmètre et contraintes

Les objectifs, le périmètre et les contraintes du test sont définis lors de discussions en interne et doivent être rédigés de façon minutieuse. Ces éléments sont d'une importance capitale pour la réussite des phases qui suivent, et ne doivent jamais être perdus de vue tout au long de leur déroulement.

Objectifs

Il s'agit de décrire les objectifs que l'on souhaite atteindre en réalisant le test.

Il est préférable de classer ces objectifs par niveaux de priorité, en distinguant bien ce qui est urgent et indispensable (objectifs prioritaires) de ce qui serait simplement intéressant, et pouvant par conséquent être testé plus tard (objectifs secondaires). Un classement en deux ou trois niveaux suffit. En voici quelques exemples :

Objectifs prioritaires :

- déterminer si le PCA est à jour ;
- vérifier que les ressources prévues en secours sont convenables ;
- s'assurer que les procédures de restauration de données informatiques fonctionnent correctement ;
- recréer l'environnement informatique de secours sur le site distant et vérifier le temps nécessaire ;
- relocaliser un service sur un site de secours ;
- s'assurer que les premières étapes du PCA, en début de crise, se déroulent comme prévu ;
- vérifier la réactivité des prestataires impliqués dans le plan.

Objectifs secondaires :

- tester l'accès des utilisateurs sur un système de secours, une fois celui-ci mis en route ;
- vérifier l'ouverture du centre de gestion de crise (à la suite des premières étapes du plan) ;
- tester une application donnée sur un système de secours ;
- tester le retour à la normale.

Les objectifs dits secondaires seront testés si la charge de travail et le contexte le permettent.

> **Ne pas dévier de l'objectif !**
>
> La société Bontemps teste la capacité à relancer ses serveurs sur un site de secours. Elle possède des serveurs Unix, Windows et un mainframe IBM.

> Tout se passe bien pour le mainframe et les serveurs Windows. Pour les serveurs Unix, en revanche, elle constate qu'il manque certains droits de licence ou, plus exactement, qu'il faut demander une montée de niveau et des correctifs auprès d'un fournisseur.
>
> L'équipe en charge du test contacte alors directement ledit fournisseur. Celui-ci entre à son tour en relation avec le responsable des achats de Bontemps, qui lui n'est pas au courant de la situation. On en reste là, malgré la pression de l'équipe de test.
>
> **Moralité :** Il ne faut pas perdre de vue l'objectif du test ! Ici, il s'agissait de « vérifier » que l'on pouvait démarrer les serveurs et non pas de « démarrer les serveurs ». Le test aurait donc dû simplement produire le constat qu'il y avait un problème à résoudre pour les serveurs Unix et non entraîner sa résolution en catastrophe !
>
> Cela ne signifie pas pour autant qu'il faille automatiquement tout arrêter sur un constat d'impossibilité. Lorsqu'un document est absent, par exemple, on le note, mais si on sait où le trouver, on le cherche ! C'est une affaire de « bon dosage » à trouver.
>
> **N. B. :** Au passage, cet exemple montre que le responsable des achats peut lui aussi être impliqué dans les tests.

Périmètre

Définir le périmètre du plan de test consiste à délimiter le champ d'action du test. Celui-ci peut inclure :

- les portions du PCA que l'on souhaite vérifier(telles que les trois premières étapes du planning ou la formation des groupes, par exemple) ;
- les activités prévues par le planning sur un site donné ;
- tout ce qui doit se passer sur un ou plusieurs sites de l'entreprise ;
- certains partenaires externes et contrats de secours ;
- une technologie donnée (en particulier, si celle-ci coûte cher pour un niveau de secours qui reste à prouver) ;
- une action particulière du plan (par exemple : mettre en route le centre de gestion de crise).

Tout ce qui se trouve en dehors du champ d'action peut également être listé, afin que le personnel effectuant les tests connaisse exactement les limites de ses actions.

Pour une série de tests ayant le même objectif, le périmètre, lui, peut changer d'un test à l'autre. Par exemple, il peut être intéressant de tester les mêmes objectifs sur les différents sites de l'entreprise (y compris ceux à l'étranger) .

Contraintes

Cet aspect est très important pour la suite. Si les contraintes sont trop fortes, le test risque d'être difficile à mener. À l'inverse, une absence de contrainte peut être préjudiciable à l'entreprise. Voici les différents éléments à déterminer pour le test en prévision :

- l'enveloppe budgétaire affectée aux coûts des machines de secours, de déplacement, de locations diverses, de licence, etc. ;

- le niveau de perturbation entraîné sur l'entreprise : peut-on réellement arrêter telle machine ? combien de temps ? quand ?
- la sécurité : peut-on obtenir des dérogations ? faut-il prévoir des mesures supplémentaires ?
- les limites de charge prévues pour les spécialistes mis à disposition pour le test ;
- pour les locaux prévus en secours, d'éventuelles contraintes d'espace, de limites électriques, de charge de machine à ne pas dépasser ;
- les approximations nécessaires (utilisation d'un site en secours à la place du site principal, par exemple).

Ces contraintes déterminent souvent les points sur lesquels le test pourra être effectué en situation réelle ou si on devra se contenter de faire une simulation. C'est en effet le test qui doit être adapté aux contraintes posées et non l'inverse.

Phase 3 – Définition de la tactique de test

Maintenant que l'on sait précisément ce que l'on veut vérifier et dans quel cadre, il faut définir la tactique à observer pour parvenir au résultat attendu tout en restant dans les limites définies.

Scénario

La situation que l'on veut tester est décrite par écrit dans un document qui sera remis à l'équipe de test au début de l'exercice. La description doit être réaliste et crédible, elle ne doit pas révéler par avance ce que les testeurs sont supposés découvrir par eux-mêmes ou évaluer. Elle doit en revanche permettre de limiter la réaction au périmètre recherché.

Il peut être intéressant de prendre pour scénario certaines des catastrophes étudiées dans l'analyse de risque (voir le chapitre 1). Cela permet de se rapprocher au plus près d'une catastrophe réellement probable.

La narration doit présenter des faits, des dates et heures précises et des constats déjà réalisés. Voici quelques exemples :

> **Scénario n° 1 : Inondation du site CTI01**
>
> **Objectif** : valider les étapes 1, 2 et 3 du PCA.
>
> **Périmètre** : le site CTI01 et son site de secours.
>
> **Contrainte** : pas d'interruption d'activité.
>
> Document remis au chef de gestion de crise.
>
> « À cause de la crue du Loir, l'environnement du site CTI01 est inondé. À 1 h du matin, le 23 mars, le niveau d'eau atteint 30 cm, mesurés à l'entrée servant de référence. La surveillance de nuit du centre appliquant la procédure appelle le responsable de site qui vient de vous réveiller. »
>
> **Pour toute question** : contacter M. Test (numéro de téléphone).

Scénario n° 2 : Reprise de l'application SAT02 sur le site d'Angers

Objectif : valider la viabilité du contrat avec la société CPPB.

Périmètre : l'application SAT02, le site de Vanves et son site de secours.

Contrainte : pas d'interruption d'activité.

Document remis au responsable de récupération des moyens techniques.

« À cause d'un problème grave sur le site principal de Vanves, il a été décidé d'arrêter certaines des applications en fonctionnement sur ce site. Le 15 mars à 9 h, il est décidé d'activer la version de secours de l'application SAT02 sur le site d'Angers, comme prévu dans la convention de secours signée avec le CPPB. Il n'est pas possible de se rendre sur le site de Vanves. Le chef de gestion de crise vous transmet ce message. »

Pour toute question : contacter M. Test (numéro de téléphone).

Exceptés les cas où l'on veut simuler un tout début de sinistre et évaluer la manière dont les dommages sont découverts, le scénario doit décrire les dommages subis par l'entreprise lors du sinistre. Tout doit être présenté de manière à donner un niveau d'information correspondant à celui obtenu en situation réelle au moment que l'on veut tester.

C'est à partir du problème ainsi posé que le destinataire du message devra enclencher les mesures prévues dans le plan au sein du cadre indiqué.

Choix de la méthode

Les différentes méthodes de test pratiquées ont été présentées dans la première section de ce chapitre. Au cours de l'élaboration de la tactique de test, on détermine à quelle méthode on recourt en fonction du scénario prévu.

Dans le cas du scénario n° 2 ci-dessus, le « test parallèle » pourra se révéler pertinent. Pour le scénario n° 1, induisant des conséquences plus lourdes si on le mène à fond, on préfèrera une revue de documents (*walk-through*) ou une simulation.

Date du test

La date et la durée du test seront fixées en fonction des disponibilités et des diverses contraintes, tout en tenant compte des possibilités d'exercice des partenaires locaux ou contractuels. Le planning des tests doit être considéré comme un engagement fort, à respecter absolument.

Une erreur courante consiste à prolonger les tests rencontrant des difficultés. Cette pratique est à éviter, l'objectif du test étant de mettre à jour la difficulté, pas de la résoudre. Il faut donc bien séparer les deux préoccupations : le test doit relever des difficultés, des anomalies ; le temps de leur résolution viendra plus tard. On ne doit pas rester « bloqué » sur un problème, mais le noter et passer outre. C'est pour cette raison que les tests effectués en première instance sont de type *check-list*, *walk-through* ou simulation, car on rencontre, à ce stade, trop de problèmes pour pouvoir dérouler l'ensemble d'un scénario en mode réel.

La résolution des difficultés découvertes se fera par des plans d'actions correctives qui seront décidés puis réalisés par la suite. Les progrès réalisés seront mesurés lors de la campagne de test suivante.

Suivi et évaluation du test

C'est un aspect essentiel : le coût de la campagne de test étant élevé, celle-ci doit se révéler productive et permettre de tirer le maximum d'enseignements.

Suivi des tests

Consistant à collecter toutes les informations significatives sur le déroulement du test, le suivi pourra être effectué par une assistance externe qui notera tout ce qui se passe en apportant un regard critique. Toutes les constatations doivent être consignées, en réalisant des fiches de test du type de celle présentée en exemple ci-après :

Tableau 6-1 : Exemple de fiche de test à compléter

Fiche de test N°5/23-1 **Objectif** : Vérifier l'adéquation de la configuration de reprise de l'application A3		
Test	**Qui ?**	**Constats**
1-1 : Se procurer la configuration de l'application A3	– le testeur – le responsable d'application (RA)	
1-2 : Vérifier la configuration A3 de secours	– le testeur – le gestionnaire de la société SecoursCo	
2-1 : Identifier les moyens techniques du secours A3	– le testeur – le gestionnaire de SecoursCo	
2-2 : Mettre en marche le secours A3 dans les délais prévus	– le testeur – le support de SecoursCo	
3-1 : Se procurer les sauvegardes A3	– le testeur – la logistique	
3-2 : Restaurer les sauvegardes A3	– le testeur – le support de SecoursCo	
4-1 : Tester un utilisateur	– le testeur	

Outre les événements constatés, ces fiches peuvent également mentionner les éventuelles actions correctives détaillées sur des fiches prévues à cette effet. Cela servira à la rédaction du bilan des tests.

En cas de difficulté à résoudre ou de décision à prendre, on procédera peu ou prou comme lors d'un sinistre réel, avec un dispositif un peu plus léger. Un coordonnateur des tests sera désigné et joignable en permanence pour cela.

Critères d'évaluation

Mieux vaut préciser à l'avance les critères qui vont être utilisés pour évaluer les tests. Les campagnes de tests peuvent en effet être ciblées sur une problématique particulière. Parmi les critères récurrents figurent notamment :

- l'existence ou non de documents importants tels que les analyses de risques, d'impact sur l'activité ou de stratégie de continuité, les définitions de responsabilités, ou encore le planning de continuité ;
- la validité de ces documents : sont-ils actualisés ? par qui ? de quelle manière ?
- l'existence et l'actualisation des inventaires d'actifs ou des configurations sur lesquelles se basent les travaux de reprises ;
- l'existence et l'actualisation des listes de personnel, avec indication du pourcentage d'erreurs, l'indication de suppléants, etc. ;
- le degré de pertinence des contrats en cours concernant les services de secours, de sauvegarde ou de dépannage ;
- l'adéquation des documents décrivant le plan de continuité ;
- la dimension praticable des plannings, des locaux, des choix techniques qui sont faits dans le plan.

Ces critères doivent devenir des préoccupations permanentes et être indiqués de manière à détecter lors de chaque test les manquements dans ces domaines, au-delà de ce que le test en lui-même est supposé vérifier.

Suivi des dépenses du test

En termes de gouvernance de la continuité, il est nécessaire de suivre avec attention les dépenses engendrées par les tests. Il faut donc en conserver la trace et vérifier le respect d'un budget prévisionnel. Les rubriques principales du budget seront :

- les coûts des jours-homme en interne consacrés aux tests ;
- les coûts des jours-homme de prestataires externes ;
- les coûts facturés par les sociétés de services de secours, de transports, de logistique ;
- les coûts des éventuelles machines, serveurs, stockage et réseau mis à disposition durant les tests et souvent facturés à l'usage ;
- les frais de transports, hôtel, repas et menues dépenses provoquées par les déplacements sur des sites de secours, par exemple.

Les tests de type revue ou simulation sont nettement moins onéreux que les tests grandeur nature. En général, on y allouera un budget annuel. Il faut alors

décider comment, dans le cadre de ce budget, les différents tests vont pouvoir être planifiés.

Les plans d'actions correctives menés après les tests sont en général comptés dans un budget différent, souvent porté par les opérationnels concernés.

Phase 4 – Mise en place de la logistique de test

Les tests nécessitent une préparation tant des employés que des sites et des différents moyens matériels nécessaires. Une logistique doit donc être prévue pour couvrir à la fois les besoins en personnel (constitution des équipes, déplacements, etc.) et en moyens techniques divers nécessaires pour le test. Le personnel habituel de l'entreprise devra lui aussi subir une préparation , de même que les sites qui vont être concernés – et donc perturbés – par les tests.

Équipe en charge des tests

L'équipe de professionnels qui va piloter les tests est aussi chargée de les préparer. Sa constitution, puisant dans les différents groupes décrits dans le chapitre 4, dépend grandement de la nature, du périmètre et du type de test réalisé.

À l'inverse de la pratique en audit qui recourt à des intervenants externes, il est souhaitable de faire réaliser les tests par ceux-là même qui mèneront les actions testées en cas de sinistre. Cela vaut également pour les groupes responsables des différentes missions. Le test vaut exercice.

Au sein de cette équipe de testeurs, on pourra également trouver :

- des prestataires externes de sociétés de secours ;
- des auditeurs qui peuvent ainsi suivre les tests, les évaluer et proposer des améliorations ;
- des clients souhaitant valider la solidité du plan de leur fournisseur et y participer ;
- des spécialistes techniques dans certains domaines pointus.

Une fois l'équipe constituée, elle est autonome et doit se suffire à elle-même.

Moyens techniques

D'autre part, il faut préparer les moyens techniques utilisés durant les tests. Cela peut se limiter à une salle de travail équipée en PC pour un test de type *walk-through* (revue de documents), mais cela peut devenir beaucoup plus lourd en cas de test en conditions réelles. Dans ces derniers cas, le groupe de gestion de crise est mis à contribution pour l'approvisionnement en moyens de secours, qui fait partie de ses missions décrites dans le chapitre 4.

À moins que la préparation ne soit elle-même partie intégrante du test, tout ou partie des moyens suivants devront en effet être prêts pour le test :

- l'infrastructure destinée au personnel testeur (PC, téléphone, bureau, télécopieurs, copieurs, etc.) ;

- le matériel nécessaire aux tests (lecteurs de bandes et cartouches, serveurs, stockage, télécommunications) avec les logiciels mis à jour et droits de licence adaptés ;
- les réservations chez les prestataires ayant eux-mêmes prévus des tests en commun avec l'entreprise, ou chez les clients éventuellement impliqués ;
- toutes les réservations nécessaires de spécialistes en support technique en interne comme en externe ;
- la documentation des tests, les formulaires et procédures dégradées devant être disponibles sur place ;
- le site de gestion de crise, qui, s'il est utilisé, doit être prêt pour être activé ;
- enfin, les fiches de test à communiquer.

La préparation logistique en elle-même peut avoir été l'objet du test précédent ou de plusieurs tests antérieurs. Dans ce cas, la préparation avant test s'arrête là où le test commence, et ne porte pas sur les points qui seront précisément testés. Cela permet de tester petit à petit l'ensemble du plan de continuité.

Intendance et déplacements

Les tests nécessitent la présence de personnel de test sur des sites distants, chez des prestataires ou sur un site de gestion de crise lointain. Il faut alors prévoir toute l'intendance liée à ces déplacements, notamment :

- prévoir qui devra se déplacer et où, arranger les déplacements, réserver les hôtels, etc. ;
- demander les autorisations d'accès et les divers droits nécessaires ;
- réserver les créneaux de présence chez les prestataires, qui peuvent être limités par contrat.

Sites de test

De la même manière, les sites doivent avoir été préparés en fonction des points que l'on veut tester. On procède donc en trois temps :

1. faire la liste de ce qui est attendu du site de secours : dates de disponibilité, matériel présent, logiciels et niveaux de mises à jour, documentation, support technique, infrastructure particulière, etc. ;
2. constater ce que le site fournit sur ces points ;
3. déterminer l'écart à combler.

Il est bon de visiter le site à l'avance afin de constater sur place les différents problèmes potentiels. Si ce site est fourni par un prestataire, cette visite devra être rendue possible par le contrat.

Souvent les contrats de prestations imposent des dates ou des périodes assez restreintes pour effectuer les tests. De plus, le recours à des spécialistes est souvent assez limité et facturé à part par le prestataire. Il arrive enfin que certains prestataires soient très exigeants sur le respect de configurations précises ou de

normes de sécurité plus élevées que celles que l'entreprise pratique en interne. Ces points sont donc à étudier au plus près avant de lancer les tests.

Phase 5 – Planning et calendrier

Cette phase du plan de test est essentielle, et, plus grand sera le soin apporté à sa réalisation, plus les risques de dépassement de délai et de budget seront réduits. Concrètement, planifier la campagne de tests consiste à décrire les activités et les tâches à effectuer, les affecter aux personnes adéquates et prévoir leur date et durée de réalisation.

Pour arriver à cet objectif, on procède généralement en plusieurs étapes :

1. prendre en compte l'ensemble du contexte des tests (cadrage des objectifs, du périmètre et des contraintes ; prise en considération de la tactique et des objectifs) ;
2. sélectionner dans le plan de continuité les missions et activités à effectuer (voir les chapitres 4 et 5), en les aménageant pour le test ;
3. affecter les activités aux employés, en leur donnant une charge (temps passé, jours-homme) et des dates ;
4. réaliser des fiches de tests à remplir par les testeurs ;
5. décrire le dispositif de suivi du test par des observateurs qui assurent le respect du cadrage et la réalisation des objectifs.

Plus l'entreprise a l'expérience des tests, plus cette phase sera détaillée et, en tout cas, fiable. Par ailleurs, il est intéressant de récupérer d'un test à l'autre ce qui a été produit lors de cette phase.

Phase 6 – Revue des risques du test

L'objectif principal du plan de test est de réduire les risques entraînés par les tests eux-mêmes. Il est alors judicieux de réunir certains des responsables de l'entreprise afin de faire un dernier bilan des risques et des différents paramètres des tests avant leur exécution.

Ce bilan consiste à répondre aux questions suivantes :

- Les objectifs des tests sont-ils corrects et bien présents dans les tests prévus ?
- Le périmètre convient-il aux exigences des opérationnels et des responsables de la continuité d'activité ?
- Les contraintes sont-elles correctement formulées et respectées par le plan de test ?
- Les scénarios, méthodes et le suivi sont-ils bien adaptés au test que l'on veut réaliser ?
- La logistique et le planning ont-ils été suffisamment préparés ou demandent-ils encore des améliorations ?
- Le suivi permet-il une remontée efficace des informations et des constats ?

- La préparation du personnel a-t-elle été suffisante ?
- Le degré d'implication des fournisseurs est-il correct ?
- Le niveau d'information des clients est-il convenable ?

Si l'idéal serait d'obtenir une réponse positive à chacune de ces questions, il n'est pas rare que certaines des réponses soient encore négatives lors de ce bilan, nécessitant assez souvent des actions correctives complémentaires telles que :

- des réductions de périmètre ou de durée des tests ;
- des visites de sites ou de fournisseurs permettant de préciser certains points ;
- l'amélioration de la communication auprès du personnel ou des clients les avertissant des tests à venir ;
- une révision des plannings et des charges ;
- le recours à un prestataire pour le suivi des tests.

Au final, les responsables doivent aboutir à un accord acceptable afin de donner le feu vert à l'exécution du test.

Phase 7 – Documentation du plan

Le plan de test se matérialise par un document qui reprend le contenu de toutes les étapes précédentes.

Voici un exemple de structure d'un plan pour une campagne de tests.

Plan de test

N° d'identification, Version, Responsable, Validation

1. Bilan des tests antérieurs
2. Cadrage des tests
   - 2.1. Objectif de la campagne de tests
   - 2.2. Périmètre concerné
   - 2.3. Contraintes à respecter
3. Tactique de test
   - 3.1. Scénario
   - 3.2. Méthode
   - 3.3. Suivi et évaluations
   - 3.4. Coordination
4. Logistique des tests
   - 4.1. Équipes
   - 4.2. Moyens techniques
   - 4.3. Sites concernés
5. Planning des tests
   - 5.1. Activités chiffrées

5.2. Affectation des équipes
5.3. Fiches de tests
6. Revue des risques
6.1. Bilan des risques (questions/réponses)
6.2. Actions de réduction des risques

Exécuter les tests

Une fois le plan de test complet et la revue des risques ayant donné le feu vert, la réalisation des tests peut avoir lieu selon le plan prévu.

Rôle et action des testeurs

La campagne de test est lancée et l'équipe de testeurs en est informée Tout testeur doit avoir préalablement pris connaissance du scénario de tests, afin de s'y conformer au plus près.

Pour réaliser les tests, le testeur doit avoir accès à deux types de documents :

- le planning contenant les activités dont il a la charge ;
- les fiches de test qu'il doit remplir.

Malheureusement, dans le domaine de la continuité d'activité, il est rare que tout se passe comme prévu. En cas de doute ou de décision imprévue à prendre face aux événements, le testeur doit avoir le réflexe de se tourner vers le coordonnateur des tests. Ce dernier garde en effet la trace de toute demande remontée jusqu'à lui et de toute indication donnée.

Consignation des constatations

Produire des informations à partir des constatations des tests est la raison d'être de la campagne de tests.

Les fiches de test sont remplies et collectées, de préférence sur le moment plutôt que quinze jours après les événements. Bien des fiches étant remplies à la main et de manière incomplète, un travail de collecte et de mise en forme est indispensable. Il doit y figurer les points particuliers que l'on cherche à vérifier, mais aussi toute autre constatation utile au plan de continuité.

Le tableau 6-2 donne un exemple de ce à quoi peut ressembler la fiche de tests précédente, une fois remplie.

Les actions décrites dans cette fiche sont extraites d'opérations qui visaient à tester la restauration d'un applicatif sur un site de secours géré par un prestataire. Il aurait été possible aussi d'y noter les durées ou les charges constatées pour la réalisation des ces activités. Ces informations sont en effet très utiles pour vérifier la faisabilité d'ensemble.

Tableau 6-2 : Exemple de fiche de test complétée

Fiche de Test N°5/23-1 **Objectif :** Vérifier l'adéquation de la configuration de reprise de l'application A3		
Test	**Qui ?**	**Constats**
1-1 : Se procurer la configuration de l'application A3	– le testeur – le responsable d'application (RA)	La configuration pour A3 existe. Le RA la trouve inexacte. Le RA la met à jour : 2 jours-homme.
1-2 : Vérifier la configuration A3 de secours	– le testeur – le gestionnaire de SecoursCo	La configuration de secours pour A3 n'existe pas. Il existe une configuration pour A2 (ancienne version d'A3).
2-1 : Identifier les moyens techniques du secours A3	– le testeur – le gestionnaire de SecoursCo	Les moyens techniques pour A2 sont identifiés mais le serveur X n'est pas disponible
2-2 : Mettre en marche le secours A3 dans les délais prévus	– le testeur – le support de SecoursCo	Seule une partie des moyens pour A2 peut démarrer (en 4 heures). Les moyens A3 ne peuvent être mis à disposition dans les délais.
3-1 : Se procurer les sauvegardes A3	– le testeur – la logistique	La logistique ne sait pas où se situent les sauvegardes A3. Seules les sauvegardes A2 sont trouvées et apportées sur le site.
3-2 : Restaurer les sauvegardes A3	– le testeur – le support de SecoursCo	Échec.
4-1 : Tester un utilisateur	– le testeur	Échec.

Remarque

On remarque dans l'exemple cité que le testeur est allé au bout des possibilités en prenant deux décisions : ne possèdant pas la bonne configuration, il a néanmoins essayé de voir si le prestataire externe de secours pouvait proposer l'ancienne (décision 1). Ayant là aussi découvert une anomalie, il a alors arrêté le déroulement des tests (décision 2). Ce test a donc été productif de résultat.

Bilan des tests

Pour un ensemble de tests donné, un bilan peut être réalisé à partir des diverses sources d'informations utiles disponibles :

- les fiches de test remplies ;
- la main courante du coordonnateur ;
- les comptes rendus des réunions de débriefing.

Ce bilan peut prendre la forme suivante et son plan peut d'ailleurs fort bien être repris pour constituer l'ordre du jour des réunions de débriefing.

Bilan de la campagne de tests 02-08/2

1. Rappel du plan de test (voir la section précédente)
2. Objectifs des tests
   - 2.1. Objectifs atteints
   - 2.2. Objectifs non atteints
   - 2.3. Causes de l'échec
3. Tâches de test
   - 3.1. Tâches réalisées
   - 3.2. Tâches non réalisées
   - 3.3. Causes de l'échec
4. Défauts détectés dans le PCA
   - 4.1. Maîtrise des risques
   - 4.2. Analyse d'impact sur les activités
   - 4.3. Stratégie de continuité
   - 4.4. Missions et responsabilités
   - 4.5. Planning des activités
   - 4.6. Tests
   - 4.7. Gestion des changements
5. Problèmes détectés
   - 5.1. Concernant les tests
   - 5.2. Concernant le PCA
6. Propositions d'amélioration
   - 6.1. Pour les tests à venir
   - 6.2. Pour le PCA
7. Plan d'action pour l'amélioration
8. Bilan général des tests (coût, durée, charge)

Suivi des actions d'amélioration

Les actions d'amélioration proposées doivent faire l'objet d'une validation et d'un suivi. En effet, elles impliquent généralement des coûts de projet et

d'investissement divers nécessitant de les intégrer dans un budget. Le suivi de ces actions tout au long de l'année est réalisé spécifiquement par la Direction de la continuité d'activité, à qui incombe la responsabilité de leur bonne fin.

La prochaine campagne de tests pourra en partie vérifier, si cela est pertinent, la bonne réalisation des actions décidées. Si cette campagne est effectuée avant la mise en place de ces actions, tombant sur les mêmes défauts, elle notera qu'ils sont en cours de suppression.

PARTIE III

L'ingénierie de la continuité

La technologie peut fournir un concours appréciable pour rendre l'entreprise plus résiliente. Encore faut-il évaluer son apport réel dans la situation particulière de chaque entreprise. C'est ainsi le rôle de l'ingénierie de rendre ce qui est théoriquement possible concrètement réalisable.

Cette partie aborde la mise en œuvre pratique des diverses technologies proposées sur le marché et utilisées en partie par les entreprises. Elle se structure en quatre chapitres :

- Le chapitre 7 présente les notions de fiabilité, de disponibilité et d'architecture technique utiles pour la suite.
- Le chapitre 8, consacré à l'informatique au centre de données, traite de la disponibilité des serveurs, du stockage et des réseaux du centre informatique qui sont au cœur de l'activité de l'entreprise.
- Le chapitre 9 traite de l'infrastructure et du poste de travail, abordant ainsi l'environnement direct de l'employé dans son bureau, avec son ordinateur personnel et son environnement bureautique.
- Enfin, le chapitre 10 traite de la spécificité du centre informatique proprement dit, afin que celui-ci constitue un point fort du dispositif.

Le schéma ci-après décrit la logique d'ensemble.

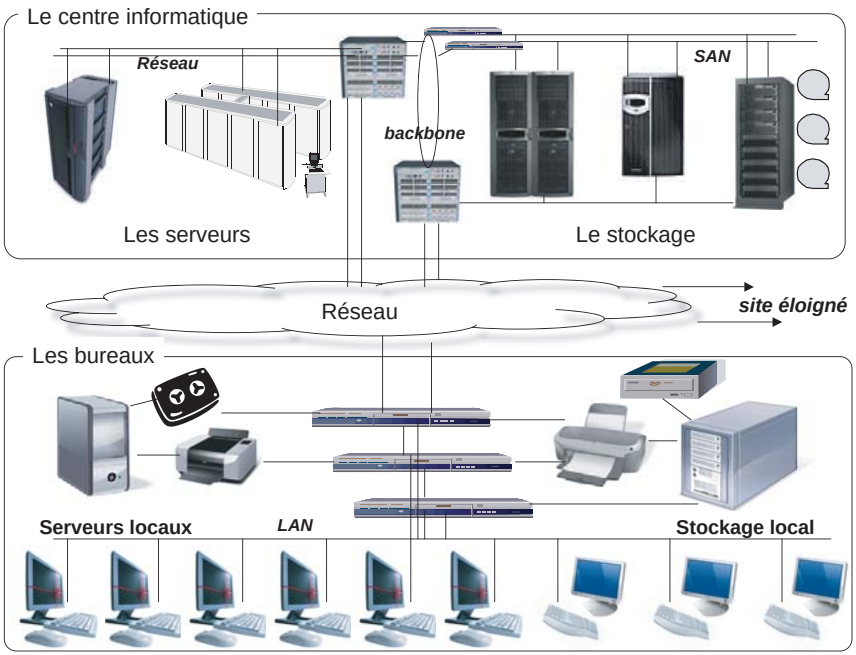


Schéma général des moyens informatiques

Chapitre 7

Construire la disponibilité

La continuité d'activité est une affaire d'organisation, de planification et de technologie. La manière dont la technologie est utilisée a des conséquences souvent négligées sur la disponibilité des moyens et donc sur la continuité des activités qui y recourent.

Ce chapitre décrit les notions de base de la disponibilité et présente des modes d'utilisation permettant l'amélioration de la continuité d'activité. Il donne des recommandations pour le choix des architectures, la mise en œuvre et les précautions à prendre pour que l'usage des technologies soit bénéfique en termes de continuité.

Notions statistiques

Les probabilités et les statistiques sont utiles pour décrire le comportement des matériels divers, qui peuvent tomber en panne et ainsi détériorer la continuité d'activité. Les notions de fiabilité, de disponibilité et de maintenabilité sont donc importantes pour sélectionner les configurations matérielles et logicielles les mieux adaptées aux besoins de continuité de l'entreprise.

Disponibilité

La disponibilité d'une machine indique la proportion du temps pendant lequel cette machine fonctionne comme prévu. Elle est souvent donnée par un pourcentage, qui doit être évidemment le plus proche possible de 100 %, le reste étant appelé l'indisponibilité.

Il est d'usage, en matière de disponibilité, de compter les « 9 » et de classer selon leur nombre. On parle couramment de disponibilité allant jusqu'à 99,999 %, qualifiée de *five nines* en anglais ou « cinq neufs ». Ce chiffre 5 est devenu en quelque sorte un idéal à atteindre. À quoi cela correspond-il dans la réalité ?

Le tableau suivant donne les temps d'arrêts maximaux à ne pas dépasser pour respecter, sur une année, les disponibilités indiquées, sachant que la machine en question doit fonctionner vingt-quatre heures sur vingt-quatre.

Tableau 7-1 : Disponibilité et temps d'arrêt maximaux

Classe de 9	Disponibilité	Temps d'arrêt maximum par an
2	99 %	87 heures et 36 minutes
3	99,9 %	8 heures et 46 minutes
4	99,99 %	52 minutes
5	99,999 %	5 minutes et 12 secondes
6	99,9999 %	31 secondes

Cela signifie que si notre machine respecte dans son cahier des charges une disponibilité « à cinq neufs », elle ne pourra pas cumuler plus de 5 minutes et 12 secondes de panne ou d'arrêt dans l'année.

Cependant le problème est que, en cas d'arrêt de cette machine, cela demanderait beaucoup plus de cinq minutes pour la remettre en marche ou la remplacer par une autre équivalente. Il faut donc analyser la disponibilité sous ses deux constituants : la panne et la facilité de réparation.

Enfin, autre aspect important, la disponibilité est souvent mesurée dans les conventions de service à la fois par année pleine, comme ci-dessus, et en moyenne annuelle sur cinq ans, par exemple. Si l'on reprend le tableau précédent, une machine disponible à 99,999 % sur cinq ans peut se permettre une panne de 26 minutes consécutives en une seule fois sur ces cinq ans. En revanche, l'année de la panne, elle ne satisfait pas au critère des cinq neufs dans l'année. Les chiffres sont donc à interpréter avec précision.

Fiabilité et réparabilité

La fiabilité mesure la propension à ne pas tomber en panne. La réparabilité mesure la facilité à réparer et donc à remettre en marche. Ces deux notions vont de pair pour indiquer la disponibilité.

Entre deux pannes consécutives, il s'écoule un certain temps, la moyenne de ces temps constatés sur une longue période est nommée « moyenne des temps de bon fonctionnement » (MTBF). Plus la MTBF est élevée, plus la machine est fiable.

Le temps passé à réparer est variable, une moyenne peut être calculée : la « moyenne des temps des travaux de réparation » (MTTR). Plus la MTTR est faible, plus la machine est réparable rapidement. La notion de réparation est à

prendre au sens large : il peut s'agir tout aussi bien d'un remplacement pur et simple.

En général, la MTBF se mesure en dizaines, voire centaines de milliers d'heures, alors que la MTTR se compte tout au plus en jours.

La MTBF est une donnée attachée à une machine, à un fabricant, et l'exploitant ne peut pas y changer grand chose. La MTTR, en revanche, lorsqu'elle porte sur du matériel standard, dépend beaucoup de l'organisation de l'entreprise. Il est en effet possible de prévoir des pièces de rechange ou une machine de secours, de manière à réduire ce délai au minimum.

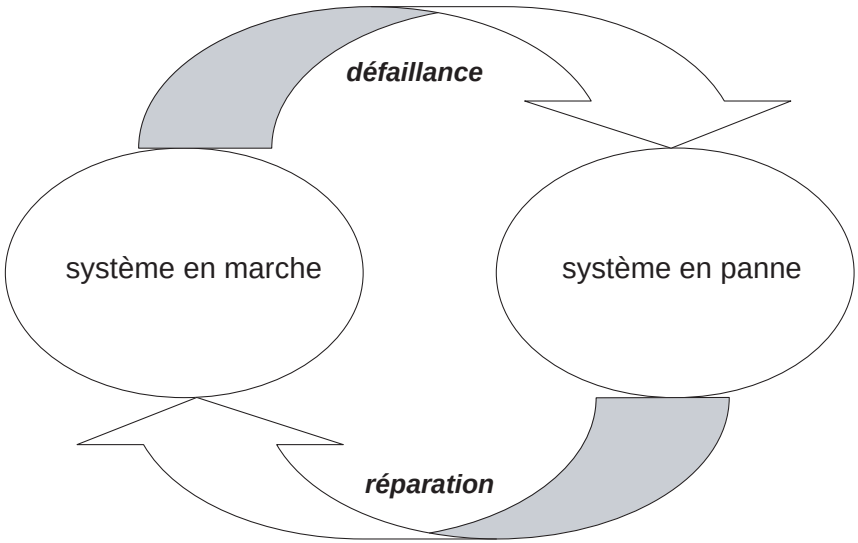


Figure 7-1 : Défaillance et réparation

On appelle *taux de défaillance* l'inverse de la MTBF et *taux de réparation* l'inverse de la MTTR.

Les statisticiens nous donnent les formules suivantes :

Indisponibilité = I = MTTR / (MTBF+MTTR)

Disponibilité = D = MTBF / (MTBF+MTTR)

Les disponibilités d'une machine en fonction de ses MTBF et MTTR peuvent être données par un tableau du type suivant.

Tableau 7-0 : Disponibilité en fonction des MTBF et MTTR

MTBF	si MTTR = 12 h	si MTTR = 1 h
10 000 h	99,88 %	99,99 %
20 000 h	99,94 %	99,995 %
100 000 h	99,988 %	99,999 %
200 000 h	99,994 %	99,9995 %
500 000 h	99,998 %	99,9998 %

Gardant à l'esprit la cible des cinq neufs, la lecture de ce tableau est instructive, car elle démontre que :

- Si l'on ne peut pas réparer la panne en moins de douze heures, alors il n'y a aucun moyen d'obtenir les cinq neufs visés. Cela ne sert à rien d'acquérir du matériel haut de gamme à haute fiabilité (MTBF élevée).
- Si l'on peut réparer en une heure, alors un matériel dans le milieu de tableau (avec une MTBF de 100 000 heures) pourra obtenir la disponibilité des cinq neufs.
- Si quatre neufs suffisent, alors un matériel ayant une MTBF de 10 000 heures suffira si l'on sait assurer une réparation en une heure.

Le prix du matériel dépend beaucoup de la MTBF : plus celle-ci est élevée, plus le matériel est cher. Le tableau ci-dessus étant donné à titre d'illustration, il est rare qu'un même matériel ait des taux de fiabilité aussi différents. En réalité, à disponibilité égale, il est nécessaire de faire un choix entre deux scénarios extrêmes pour l'achat de matériel, informatique ou non. Ces scénarios peuvent être typés ainsi :

1. acheter une machine plutôt bon marché, qui tombera en panne assez souvent (une fois par an ?) mais que l'on saura réparer vite (en moins d'une heure), parce que l'on aura prévu des pièces de rechange, par exemple – la fréquence régulière de la panne fait d'ailleurs que l'on sait, à force, bien la réparer ;
2. acheter une machine onéreuse, à haute disponibilité, qui ne tombera en panne que très rarement (une fois tous les sept ans ?) – peut-être ne saura-t-on pas la réparer, mais statistiquement, la machine sera remplacée avant que la panne n'arrive ; il est rare en effet qu'un matériel soit conservé plus de cinq ans.

Au final, le choix se fixera toujours sur une option se situant entre ces deux extrêmes.

> **Attention : Ne pas tout miser sur la fiabilité aux dépens de la réparabilité !**
>
> La tendance naturelle, malheureusement, est de chercher avant tout la fiabilité au prix fort et de négliger la réparabilité. Il se révèle pourtant très utile d'étudier les possibilités

en cas de panne de la machine : prévoir des pièces de rechange, voire une machine de secours, permet en effet d'améliorer très fortement la disponibilité, sans pour autant grever les coûts.

Les modèles redondants

Un modèle redondant permet d'améliorer la disponibilité en multipliant tous ses éléments vitaux par deux. Ainsi, il faudra subir deux pannes au lieu d'une pour rendre le modèle redondant indisponible, la deuxième panne survenant alors que la première n'a pas encore été réparée. Ce modèle est dit « à tolérance de panne ».

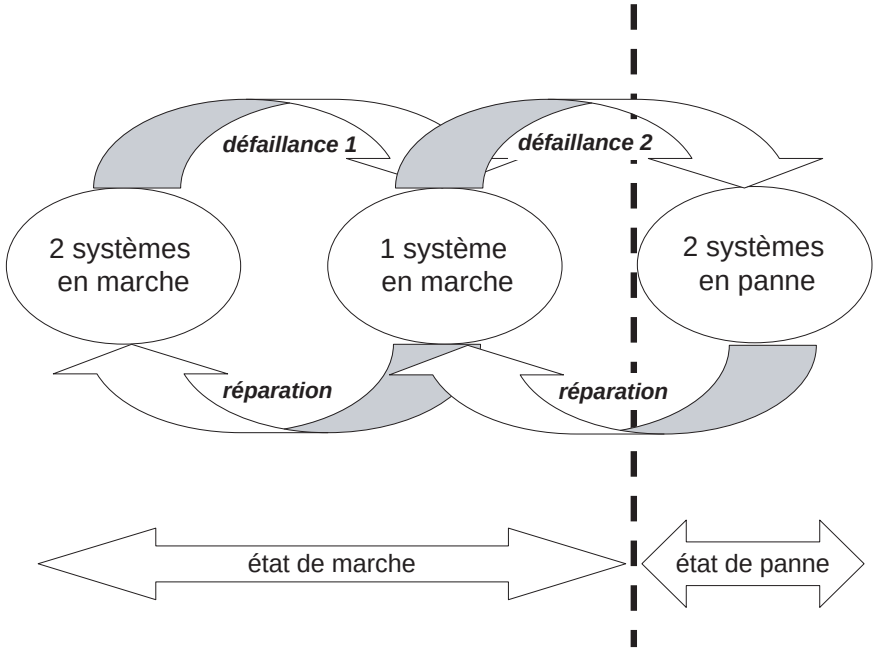


Figure 7-2 : Le modèle redondant

L'indisponibilité résultante étant le produit des indisponibilités de chaque machine, elle est ainsi beaucoup plus faible. Un ensemble de deux éléments « à deux neufs », par exemple, devient « à quatre neufs ». La disponibilité est donc plus forte, mais le coût a lui aussi doublé ou presque. En outre, si la panne arrive malgré tout, alors plus rien ne marche.

De plus, dans le cas de serveurs informatiques, il est nécessaire de s'assurer que les données sont accessibles par les deux machines et que les utilisateurs peu-

vent être reconnectés de l'une à l'autre. Cela suppose de partager l'accès aux données entre les deux machines et de prévoir également en double les connexions. Il faut donc ici considérer aussi le problème de la défaillance du stockage des données et de l'indisponibilité du réseau (voir le chapitre 8).

Ce modèle possède plusieurs variantes, en fonction de l'utilisation des deux machines : une machine peut être libre pendant que l'autre travaille ou la charge peut être répartie sur les deux en parallèle. Dans ce dernier cas, il faudra alors tenir compte de la fiabilité de l'élément répartiteur.

L'inconvénient principal des modèles redondants réside donc dans le fait que chaque fois qu'on introduit un élément de solution, on introduit par la même occasion une nouvelle source de panne possible.

Le modèle n+1

Dans le modèle dit *n*+1, la charge de travail est répartie sur *n* machines. Une machine supplémentaire est mise à part, à l'arrêt ou en veilleuse. Cette machine inactive est destinée à remplacer la machine défectueuse en cas de panne, après un délai d'activation plus ou moins long. Lorsqu'il s'agit de serveurs informatiques, on parle souvent de *cluster* ou « grappe » n+1.

Il en résulte que, pour que l'ensemble tombe en panne, il faut que deux machines au moins tombent en panne parmi le nombre *n*. L'indisponibilité conséquente peut donc se calculer ainsi :

Indisponibilité résultante = n x (n-1) x I^2

Remarquons que si l'on fait cet exercice avec, par exemple, dix machines de classe 2, on ne gagne quasiment rien en disponibilité (99,1 % au lieu de 99 %) !

En revanche, le bénéfice de ce modèle réside dans la *conséquence* de la panne, qui est fortement minimisée : au lieu de tout perdre, on ne perd qu'un dixième des machines, et donc un dixième de la capacité de traitement. Le risque est donc diminué à proportion. C'est pour cette raison que les opérateurs de type fournisseurs d'accès à Internet, par exemple, répartissent leurs traitements sur une grande quantité de serveurs moyennement fiables. Ils obtiennent ainsi souvent des pannes aux effets marginaux, qu'ils savent réparer rapidement.

Avec dix machines de classe 3, on obtient un ensemble de classe 4. Là encore, l'effet de la panne est de perdre un dixième de la capacité de traitement. Enfin, en termes de coût, les machines nécessaires pour réaliser ces grappes sont moins puissantes et donc moins onéreuses. Même s'il faut en acheter un nombre plus important, le coût total reste inférieur.

Prise en compte de la panne de mode commun

Les analyses précédentes ne doivent pas pour autant négliger la panne dite de mode commun. En effet, ce type de panne est transverse au problème considéré. Lorsqu'on étudie par exemple des serveurs de constructeurs différents mais

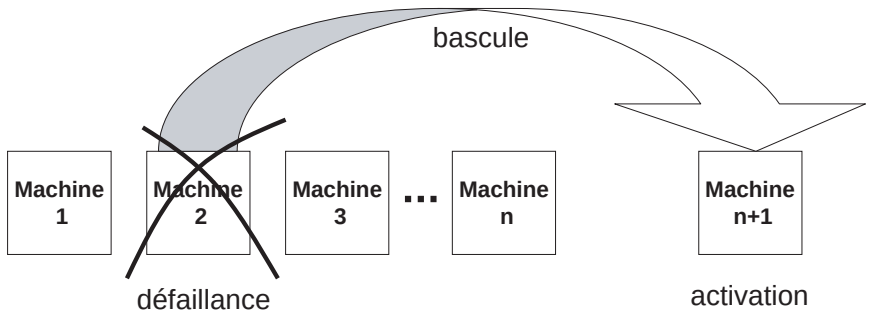


Figure 7-3 : Le modèle n+1

fonctionnant avec des ventilateurs de même modèle et du même fournisseur, alors la panne de ventilateur aura des caractéristiques communes à tous.

Par extension, la panne de mode commun est celle qui s'impose à tous et qui évite de calculer trop loin… Lorsqu'on étudie la fiabilité d'un ensemble de serveurs, ce sera par exemple la panne d'électricité. On aura beau réduire les indisponibilités des serveurs par diverses approches, il arrive un moment où une autre panne, non prise en compte auparavant car trop peu probable, s'impose désormais comme la plus grave. Il ne sert à rien, en effet, d'arriver à une disponibilité de classe 4 avec des serveurs si leur alimentation électrique est toujours en classe 3, par exemple.

L'analyse des risques doit donc absolument rechercher ce type de panne générale, permettant de savoir où porter réellement ses efforts. De plus, si c'est cette panne que l'on doit subir, cela permet de ne pas trop pousser la recherche de disponibilité du reste.

Les exemples de panne de mode commun ne manquent pas :

- pannes de fournitures et d'alimentation électriques sur toute la chaîne de distribution ;
- bogues dans un logiciel : un bogue dans une application sur un serveur se retrouvera sur le serveur de secours ;
- panne du système d'exploitation ou du middleware (logiciel intercalé entre le matériel et l'application), qui peut être commun à plusieurs machines : une panne sur l'une risque fort de se retrouver sur l'autre – les produits de virtualisation entrent dans cette catégorie ;
- défaillance d'un système informatique utilitaire utilisé par tous (coupe-feu, antivirus ou serveur d'autorisation) qui empêche le fonctionnement de tous les autres serveurs en attente ;

- panne des systèmes de refroidissement ou de climatisation, particulièrement sensibles avec des serveurs à haute compacité (serveurs lames) ;
- atteinte aux gaines enterrées : câbles de réseau, téléphonie, eau, gaz, électricité, etc.,peuvent être détériorés par une pelleteuse ou un éboulement de terrain ;
- par extension, des événements qui s'imposent à tous, comme les arrêts forcés pour le changement d'heure des systèmes qui ne le font pas automatiquement, par exemple, ou les coupures obligatoires de courant pour contrôle ;
- enfin, bien évidemment, tout ce qui est de l'ordre du tremblement de terre, de l'incendie, de l'inondation et autre sinistre détruisant tout un ensemble sans distinction.

> **Exemple : la pelleteuse et le pont de Suresnes**
>
> Les environs de Puteaux et de Courbevoie ont vu s'implanter de nombreux sites informatiques. Dans les années 80, la société SLG avait un centre important dont la connexion au réseau X25 était vitale à l'époque. Un contrat de disponibilité avait été négocié avec un grand opérateur qui fournissait plusieurs connexions parallèles indépendantes.
>
> Un jour, une panne de réseau survient ; les lignes basculent sur le secours... Or lui aussi est en panne. Plus aucune connexion réseau ne fonctionne. Une pelleteuse au bord du pont de Suresnes avait malencontreusement sectionné des câbles. Et si l'opérateur avait effectivement prévu deux cheminements différents, pour le passage de la Seine, les deux voies se retrouvaient côte à côte sur le pont, créant ainsi les conditions d'une panne de mode commun.

Dans certains cas, on peut réduire la probabilité d'occurrence d'une panne de mode commun ou en diviser les effets pour éviter qu'elle soit commune.

On peut limiter les situations où ce type de panne provoque un sinistre, en mettant en application le bon sens populaire : « ne pas mettre tous ses œufs dans le même panier ». En pratique, cela se traduit par des recommandations mentionnées dans les chapitres 8, 9 et 10.

Arrêts de fonctionnement

L'indisponibilité se traduit par un arrêt du fonctionnement des machines. On distingue deux types d'arrêts : planifiés ou non. L'interruption non planifiée correspond aux diverses pannes et se gère en termes de fiabilité et de réparabilité. Cela ne veut pas dire pour autant que l'arrêt planifié n'est pas subi lui aussi comme une contrainte dont on voudrait se passer. Il doit faire l'objet d'une gestion tout aussi soigneuse.

Arrêt planifié

L'arrêt planifié est une interruption du fonctionnement des machines qui est prévue et normalement arrêtée au calendrier.

On distingue trois causes d'arrêts planifiés :

- **les arrêts permettant de faire évoluer la machine** – il s'agit de remplacer un élément par un autre plus efficace ou d'ajouter des composants pour rendre la machine plus puissante, par exemple ;
- **les arrêts pour maintenance** – un pièce vieillit et doit être remplacée pour éviter la panne ; un système d'exploitation doit être corrigé pour résister à une faille de sécurité ou à un virus… ;
- **les arrêts réglementaires** – ils sont effectués pour procéder à des contrôles techniques ou changer certains paramètres (changer l'heure sur certains matériels, par exemple).

Les évolutions technologiques cherchant à minimiser l'impact de ces arrêts, il est possible de plus en plus d'ajouter de la mémoire ou de changer un ventilateur sans arrêter toute la machine. Les efforts sur le matériel ont permis de limiter les cas où l'arrêt s'impose. On parle alors d'élément insérable à chaud (*hot pluggable*). En revanche, en ce qui concerne le système d'exploitation, les middlewares et les applications, il est beaucoup plus difficile d'éviter l'arrêt, ne serait-ce que parce que la plupart des améliorations installées ne deviennent effectives qu'après redémarrage de la machine – opération qui nécessite quelques minutes.

Lorsque l'arrêt de la machine est encore inévitable, les assemblages de type n+1 sont plus facile à exploiter : il permettent par exemple de n'arrêter qu'une machine sur les n, puis de la redémarrer avant d'arrêter la suivante, et ainsi de suite. Dans les systèmes redondants, il faut dans le meilleur des cas que la charge puisse se satisfaire d'une seule machine et que l'on puisse arrêter 50 % de la puissance pour mener l'opération. On effectue généralement ces actions lorsque la charge est faible, la nuit par exemple.

De plus en plus, en effet, les arrêts planifiés sont vécus comme des contraintes peu commodes. Pour des serveurs web ouverts au grand public (services bancaires, par exemple), on cherche à les effectuer au moment du plus faible trafic (en général le dimanche, vers deux heures du matin).

La possibilité de raccourcir – voire d'éliminer – les temps d'arrêt planifiés est intéressante à considérer dans les critères de choix de matériels.

Impact de l'arrêt

Lorsqu'un système s'arrête, que ce soit à cause d'une panne ou d'un arrêt planifié, l'impact sur le service ou les traitements assurés peut être variable selon les situations.

- **Pour un système simple** : tout est interrompu. On effectue les actions de réparation ou de remise en état et le redémarrage n'a lieu que lorsqu'elles sont achevées. Cela peut être long et difficile à prévoir.
- **Pour un système redondant** : la première panne ne devrait a priori pas se sentir, grâce au système de basculement sur le second système, mais il arrive

que celui-ci ne soit pas immédiat. Tous les usagers étant sur le même système, ils sont traités de la même manière, mais il faut pour bien faire que les données et le réseau soient accessibles aux deux machines indifféremment. Cela peut tout aussi bien aller vite et s'automatiser en partie, comme cela peut ne pas être totalement maîtrisé par les exploitants. Bien évidemment, si la panne est double, tout est arrêté et on est alors ramené au cas précédent.

- **Pour un système en grappe *n*+1** : les traitements et les utilisateurs sont répartis sur *n* systèmes. Ne sont donc concernés par la panne que les 1/*n* utilisateurs de l'élément défaillant. Normalement, le système de secours remplace assez vite le système en panne et les utilisateurs sont peu touchés. De plus, comme cette panne se produit relativement souvent, les opérateurs savent la traiter. En cas de deuxième panne, les 1/*n* utilisateurs sont alors arrêtés pour de bon. Ils ne retrouvent le service que lorsqu'un système supplémentaire de réserve est démarré ou réparé. Là encore, pour que tout ceci fonctionne bien, il faut que les données et le réseau soient accessibles à toutes les machines. Sur ces systèmes, la panne peut fort bien ne pas être découverte tout de suite car les effets en sont réduits et peuvent ressembler à des problèmes de performance. Il faut donc bien surveiller ces systèmes.

Les questions cruciales à se poser s'avèrent donc être des questions d'architecture technique : ne faut-il qu'un seul serveur – auquel cas il faudra une machine à tolérance de panne ? peut-on répartir les traitements sur *n* machines – auquel cas on aura recours à une grappe de serveurs ?

Lorsque se produit une panne dite de mode commun, les systèmes qui en sont victimes ne fonctionnent plus, quelle que soit leur résilience propre. Il faut alors avoir prévu un mécanisme de secours ou un redémarrage sur un environnement non soumis à cette panne. C'est ce qui est fait généralement en disposant de plusieurs sites.

Site secondaire et site distant

Toutes ces considérations entraînent en effet les entreprises à définir trois types de sites afin de répartir les risques et de diminuer les conséquences de sinistres : un site primaire et un site secondaire à faible distance d'un de l'autre, ainsi qu'un troisième site distant, éloigné de l'ordre de cent kilomètres au moins des deux autres.

Le duo primaire-secondaire

Afin de limiter les risques liés à une panne ou à un sinistre local, il est recommandé de répartir les éléments techniques sur deux sites voisins. Éloignés de quelques centaines de mètres ou de quelques kilomètres au maximum, ces sites sont qualifiés de « campus » ou « métropolitains » par les anglo-saxons : on peut souvent aller de l'un à l'autre sans passer par le domaine public.

Le but de cette répartition est triple :

1. **Limiter les pannes de mode commun** – Il faut donc faire attention à bien séparer les alimentations électriques, les cheminements de câbles divers, les accès télécom, etc. Une panne sur un site ne doit pas générer une panne sur l'autre.
2. **Permettre la répartition des systèmes en grappes ou en redondance** – La moitié des serveurs se trouve sur un site, l'autre moitié sur l'autre. Il en va de même pour le stockage. Les distances faibles, ne dépassant pas quelques kilomètres (chiffre en hausse permanente, mais limité par les lois de la physique), permettent en effet ces choix technologiques.
3. **Faciliter la reprise d'un site sur l'autre** – En cas de sinistre sur l'un des sites, l'autre est suffisamment proche pour simplifier les activités de reprise. Grâce aux technologies récentes de répartition de charge, la bascule de la charge d'un site sur l'autre (ou plutôt d'un serveur sur un autre au sein d'une grappe) est une activité courante.

La plupart des architectures techniques, même monolithiques, permettent une répartition sur deux sites proches reliés par des liens à haut débit fiables.

Le site distant

Ce troisième site est éloigné des deux autres de quelques centaines de kilomètres. Il ne doit pas être soumis aux mêmes sinistres dits régionaux : altitude, bassin fluvial, zone sismique différents, de même que les équipements potentiellement dangereux se trouvant à proximité (aéroport, industries à risque, etc.).

En cas de perte des deux sites primaire et secondaire, ce troisième site sera utilisé comme lieu de reprise. La probabilité qu'on y ait recours est certes plus faible et les technologies d'assistance au redémarrage sont également d'une autre nature. Pour cette raison, certaines entreprises ne prévoient pas ce site comme s'il était leur propriété, mais font appel à une prestation.

En réalité...

Les entreprises qui travaillent sur trois sites selon le modèle idéal décrit ci-dessus sont fort peu nombreuses.

Certaines entreprises qui ont déjà mis en place un schéma à deux sites métropolitains voisins considèrent comme exceptionnelle la nécessité d'un site distant. D'autres ne possèdent qu'un seul site principal simple sur lequel elles répartissent leurs moyens, assorti d'un site distant (100 km) vers lequel elles envoient régulièrement des fichiers ou des éléments susceptibles de faciliter la reprise. D'autres, enfin, n'ont qu'un seul site en tout et pour tout et sont peu préparées à redémarrer ailleurs.

Sans atteindre forcément l'idéal présenté ci-dessus, il est recommandé de diversifier au maximum l'emplacement des éléments nécessaires à la reprise de l'activité.

Types d'architectures

Pour adapter les schémas précédents aux systèmes informatiques, il est primordial de considérer la manière dont les applications et les données peuvent se répartir sur les systèmes techniques et les sites.

Entrer dans le détail de ces aspects serait fastidieux et sortirait du cadre de cet ouvrage ; il est néanmoins nécessaire de connaître dans les grandes lignes les différentes catégories techniques dans lesquelles on peut classer les applications.

Architecture monolithique

Dans une architecture monolithique, il est impossible de découper les applications, et les données sont d'un seul tenant. Cette situation se rencontre très souvent dans les applications traditionnelles d'entreprise : le fichier du personnel, par exemple, est unique et la paie est gérée par un seul programme ou groupe de programmes. L'accès des programmes aux données est assez rudimentaire et exclusif.

Dans ces conditions, il n'est pas possible de simplement répartir les traitements sur plusieurs machines. Il va falloir alors mettre en jeu des mécanismes de tolérance de panne ou de redondance simple 100/0, c'est-à-dire avec une machine supportant 100 % des traitements tandis qu'une autre est en attente à côté.

On se trouve cette fois dans la situation inverse : les traitements sont réalisés en séquences plus courtes ne portant que sur une partie des données. Les données elles-mêmes peuvent être réparties en lots relativement indépendants.

Architecture granulaire

Par construction, les dépendances entre traitements et les liens entre les données sont suffisamment réduits pour qu'il soit possible de distribuer ces applications sur n serveurs. L'exécution d'une application pour un utilisateur donné se traduira ainsi par l'exécution de plusieurs traitements les uns à la suite des autres sur des plateformes différentes ayant des échanges plus ou moins complexes entre elles. On parle assez souvent, dans ce contexte, d'architecture « client-serveur » et de « n tiers », ou encore d'environnements « granulaires et autonomes ».

Ces traitements se prêtent aisément à des approches de type grappe n+1. L'importance du réseau assurant des échanges entre les machines est accrue dans ce type d'architecture.

Une réalité multiple

Bien évidemment, en réalité, l'entreprise cumule diverses situations découlant de l'histoire de ses choix informatiques.

- Les situations monolithiques se rencontrent souvent dans les environnements de type « grands systèmes » anciens ou avec les grandes bases de données conçues dans les années 1980-1990 qui sont toujours en exploitation sans modification.
- Les architectures granulaires se rencontrent beaucoup dans l'informatique des serveurs web, des serveurs d'applications pour Internet et des divers outils associés (pare-feu, anti-virus, gestionnaire d'identités).

Les grands progiciels d'entreprise cumulent souvent ces deux types d'architectures : monolithique pour les bases de données centrales, assez granulaire pour des traitements de modules professionnels ou pour des présentations de données spécifiques, le tout couplé à des applications beaucoup plus anciennes (dites « héritées »), la plupart du temps monolithiques elles aussi.

Dans la réalité, on aura donc à faire cohabiter des systèmes à tolérance de pannes, des systèmes redondants et des grappes n+1. Il faudra cependant prendre soin de bien choisir l'architecture la mieux adaptée à chaque usage.

Chapitre 8

L'informatique au centre de données

Le centre de données, ou centre informatique, abrite des éléments clés pour l'activité de l'entreprise : les serveurs, le stockage et des matériels de réseau ou périphériques. La manière dont ces différents matériels sont choisis, organisés et gérés va influencer la disponibilité générale des services qu'ils produisent.

Des recommandations en matière de choix d'architecture et des listes de points importants à considérer s'imposent pour mettre en œuvre une informatique propice à la continuité d'activité.

Les serveurs

Les serveurs jouent un rôle central dans les traitements informatiques. Pour améliorer leur disponibilité, différentes approches se sont développées, qui mettent en œuvre les concepts présentés précédemment (voir figure 8-1).

Les solutions présentes sur le marché ont différentes caractéristiques qu'il est bon de connaître lorsqu'on construit sa stratégie de continuité (voir le chapitre 3).

Serveurs à tolérance de panne

L'une des manières d'obtenir des machines fiables consiste à doubler les éléments qui risquent le plus de subir une défaillance et à s'assurer par un système approprié que la machine, en cas de panne d'un élément, utilise automatiquement l'autre.

Les machines ainsi conçues sont dites « à tolérance de panne » (*fault tolerant*), en ce sens qu'elles acceptent une panne de chacun des composants doublés. Lorsqu'un élément est tombé en panne, la machine continue à fonctionner et l'administrateur a juste à changer la pièce ultérieurement, la plupart du temps sans interrompre le système.

Ces machines ont connu leur heure de gloire dans les années 1985-1995. Les marques Tandem et Stratus se sont illustrées dans ce domaine. Elles sont plus chères que des machines normales, pour deux raisons :

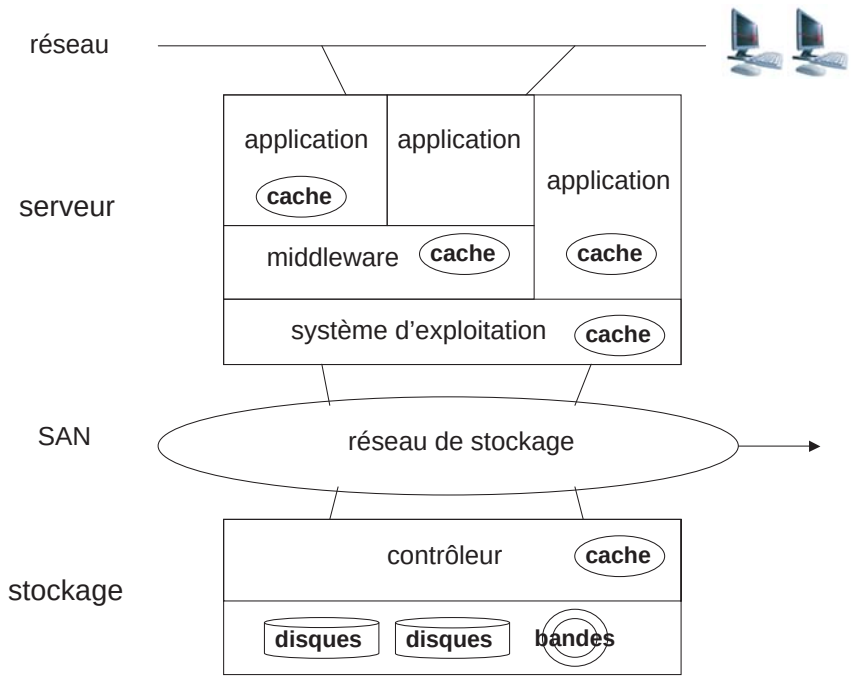


Figure 8-1 : Schéma d'un serveur et de son stockage

- une bonne partie du matériel existant en double, la note est elle-même doublée ;
- le système supervisant le bon fonctionnement en cas de panne est peu commun – son prix est en conséquence.

Lors de l'appréciation des risques sur ces machines, on prendra de préférence le scénario dans lequel la panne la plus à craindre est de mode commun. La machine étant suffisamment fiable, le risque premier est en effet la perte du site ou de l'alimentation électrique, par exemple. La solution sera alors de placer une machine de ce type sur le site principal en prévoyant une autre machine hors de portée des pannes de mode commun, c'est-à-dire à distance et alimentée différemment.

Mise en grappe

Concernant les serveurs, les offres de mise en grappe, ou *clustering*, sont nombreuses et riches en fonctionnalités. Pour rester dans le cadre de cet ouvrage, nous n'abordons que les aspects ayant trait à la continuité d'activité.

Les points à considérer pour mettre en œuvre des mécanismes de continuité sont les suivants :

- considérer la répartition des charges : est-elle souple et dynamique ou figée ?
- déterminer ce qui peut être isolé en cas de défaillance, ou ce qui peut être échangé immédiatement sans interruption ;
- déterminer – et si possible éliminer – les points uniques de défaillance ;
- considérer les situations demandant l'arrêt des machines et en réduire le nombre ;
- étudier la faisabilité des mécanismes de bascule (d'une machine vers une autre ou plusieurs autres) ;
- privilégier les machines qui détectent bien et tôt les défaillances et qui émettent des alertes ;
- étudier les capacités de retour à la normale ;
- étudier la connexion au réseau et son transfert en cas de défaillance ;
- étudier la connexion au stockage et son transfert en cas de défaillance ;
- analyser les mécanismes d'automatisation et de script (programme de commandes) ;
- faire la liste des pièces qu'il faut conserver sur le site pour une réparabilité optimale.

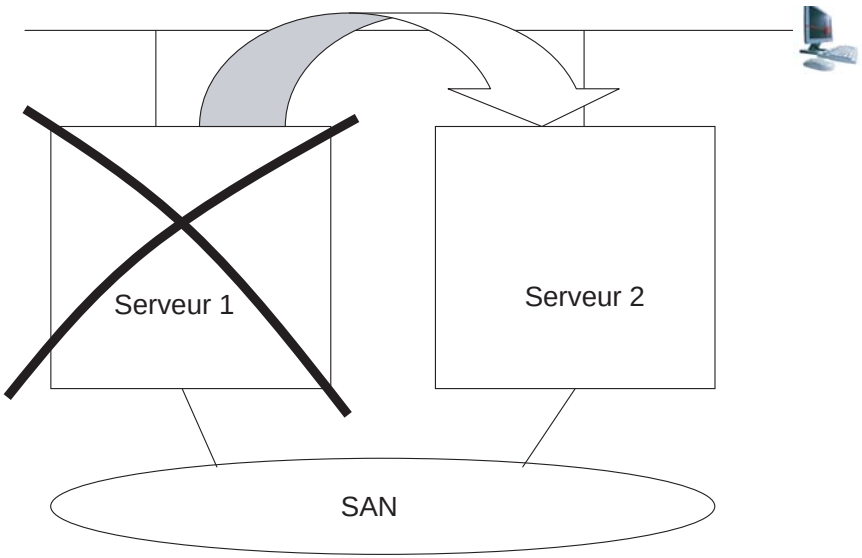


Figure 8-2 : Bascule d'un serveur sur un autre

En général, l'entreprise choisit un ou deux fournisseurs et conserve la même solution à long terme. La maintenance est souvent négociée à part. Cette solution doit être connue afin que les différentes parties prenantes puissent en tirer le meilleur profit en termes de disponibilité.

Enfin, il faut garder à l'esprit que le *cluster* peut se construire sur un ou deux sites, à priori assez proches.

Virtualisation

La virtualisation est un ensemble d'outils logiciels et de middleware qui permettent de :

- découper un serveur physique donné en plusieurs « serveurs logiques » ou « machines virtuelles » à géométrie variable ;
- masquer aux serveurs logiques la réalité du matériel existant réellement.

La virtualisation s'accompagne d'outils de gestion qui permettent de travailler sur les machines virtuelles. Le travail de l'exploitant est alors modifié : au lieu de gérer uniquement des machines réelles avec leurs caractéristiques techniques propres, il gère d'un côté des machines virtuelles (abstraites) et de l'autre les machines réelles (ou physiques en général moins nombreuses) sur lesquelles tournent les machines virtuelles. Par ailleurs, il existe un certain niveau d'interchangeabilité entre les machines réelles : une machine virtuelle peut, dans certaines limites, fonctionner sur différentes machines physiques.

Du point de vue de la continuité d'activité, la virtualisation présente des avantages mais aussi des inconvénients.

Avantages de la virtualisation

Une machine virtualisée est constituée de fichiers. Elle est donc téléchargeable ou peut être envoyée par simple transfert de fichier. Cela simplifie les scénarios de reprise distante : une machine virtuelle tournant sur une machine réelle défaillante sera « photographiée » et les fichiers la décrivant envoyés sur le site distant, où cette machine virtuelle pourra être « régénérée » sur une machine réelle en état de marche. Ces actions pouvant s'automatiser, il devient alors possible de « cloner » les machines virtuelles.

On voit donc l'intérêt de cette technologie pour les scénarios de reprise.

- Il est possible assez facilement de tenir prêtes des machines réelles à distance pour recevoir les machines virtuelles.
- Le transfert et la régénération d'une machine virtuelle sur un autre site sont rendus beaucoup plus faciles.
- Bien des tâches peuvent s'automatiser, en portant sur plusieurs machines ou plusieurs sites à la fois.
- La machine virtuelle hérite de la fiabilité de la machine réelle sur laquelle elle fonctionne, pour le meilleur et pour le pire.

Ainsi, la généralisation des outils de virtualisation révolutionne le travail de reprise et d'administration des machines.

> **Remarque**
>
> Les aspects de connexion au réseau et de stockage, qui sont à la limite du périmètre virtualisé, ne doivent pas être oubliés dans les schémas de continuité d'activité.

Inconvénients de la virtualisation

Cependant, l'usage de la virtualisation dans le cadre d'un plan de continuité comporte également un certain nombre d'inconvénients.

- Elle représente un outil de plus sur les machines, et donc une cause de panne supplémentaire.
- Les machines virtuelles gérées à la place des machines physiques ne peuvent pas fonctionner sur un serveur classique : elles nécessitent un serveur équipé au moins d'une couche de virtualisation adaptée, ce qui limite les scénarios.
- Le matériel utilisable en cas de reprise doit avoir prévu la virtualisation, ce qui représente un effort et un coût supplémentaire.
- Le matériel que l'on peut utiliser pour la reprise doit avoir été prévu par la virtualisation, qui doit tenir compte de ses caractéristiques : cela limite les cas possibles ; la situation est pire sans virtualisation toutefois.
- Les outils restent compartimentés selon les différentes technologies : les outils pour matériels Unix IBM ne sont pas du tout les mêmes que pour ceux d'HP et très différents de ceux des matériels à processeur Intel fonctionnant avec Windows.
- Il faut gérer à la fois des configurations réelles et virtuelles.

Malgré tout, dans l'ensemble, les spécialistes s'accordent à dire que l'usage de la virtualisation en environnement Intel/Windows est plutôt bénéfique dans le cadre d'un plan de reprise.

Le stockage

Le stockage représente le deuxième pilier de l'informatique, car c'est là que résident les données. Les fournisseurs de stockage ont développé des offres de plus en plus indépendantes des serveurs, proposant des fonctions très intéressantes pour sauvegarder les données, les répliquer à distance et les restaurer sur des systèmes de secours.

Toutes ces fonctions sont à regarder de près pour élaborer une stratégie de continuité. En effet, la multitude de combinaisons possibles entre les serveurs, les outils logiciels, les fonctions propres au stockage et les agencements de sites rend les choix difficiles.

Fonctions des contrôleurs

Le contrôleur est en quelque sorte le chef d'orchestre du stockage : il prend la responsabilité des données, les conserve et les protège ; il sait où les retrouver, répond aux demandes d'accès des serveurs, demande des traitements spécifiques, transfère des données d'un support à un autre (d'un disque vers une bande, par exemple), etc. Appliqué au contrôleur, le mot « donnée » est d'ailleurs abusif. En général, celui-ci ne voit en effet que des ensembles de bits ou blocs dont il a la charge. Il n'a pas notion du fait que ces blocs constituent une donnée ou appartiennent à un même fichier, cette connaissance étant réservée au domaine du serveur.

En se concentrant sur les enjeux de continuité, il est important d'étudier les points suivants.

- Nature du contrôleur : est-ce un serveur simple, sans redondance (plutôt rare), ou une grappe de serveurs (plus usuel) ? Encore mieux : est-ce un matériel spécifiquement étudié pour la fiabilité ?
- Le contrôleur sépare-t-il les traitements d'avant-plan (vers les serveurs) et d'arrière-plan (vers les disques) sur des processeurs séparés ?
- La manière dont le contrôleur est connecté aux serveurs permet-elle la redondance ou l'équilibrage sur plusieurs voies ? Passe-t-elle par un réseau spécialement dédié au stockage ?(Voir la section sur les SAN en fin de chapitre).
- La manière dont le contrôleur est connecté aux disques ou mémoires diverses est-elle suffisamment fiable ?
- La manière dont le contrôleur répartit les blocs écrits sur plusieurs disques avec bit de parité, la gestion des groupes RAID qui utilise plusieurs lots de disques en parallèle et assure des niveaux de fiabilité différents qu'il faut connaître.
- Qualité du cache interne : est-il volatile ? Conserve-t-il ses données en cas de coupure de courant ?
- Le contrôleur permet-il le routage d'entrée/sortie ? Cette fonction consiste à router les écritures vers un autre contrôleur distant et à en garantir la bonne exécution locale et distante, synchronisée ou non.
- Le contrôleur permet-il de réaliser des clichés (*snapshots*) ? Cette fonction consiste cette fois à garder une image figée des données pendant un certain temps. Tant que les données sont figées, les modifications qui les concernent sont alors consignées ailleurs sans inconvénient.
- Le contrôleur peut-il gérer des cohérences entre données ou blocs ? (c'est-à-dire modifier tous les blocs d'un même groupe ensemble ou n'en modifier aucun).

Toutes ces fonctions présentent un grand intérêt dans les différents schémas de continuité d'activité, comme l'illustrent les trois exemples suivants.

Snapshot ou cliché

Le *snapshot* permet de figer une image des données et de les sauvegarder sur bande (cela peut prendre cinq heures et plus) pendant que la production continue sans interruption. Sans cette fonction, il faut interrompre les écritures dans les fichiers à sauvegarder, et donc interrompre une partie de l'activité.

Routage d'entrée/sortie

Le routage d'E/S permet, sous certaines conditions, de conserver sur un site distant une copie exacte du stockage principal. En cas de plan de reprise sur ce site distant, les données y sont identiques.

RAID

Le RAID (*Rapid Array of Independent Disks* ou baie de disques indépendants) permet, avec des disques simples, d'obtenir une bonne fiabilité : en cas de défaillance d'un disque, les données sont reconstituables à partir des autres disques.

Toutes ces fonctions ne sont pas présentes de la même manière dans les matériels disponibles sur le marché. Des substitutions sont possibles, certaines fonctions pouvant être absentes du stockage si elles sont contenues dans le middleware, par exemple.

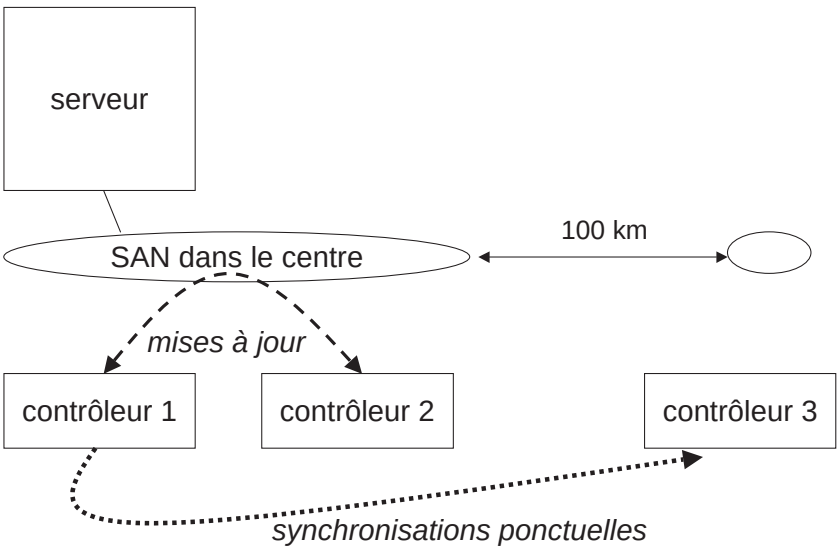


Figure 8-3 : Contrôleurs échangeant sur un SAN local et avec un site distant

Remarque

Notons enfin que, dans certains cas particuliers, les fonctions de contrôleur résident dans un serveur au sein d'une grappe, voire dans une partition virtualisée sur un serveur. Mais cela ne change pas radicalement ce qui est dit plus haut.

Fonctions du middleware

« Middleware » est un terme générique pour désigner le logiciel qui se situe au-dessus du système d'exploitation mais en dessous des applications. Il joue un rôle important dans la gestion de la conservation des données et il faut donc s'en préoccuper dans une approche de continuité des traitements.

Systèmes de fichiers

Le système de fichiers (*file system*) permet tout simplement de gérer les fichiers, ce qui est une forme de conservation des données. On y trouve plusieurs fonctions utiles pour la continuité d'activité, parmi lesquelles :

- la capacité à reconstituer des fichiers endommagés ;
- la protection des accès en écriture et en lecture ;
- le support des grappes (*clustered file system*) qui permet à des serveurs différents d'accéder concurremment et en même temps aux données tout en garantissant leur intégrité.

Cependant, l'importance des systèmes de fichiers pour la continuité s'amoindrit de plus en plus. En effet, pour disposer de fonctions avancées, on leur préfère les SGBD ou les systèmes NAS, qui sont des serveurs dédiés au système de fichiers.

Moniteurs transactionnels

Les moniteurs transactionnels sont des middlewares qui assurent la bonne exécution des transactions, c'est-à-dire des modifications coordonnées des données.

Parmi les fonctions utiles qu'ils présentent en termes de continuité, on citera essentiellement :

- la capacité à reconstituer un état correct des données en annulant une transaction qui s'est mal déroulée ;
- la possibilité de router une transaction (*transaction routing*) vers un autre système pour qu'elle s'y exécute, ce qui permet d'avoir des données identiques sur deux sites différents, par exemple.

Les moniteurs transactionnels sont eux aussi en perte de vitesse, car supplantés par les SGBD qui possèdent, entre autres, les mêmes avantages.

SGBD

Les SGBD ou systèmes de gestion de bases de données prennent une place prépondérante dans la continuité d'activité. Ils concentrent en effet des fonctions indispensables :

- la capacité à reconstruire un état « propre » des données après un incident (matériel ou non), en annulant les modifications qui ont échoué (*rollback* ou retour en arrière) ;

- la possibilité de réaliser des mises à jour de données sur plusieurs bases réparties potentiellement en des lieux différents, avec un engagement sur le résultat (*commit* ou validation) quoi qu'il arrive ;
- la faculté de figer un état cohérent des données et de noter à part, dans un journal, la totalité des modifications qui y sont apportées par la suite sur une période donnée ;
- la possibilité de reconstituer des données correctes en partant d'un état antérieur correct et en lui appliquant les modifications contenues dans un journal (*forward recovery* ou restauration par progression) ;
- de manière générale, la possibilité de procéder à des interventions intelligentes sur les données, les SGBD en permettant la compréhension ; il est ainsi possible à un administrateur de « nettoyer » des tables en annulant certaines transactions et pas d'autres – à pratiquer avec modération toutefois.

De manière à obtenir une protection optimale en cas de sinistre, on établit en général une base primaire « active » sur un site et une base de secours « en sommeil » sur un autre site. La base en sommeil peut se contenter d'une copie ponctuelle des données tout en recevant le journal des mises à jour. En cas de besoin, il faudra, pour la « réveiller », appliquer les journaux afin de reconstituer les données, ce qui peut prendre un certain temps. On se trouve alors dans la catégorie du « secours tiède » (moyens préparés mais pas prêts à l'usage : voir le chapitre 3).

En revanche, la base de secours peut être totalement à jour en permanence si elle applique les modifications de la base primaire au fur et à mesure. Cela peut se faire soit de manière synchronisée avec la base primaire, soit de manière asynchrone. L'intérêt majeur est que ce qui est validé (ou « commité ») sur un site, l'est également sur l'autre.

Enfin, dans les approches les plus avancées, il n'est plus fait de distinction entre base primaire et base secondaire : plus exactement, les activités sont réparties entre les deux bases, chacune étant « primaire » pour elle-même et « secondaire » pour l'autre.

Il existe aussi des mises en œuvre intéressantes dans lesquelles la base secondaire est utilisée par des applications qui ne travaillent qu'en lecture. Cela permet ainsi de soulager la base primaire et de rentabiliser les investissements pour le secours en cas de sinistre. S'il est besoin de basculer sur la base de secours, les applications en lecture sont alors arrêtées et les applications de production démarrées.

Par précaution, il faut, évidemment, ne pas stocker le journal et les copies de la base de données au même endroit que la base active. En effet, en cas de perte du système de stockage, on perdrait par la même occasion la capacité à reconstruire les données.

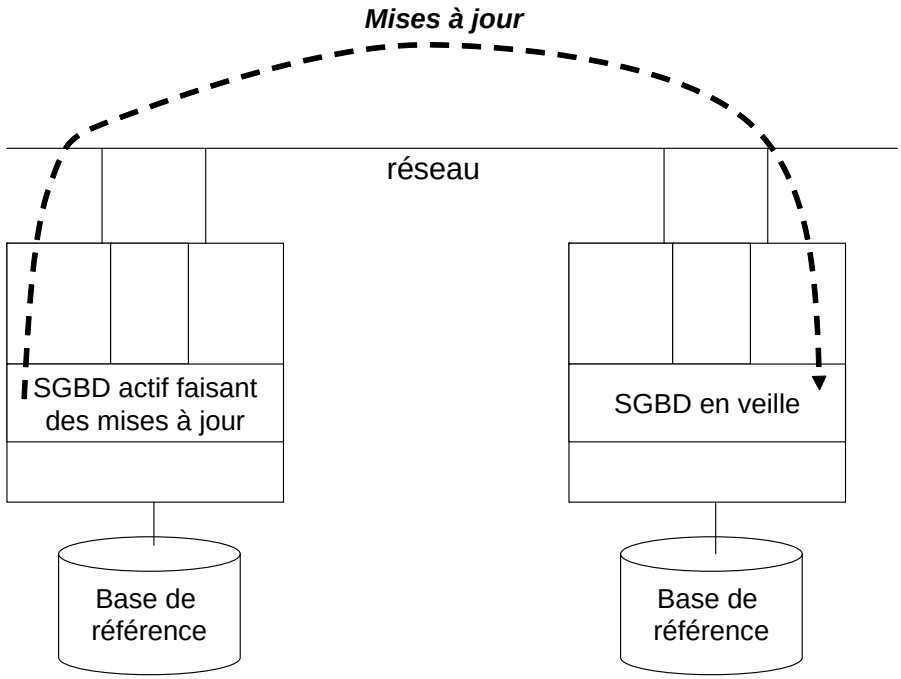


Figure 8-4: : Deux SGBD échangeant à distance

Caches internes et risques associés

Le cache est une zone de mémoire provisoire où l'on place des données en transit. Un programme met des données en cache, par exemple, avant qu'elles ne soient envoyées à un contrôleur de stockage. Le contrôleur lui-même peut ensuite mettre ces données en cache avant qu'elles ne soient écrites sur disques, lieu de leur stockage final et sécurisé. Ce mécanisme permet d'obtenir des gains en performance considérables.

La fiabilité de ces zones de cache est souvent sujette à caution. En effet, elles ne sont généralement pas protégées en cas de panne d'électricité par exemple, alors qu'un disque, lui, conserve bien évidemment son contenu. L'apparition des caches non-volatiles représente ici une avancée positive.

Concernant la continuité d'activité, les caches posent problème car, bien que parfois très important pour la récupération des données, leur contenu est très souvent perdu en cas de sinistre. De plus, les systèmes de routage ou de propagation des entrées/sorties (voir page 178) ne répercutent sur le site distant que les écritures sur disque. Or, les écritures de données modifiées en cache n'ont pas encore fait l'objet d'une demande d'écriture sur disque et sont ainsi igno-

rées du contrôleur. L'application considère alors que la donnée est modifiée, alors qu'elle ne l'est pas, ni sur le stockage primaire, ni sur le secondaire. Cette incohérence portant sur des données potentiellement importantes pour l'entreprise crée une situation très difficile à gérer en cas de reprise.

Un contrôle se révèle donc nécessaire sur tout cela. Il existe des produits qui, lorsqu'une donnée modifiée est écrite en cache, forcent immédiatement l'écriture sur disque. Les grands systèmes (mainframe IBM), et souvent les SGBD, gèrent cela ainsi de manière très précise. En cas de doute, il faut vérifier que les produits ou outils complémentaires adéquats sont en place et bien actifs.

Protection continue des données (CDP)

La CDP (*Continuous Data Protection*) ou protection continue des données est une technique assez récente qui consiste à surveiller un système en capturant toutes les modifications de données y ayant lieu. Ces modifications, une fois capturées, sont conservées en lieu sûr, généralement sur un serveur dédié à cette fonction de CDP. La fiabilité de ce serveur de CDP doit donc être considérée avec la plus grande attention.

Le système ainsi surveillé est accompagné d'agents de surveillance propres au produit assurant la CDP, dont il faut également étudier la fiabilité. Vus du système surveillé, ils sont en effet considérés comme des « corps étrangers » provenant d'un autre fournisseur.

Proposant des pistes d'amélioration intéressantes en matière de continuité, cette technologie est toutefois récente et doit encore faire ses preuves.

Stockage en réseau NAS

Le stockage en réseau NAS (*network-attached storage*) est un serveur de fichiers attaché au réseau IP (protocole Internet). Les serveurs d'applications s'adressent à lui pour accéder à des fichiers partagés en mode lecture ou écriture. Le NAS met ainsi en œuvre un ou plusieurs systèmes de fichiers.

Concernant la continuité d'activité, les avantages du NAS sont hérités à la fois de sa nature de contrôleur et de celle de serveur. Les caractéristiques mentionnées précédemment au sujet des serveurs, contrôleurs et systèmes de fichiers restent donc valables pour ce type de stockage. Parmi elles :

- l'agencement interne du NAS , qui peut être à base de tolérance aux pannes ou de redondance en grappe 1+1 ;
- la capacité à reconstruire des fichiers endommagés ;
- la possibilité de figer des clichés (*snapshots* : voir page 179) sur des fichiers entiers et à intervalles rapprochés ;
- la possibilité de revenir en arrière sur un cliché antérieur, fichier par fichier ;
- la capacité à sauvegarder directement à partir du NAS sur des systèmes à bandes, par exemple, sans passer par les serveurs ;

- la capacité à router sur un site voisin ou distant les modifications apportées aux fichiers, tout en restant sur le réseau IP habituel ;
- la possibilité de déplacer des groupes de fichiers entiers d'un NAS à un autre, qu'ils soient proches ou distants.

La simplicité d'utilisation des NAS dans les environnements utilisant de nombreux fichiers, surtout s'ils sont partagés, leur a donné une place prépondérante dans les entreprises et dans les plans de reprise.

Sauvegarde et restauration

On présente souvent la sauvegarde sur bande comme étant l'unique précaution à prendre pour se prémunir d'une perte de données catastrophique. Assez souvent, les questionnaires d'audit se focalisent donc sur la sauvegarde, selon une vision remontant aux années 1980.

La sauvegarde est-elle encore utile ?

Les descriptions qui précèdent montrent que bien d'autres technologies sont disponibles pour éviter les pertes de données et faciliter leur reconstruction. Cela ne veut pas dire – loin de là – que la sauvegarde ne sert à rien : il reste des situations où elle est nécessaire, même si celles-ci deviennent, avec l'expansion des nouvelles technologies, de plus en plus rares.

Plus la pratique des technologies comme le *snapshot* ou la copie miroir locale et distante effectuée par des systèmes de stockage, des NAS ou des SGBD se répand, plus la nécessité technique d'une sauvegarde sur bande diminue. Cinq raisons maintiennent toutefois son usage :

- Les technologies citées ne sont pas employées partout, car tous les systèmes en place ne le permettent pas.
- Le coût des investissements nécessaires dans ces nouvelles technologies est élevé, la formation des exploitants coûteuse et longue. La sauvegarde demeure une solution bon marché, simple et assez efficace, qui a tout du moins le mérite d'exister.
- Quand toutes les autres solutions ont échoué, recourir au stockage de bandes à l'abri des désastres reste la solution ultime.
- La réglementation l'exige dans un certain nombre de cas.
- La proximité technologique avec l'archivage (qui n'est pas une sauvegarde) fait que certains utilisateurs conservent des archives à partir des sauvegardes sur bandes.

Dans la réalité, on constate que la sauvegarde sur bande combinée aux autres techniques mentionnées précédemment permet d'arriver à des solutions de compromis d'efficacité et de coût intéressantes.

La problématique spécifique de la sauvegarde des données sur PC, en particulier sur les ordinateurs portables, sera vue dans le chapitre 9.

Objectif : restaurer les données

Il ne faut surtout pas perdre de vue l'objectif auquel tous ces moyens techniques doivent parvenir : restaurer les données qui ont été perdues. La sauvegarde n'a en effet aucun intérêt si les données ne peuvent être restaurées ou si la restauration ne fournit pas de données correctes.

Les grandes entreprises ne possèdent généralement pas un seul système de sauvegarde et restauration, mais plusieurs. On distingue trois catégories de sauvegardes, souvent dictées par les outils eux-mêmes.

- **Les sauvegardes complètes** : tout est sauvegardé en totalité. La restauration est ainsi aisée, car il n'y a aucune question à se poser. En revanche, la sauvegarde est longue et si les données ont peu évolué, a quantité de cassettes ou autre média s'accroît inutilement, car contenant de nombreuses données identiques d'une fois sur l'autre.
- **Les sauvegardes incrémentielles** : ne sont sauvegardées que les données qui ont changé par rapport à la sauvegarde précédente, la première sauvegarde étant complète. Cette méthode est rapide et peu consommatrice d'espace sur les bandes. Cependant, lors de la restauration des données, elle implique souvent de rechercher toute une série de bandes de sauvegardes diverses. À l'inverse de la précédente, cette méthode est donc efficace en sauvegarde mais difficile en restauration.
- **Les sauvegardes différentielles** : après une première sauvegarde complète, cette méthode ne sauvegarde que les données ayant été modifiées depuis la dernière sauvegarde complète. La restauration nécessite alors d'avoir seulement la dernière sauvegarde complète et la dernière sauvegarde différentielle. Envisagée en général fichier par fichier, cette méthode est un bon compromis : plus longue en sauvegarde que la sauvegarde incrémentielle, mais plus rapide en restauration.

Gérer les cassettes et autres supports

Les cassettes de sauvegarde ou autre média (disques optiques, DVD, etc.) nécessitent une gestion particulièrement soigneuse dans le cadre du plan de continuité. Les aspects suivants doivent être absolument pris en compte :

- Les cassettes doivent être entreposées dans un lieu sûr, à l'abri des risques qui pèsent sur les systèmes dont elles sont les sauvegardes.
- Les employés qui viendront récupérer les cassettes en cas de sinistre doivent pouvoir les trouver et les identifier facilement.
- Si certaines cassettes sont constituées en lots à manipuler ensemble, ceux-ci doivent être évidents (regroupés dans une mallette, par exemple).
- À l'inverse, il peut arriver que certaines cassettes ne doivent pas se trouver ensemble (sauvegardes de clients différents, par exemple, qui ne doivent absolument pas être mélangées) : cela doit être clairement identifiable.

- Dans les cas où des contraintes s'appliquent sur les lots de cassettes (confidentialité, urgence, destination particulière, etc.), celles-ci doivent être indiquées et faciles à comprendre par les personnes chargées de les récupérer.
- Il peut être intéressant d'indiquer une priorité de traitement ou de prise en compte, lorsque les lots de cassettes ne peuvent être déménagés en une seule fois. Celle-ci est basée alors sur les délais de restauration (par exemple : immédiat, moins de 4 heures, même jour, moins de 24 heures, de 24 à 72 heures, plus de 72 heures).
- Le moyen de transport peut être éventuellement indiqué sur les lots.
- Il est indispensable de tester régulièrement la lisibilité des cassettes et de copier à neuf celles qui vieillissent mal, avant qu'elles ne deviennent illisibles.
- Les cassettes devenues inutiles doivent être éliminées (ou recyclées).
- Les consignes des fabricants pour le stockage doivent être respectées absolument.

Un système de gestion informatique des sauvegardes peut être utile pour administrer tout cela.

> **Exemple : un oubli fâcheux**
>
> La société de service informatique SLBanque gère l'informatique de la Banque du Musée, en banlieue parisienne. Les systèmes de production (ordinateurs, stockage) sont situés dans un centre informatique proche du périphérique. Des sauvegardes sont effectuées régulièrement et, tous les lundis, des convoyeurs viennent prendre livraison de mallettes de cartouches à destination d'un centre d'entreposage en province proche.
>
> Un lundi, des travaux importants ont lieu au centre, nécessitant de désactiver en partie l'ouverture automatique des portes. Les convoyeurs effectuent malgré tout leur transfert habituel, et une fois partis, des livreurs arrivent avec du matériel d'un tout autre ordre. Après 45 minutes, la livraison est finie et l'on ferme enfin les portes à la main. C'est là qu'on aperçoit une mallette de cassettes oubliée, restée là pour caler une porte !
>
> Il n'a pas été possible de retrouver ou d'appeler les convoyeurs. Fort heureusement, le nom du client était indiqué sur la mallette et celui-ci, une fois averti, a prévenu qui de droit.
>
> **Et pourtant...** le client aurait-il constaté seul qu'il lui manquait une mallette ? Cette mésaventure a conduit par la suite la société SLBanque et ses clients à revoir leurs procédures de sortie des cassettes de sauvegarde.

Robots de sauvegarde

Les robots de sauvegarde sont des matériels périphériques qui servent à sauvegarder et restaurer les données sur un support en général amovible (cassette, cartouche…). Ils sont la plupart du temps partagés par différents environnements techniques et utilisés par de nombreux serveurs ou NAS. Leur constitution mécanique, comportant un grand nombre de pièces en mouvement, les rend fragiles et leur fiabilité dépend avant tout d'une bonne maintenance.

Le matériel avec lequel la sauvegarde est effectuée peut être différent de celui avec lequel la restauration sera réalisée : il suffit de ne pas se trouver sur le même site. Des précautions de compatibilité sont nécessaires, sous peine de ne pouvoir restaurer correctement.

Il existe des systèmes qui virtualisent les bandes et les dérouleurs de bandes : les VTS (*virtual tape servers* ou serveurs à bande virtuelle). Nombre d'opérations d'écriture et de lecture se font alors sur disques au lieu de se faire sur du matériel réel à bande. Toutefois, la sécurité des opérations de sauvegarde est garantie par la réalisation finale de cassettes de sauvegarde appropriées. Ces systèmes permettent ainsi d'éviter les créations inutiles de cassettes.

Tous ces systèmes proposent souvent d'autres fonctions en option, dont il faut tenir compte dans le cadre d'un plan de continuité. En effet, il faut être sûr de pouvoir restaurer :

- la compression des données – il faut pouvoir décompresser lors de la restauration ;
- le chiffrement – de la même manière, il faut pouvoir déchiffrer et avoir les droits techniques et administratifs pour le faire ;
- la déduplication (élimination de doublons pour gagner de l'espace), qui pose le même type de contraintes.

La capacité à effectuer une restauration correcte sur un système potentiellement différent du système de sauvegarde est fondamentale. Sans cela, en effet, toute sauvegarde est inutile. Parmi les points à considérer, on compte :

- la compatibilité des formats en tous genres (cassette, dérouleur, chargeur, codage, etc.) ;
- la compatibilité des logiciels, qui est une exigence très forte – dans presque tous les cas, on aura besoin pour la restauration du même logiciel que celui qui a servi pour la sauvegarde ;
- une bonne gestion des droits associés – l'administrateur qui charge une sauvegarde doit disposer des droits nécessaires, l'outil doit l'autoriser à opérer ;
- les performances – la restauration ne devant pas durer dix heures si l'on dispose d'un temps limité à quatre heures, les débits doivent être calculés correctement ;
- l'état des matériels de restauration, qui doit être vérifié et testé, avec des contrats de maintenance convenables ;
- l'existence et l'actualité des licences d'utilisation.

Tous ces aspects sont importants, surtout dans les cas où le logiciel et les moyens de restauration utilisés sur un site de secours ne sont pas ceux que ce site emploie pour son usage propre.

Les réseaux du centre informatique

Le centre informatique dispose de plusieurs types de réseaux :

- le réseau assurant la connexion des terminaux et postes de travail aux serveurs ; le protocole IP y est omniprésent ;
- le réseau supportant les échanges des serveurs entre eux, avec plusieurs vitesses et débits possibles : si des protocoles de grappe existent encore, IP à haute vitesse se généralise et on assiste à l'émergence de technologies nouvelles comme Infiniband ;
- le réseau de stockage SAN (*Storage Area Network*), qui connecte le stockage en groupes aux divers serveurs.

Pour optimiser les débits, réduire les risques et isoler les perturbations, ces différents réseaux peuvent être cloisonnés et recourir à des protocoles divers. Ils peuvent aussi, pour des raisons d'efficacité, partager des artères rapides. Les câblages sont de natures différentes, même si la fibre optique se généralise.

En général, on fait encore la distinction entre SAN et réseau traditionnel.

Réseau de stockage SAN

Le SAN (*Storage Area Network*) est un réseau qui assure la connexion entre des contrôleurs de stockage, des unités de disques diverses et des serveurs. On le trouve principalement en salle informatique, dont il ne sort que pour assurer une liaison avec un site secondaire très proche.

La principale technologie réseau du SAN est la technologie d'interconnexion appelée *Fibre Channel* (FC), qui opère principalement – mais pas seulement – sur fibre optique à courtes distances. La liaison avec le troisième site distant, s'il existe, nécessitera une autre technologie et un couplage avec des routeurs spéciaux. De nouvelles techniques normalisées apparaissent, tel le protocole iSCSI (*Internet Small Computer System Interface*), appelé aussi SCSI sur IP, qui consiste à transmettre les instructions et données dans des paquets IP. Elles rapprochent le SAN des techniques de réseau traditionnel.

Comme tout réseau, le SAN utilise des routeurs et des commutateurs plus ou moins puissants et évolués.

En ce qui concerne le SAN, la fiabilité et la disponibilité méritent la plus grande attention : un SAN en panne, même partiellement, peut paralyser une salle informatique entière, dans le cas où les serveurs principaux ne peuvent plus accéder à leur stockage.

Réseau traditionnel

Concernant le réseau traditionnel, l'analyse et les mesures à prendre ressemblent beaucoup à celles ayant trait aux serveurs. On y retrouve en effet les mêmes orientations et architectures :

- la segmentation ou répartition sur des éléments en grappes de type n+1, avec de petites machines simples dédiées à une tâche particulière (pare-feu, anti-virus, détecteurs divers, etc.) ;
- la consolidation (monolithique) sur des équipements très puissants, uniques et donc à tolérance de panne ;
- la virtualisation, qui permet à une même machine d'abriter des fonctions multiples ;
- la redondance qui, associée à une virtualisation simple, permet d'abriter deux machines virtuelles dans une même machine physique et d'en arrêter une sans interrompre l'autre.

Les évolutions du réseau sont par ailleurs dictées par les évolutions des serveurs : si l'on consolide dix serveurs pour n'en faire qu'un seul, le réseau qui les reliait change de nature de même que sa vulnérabilité aux pannes. Les deux approches doivent être associées pour obtenir une configuration à haute disponibilité.

Performance et fiabilité des réseaux

Quel que soit le type de réseau, il est indispensable de porter un regard attentif et critique sur les points suivants :

- la possibilité pour des matériels de constructeurs différents de travailler ensemble ; en effet, le respect des protocoles n'est souvent pas suffisant et il faut également étudier les comportements de matériel en présence d'anomalies ou de pannes partielles – ce comportement doit être cohérent d'une machine à l'autre ;
- la tolérance aux pannes des éléments centraux qui constituent des points uniques de défaillance, tels que les commutateurs directeurs ;
- la possibilité ou non de diversifier les chemins d'accès entre l'origine et la destination, afin de se prémunir d'une panne sur un chemin ;
- la souplesse de passage d'un chemin à un autre en cas de panne du premier : est-ce automatique ou manuel ? Peut-on utiliser deux voies en parallèle ou de manière alternée ?
- le comportement des matériels en cas de redémarrage suite à divers types d'interruption, qui doit être cohérent et rétablir un état du réseau acceptable ;
- la conservation des changements de paramètres dynamiques, afin d'éviter, en cas de redémarrage, de faire une restauration sur un état antérieur incorrect.

Construire un réseau performant, c'est aussi construire un réseau fiable. Là encore, les pannes de mode commun ne doivent pas être négligées dans l'évaluation de la fiabilité (voir le chapitre 7).

Chapitre 9

Infrastructure et poste de travail de l'employé

Tout ce qui a trait à l'environnement de travail de l'employé – téléphonie, poste de travail en réseau, bureau – ne doit pas non plus être négligé. Ces éléments, utilisant des technologies de plus en plus avancées, sont en effet des points vulnérables mais indispensables à la continuité de l'entreprise.

Ceci inclut dans une certaine mesure les problématiques liées aux ressources humaines, bien que ce sujet soit à la limite du périmètre de cet ouvrage.

Les réseaux

L'analyse de la disponibilité du réseau se révèle toujours compliquée, parce qu'un réseau n'est pas un « objet technique » comme les autres. En effet, ce n'est pas parce que les routeurs ou commutateurs fonctionnent que le réseau est disponible. Le bon fonctionnement d'un réseau implique en général deux acteurs – chacun à une extrémité – avec la plupart du temps un opérateur entre les deux. C'est un jeu à trois. Quant aux cas où le réseau fonctionne mal, il n'est pas toujours aisé d'en déterminer les causes. La vision de son état de fonctionnement peut d'ailleurs être différente selon l'endroit d'où on l'observe.

Par ailleurs, lorsque seul le réseau ne fonctionne pas dans une entreprise, les techniciens les plus avancés se retrouvent désemparés : aucune machine à réparer. Tout au plus peut-on essayer de basculer vers un autre réseau ou un autre opérateur en espérant que celui-ci ne sera pas victime de la même avarie.

Réseau téléphonique

En dépit de la montée en puissance des nouvelles technologies, le téléphone joue encore un rôle primordial dans la vie de l'entreprise, comme l'illustre l'exemple suivant.

> **Exemple : l'acheteur et le téléphone**
>
> M. Achat est acheteur chez un fabricant qui dépend fortement de ses fournisseurs en termes de délais. Un soir, de retour à son domicile, il voit au journal télévisé régional qu'un

> incendie s'est déclaré chez son principal fournisseur. La télévision montre des flammes et le commentaire est imprécis. Souhaitant avoir plus d'information, M. Achat essaie d'appeler le site sinistré : impossible. Le site est trop éloigné pour qu'il s'y rende en voiture.
>
> Le lendemain matin, il cherche à joindre son commercial attitré chez le fournisseur – en vain. Par précaution, il passe commande chez un autre fournisseur, pratiquant des prix très élevés, sacrifiant ainsi à la sécurité.
>
> Trois jours après, M. Achat apprend que le sinistre ne concernait ni l'usine ni les stocks de son fournisseur, mais uniquement des bureaux et la salle de l'autocommutateur.
>
> **Moralité :**
> – il peut être utile de disposer du numéro de portable de son commercial ;
> – en cas d'incendie, il faut essayer dans la mesure du possible de transmettre à la télévision des informations précises, en espérant qu'elles passeront à l'antenne… ;
> – la société sinistrée doit prévoir un accueil téléphonique de ses clients, dans des cas semblables de sinistre : son opérateur doit avoir des solutions.

Les réseaux téléphoniques n'ont pas été conçus en prévision que tout le monde appelle tout le monde au même moment (plus exactement, qu'une moitié des abonnés appelle l'autre moitié). Ils sont dimensionnés pour permettre le trafic de quelques pourcents d'une zone donnée (on cite souvent le chiffre de 10 % en Amérique du Nord). Cela est valable aussi bien pour la téléphonie fixe que pour la téléphonie mobile. Ainsi, en cas de sinistre régional, ou simplement d'incident ou événement attirant la curiosité générale, il est impossible de compter sur un acheminement sûr des appels.

Vu de l'utilisateur en entreprise, le réseau téléphonique peut être décomposé en trois parties, dont chacune mérite l'attention :

- les cheminements internes à l'entreprise, courant dans des goulottes, avec des connexions situées dans des répartiteurs ou armoires qu'il faut vérifier ;
- le cheminement hors de l'entreprise, dirigé vers les moyens techniques de l'opérateur (central téléphonique) en passant par la voie publique et ses aléas ;
- l'autocommutateur de l'entreprise, qui est une machine s'apparentant désormais à un ordinateur, avec sa redondance interne, sa maintenance, ses mises à niveaux et ses techniciens.

Câblage interne

Concernant le câblage interne et les armoires de répartition, il faut s'assurer que :

- les cabinets de passage des câbles sont fermés à clé ;
- les répartiteurs et sous-répartiteurs sont équipés en systèmes anti-incendie (extincteurs automatiques à eau ou *sprinklers*) ;
- rien d'autre n'est stocké sur place (si ce n'est de la mort au rats… mais pas les guirlandes de Noël !) ;
- les clés sont en possession des personnes habilitées et d'elles seules ;

- l'éclairage est suffisant dans les cabinets ;
- la séparation avec le réseau informatique, qui utilise souvent les mêmes installations, est faite correctement – en effet, ce dernier peut dégager de la chaleur car il est actif ;
- l'accès aux goulottes y est suffisamment restreint.

Le cheminement du câblage doit être connu et documenté, les entrées dans les locaux et « têtes télécom » (points d'arrivée des fils) localisées sur un plan du bâtiment.

Câbles extérieurs

Les câbles externes ne dépendent pour l'essentiel pas de la société, mais de l'opérateur télécom. C'est souvent le point faible de la chaîne qui relie l'autocom de l'entreprise au central de l'opérateur ou à divers POP (points de présence). Il faut donc surveiller certains aspects, même s'ils ne sont généralement pas du ressort de l'entreprise :

- les tempêtes, la glace ou la neige peuvent endommager les lignes aériennes : une inspection sur place permet au moins de comprendre le risque ;
- les accidents de véhicules contre des poteaux téléphoniques peuvent eux aussi affecter les lignes ;
- les lignes enterrées sont soumises aux aléas des travaux publics (voir page 166 l'anecdote du pont de Suresnes).

L'entreprise peut demander ou l'opérateur téléphonique proposer des cheminements séparés. Il faut alors étudier par où les câbles passent et comment effectuer la séparation : quelle distance y a-t-il entre les câbles, quels sont les points de regroupement, comment se font les passages de rivières, etc. ?

Le fait de passer par un deuxième opérateur n'est pas une garantie, car ce dernier peut fort bien emprunter une ligne louée auprès du premier opérateur. Il peut donc être utile de se renseigner sur tous ces points et, pourquoi pas, de parcourir en voiture le trajet emprunté par les câbles.

Quant aux opérateurs mobiles, ils encourent des problèmes du même ordre, à ceci près que certaines portions de câblage sont remplacées par des ondes hertziennes dont la fiabilité va dépendre des pylônes, des antennes, des émetteurs et d'autres matériels informatiques. La téléphonie mobile est également sensible aux intempéries, des vents forts pouvant, par exemple, endommager les antennes.

Autocommutateur

L'autocommutateur accueille les lignes téléphoniques externes et distribue les appels sur d'autres liens internes. Associés à l'autocommutateur, on trouve souvent d'autres matériels tels que des serveurs interactifs de réponse vocale, des boîtes vocales, des répondeurs, des systèmes de routage d'appels, des moyens de conférence, etc.

Il faut alors procéder comme pour une petite salle informatique, en vérifiant les points suivants :

- la liste des équipements, avec descriptions et numéros de série ;
- les contacts et numéros du service de maintenance, en cas de panne ;
- les sauvegardes qui doivent avoir été faites et leur lieu de conservation ;
- des éléments tels que les alimentations électriques secourues, les alarmes en cas de dépassements de température ou de taux d'humidité ;
- la sécurité d'accès : les clés du local de l'autocom (fermé à clé) doivent être en possession de quelques personnes responsables identifiées ;
- les systèmes anti-incendie : ceux-ci doivent être prévus et leurs tests avoir été exécutés et notés.

La similitude avec la salle informatique ne s'arrête pas là : il est en effet possible de louer un autocom de secours qui peut être amené dans un conteneur et connecté au réseau de l'entreprise. Ce type de contrat peut avoir été prévu en secours (voir le chapitre 3).

La similitude avec les pratiques des informaticiens est cependant faible, la téléphonie restant un monde à part.

Réseau informatique

Le réseau informatique du lieu de travail se décompose lui aussi en trois parties, qui présentent une analogie forte avec la téléphonie :

- le réseau local (LAN – *Local Area Network*), proche du poste de travail des employés ;
- des matériels de commutation ou de routage, des contrôleurs de réseau, des serveurs bureautiques ou d'impression, des imprimantes départementales, situés en général dans de petites salles ou des sites appropriés dans les locaux ;
- le réseau externe à l'entreprise, pour lequel les commentaires sont les mêmes que précédemment pour la téléphonie.

Le réseau fédérateur (*backbone*) de l'entreprise, présent en salle informatique, est traité dans le chapitre 8.

Réseau local (LAN)

Le *Local Area Network* (LAN) est le réseau interne aux bureaux qui connecte les postes de travail aux divers équipements utiles.

Comme on l'a vu plus haut, une partie du câblage du réseau interne à l'entreprise, de même que certains moyens de répartition, est souvent très voisine physiquement de la téléphonie. Les mêmes remarques s'appliquent donc en ce qui concerne les goulottes, les cabinets de répartiteurs, etc.

L'apparition de la téléphonie sur IP transforme le téléphone en véritable terminal Internet branché sur le LAN. Ce téléphone a toutefois besoin d'une alimen-

tation électrique qui est souvent fournie par le LAN lui-même, moyennant des aménagements. Cela ajoute un risque dont il faut tenir compte dans les armoires de câbles.

En règle générale, il faut contrôler :

- les cheminements des câbles et leur protection ;
- les installations de répartiteurs, ou sous-répartiteurs, avec des documents à jour, des plans clairs, des terminaisons identifiées ;
- les salles ou placards utilisés, qui doivent être fermés à clé, les clés étant disponibles auprès de personnes clairement identifiées ;
- les moyens anti-incendie, inspectés régulièrement avec une preuve de l'inspection.

Serveurs bureautiques

Les serveurs bureautiques complètent le poste de travail (PC) de l'utilisateur et conservent des documents (fichiers Word, Excel, etc.), permettant de fournir du stockage local ainsi que des moyens d'impression et de messagerie, par exemple. Leur défaillance empêche, entre autres, l'accès des utilisateurs à leurs documents, l'échange de messages et l'impression. Ces serveurs sont considérés de plus en plus souvent comme critiques par les entreprises.

La pratique qui consistait à installer ces serveurs bureautiques près des photocopieuses ou des machines à café a vécu. Les grandes orientations actuelles consistent à déplacer et consolider ces serveurs, en fonction de leur mission :

- sur des NAS (voir le chapitre 8), pour les serveurs de fichiers, souvent déplacés dans un centre informatique ;
- sur de gros serveurs de messagerie (en grappe ou redondance), situés en général dans un centre informatique ;
- sur de petits serveurs dédiés aux impressions avec une imprimante locale, départementale ou multifonction proche des utilisateurs.

Au vu de ces évolutions, les serveurs bureautiques rejoignent les serveurs de stockage associés au centre informatique. Ils bénéficient alors de toute l'infrastructure et des systèmes de sauvegarde du centre.

Si l'entreprise utilise encore des serveurs bureautiques délocalisés, il faut alors :

- identifier les administrateurs et les responsables ;
- s'assurer qu'il n'y a pas de surchauffe ou d'anomalies d'environnement (vibrations, humidité hors norme) ;
- s'il y a des sauvegardes, s'assurer qu'elles sont bien réalisées et entreposées en lieu sûr ;
- s'il y a des imprimantes, limiter la quantité de papier entreposée près des machines, qui constitue un risque supplémentaire d'incendie.

Le poste de travail

Le poste de travail de type PC a une importance variable dans l'informatique générale de l'entreprise. Historiquement, l'informatique est apparue bien avant le PC et utilisait des terminaux passifs. Les premiers PC ne servaient qu'à la bureautique et leur connexion réseau entre eux et aux serveurs ne s'est faite que progressivement. Aujourd'hui, l'utilisateur ne connaît plus l'informatique que par son PC.

Une importance variable

Au sein de l'entreprise, plusieurs usages du PC cohabitent à des degrés divers.

- Avec les architectures dites « client-serveur », le PC a acquis une importance nouvelle : il devient dépositaire d'une partie des applications de l'entreprise, dont certaines sont critiques.
- Le PC est toujours la base des applications bureautiques (traitement de texte, tableur) qui sont de plus en plus intégrées dans le système d'information de l'entreprise.
- Le PC est très souvent aussi un « client lourd » de messagerie, dépositaire de la boîte aux lettres de son utilisateur.
- Il est quelquefois utilisé en tant que client léger ou simple navigateur web, auquel cas il peut être remplacé par des terminaux légers.
- Les données qu'il manipule sont présentes soit sur son disque dur, soit sur un serveur de fichiers local de l'entreprise (voir NAS ou serveur de fichiers dans le chapitre 8), soit sur un serveur central au centre informatique.

Le PC est donc dépositaire d'une partie plus ou moins importante des données vitales de l'entreprise. Même si cette part est actuellement en diminution, car on préfère centraliser le stockage sur des moyens plus sûrs, on ne peut pour autant l'ignorer.

Par ailleurs, en tant que poste de travail commun, les accès aux serveurs et applications centralisés de l'entreprise passent par le PC, sa perte empêchant donc tout travail sur l'informatique.

Enfin, certains utilisateurs créent, modifient et suppriment sur leur PC des données vitales pour l'entreprise. Cette pratique quelque peu dangereuse existe par exemple dans certains services financiers où des données ainsi gérées sont injectées dans des outils de reporting comptable. Ces données présentent un risque (pas uniquement en termes de continuité, d'ailleurs) qu'il faut identifier. On les appelle « données utilisateurs » (*user data*).

Se prémunir contre la perte du PC revient donc à protéger des données, protéger des applications et permettre de continuer à travailler malgré tout.

Protection des données

Trois niveaux de protection sont généralement pratiqués en ce qui concerne les données manipulées sur PC .

1. **Aucune protection** : si le PC est détruit ou si le disque dur est hors service, la donnée est détruite ou plus exactement perdue.
2. **Protection locale** : l'utilisateur dispose d'un graveur de DVD, d'un enregistreur sur cassette ; les données qu'il veut conserver sont ainsi sauvegardées localement.
3. **Protection par le réseau** : les données du PC sont conservées sur un serveur NAS ou autre, où les sauvegardes sont organisées.

En matière de continuité d'activité, il est important pour l'entreprise de s'assurer que les sauvegardes sont effectuées convenablement. Si ce n'est pas le cas, il faut modifier la manière de faire en généralisant la protection par le réseau (cas n° 3).

Protection des applications

Pour les applications utilisées sur PC, le même schéma se retrouve à quelques détails près.

1. **Aucune protection** : en cas de perte, l'application n'est a priori pas récupérable.
2. **Protection locale** : le CD d'installation a été conservé et on peut réinstaller localement l'application perdue.
3. **Protection par le réseau** : en cas de perte, l'application peut être téléchargée et réinstallée à partir d'un lieu de conservation central.

Il est clair que les pratiques sont à étudier pour vérifier que les applications vitales de l'entreprise se trouvent bien dans le dernier cas (sur le réseau). Une amélioration des pratiques est à envisager sérieusement si ce n'est pas le cas.

Certaines entreprises limitent la protection locale (cas n° 2) au strict minimum, voire l'interdisent, cette pratique de « bricolage » local étant jugée dangereuse. Certains outils sont capables, à partir du réseau, de détecter des applications installées localement et de les désactiver après avoir averti un administrateur.

Comment continuer à travailler ?

Pour pouvoir continuer à travailler en cas de sinistre, l'utilisateur aura besoin de récupérer ses données et ses applications locales. Cela est réalisable dans les cas suivants :

- lorsque celles-ci sont accessibles via le réseau (cas n° 3 ci-dessus) et que le réseau est en état ;
- lorsque celles-ci sont récupérables via un support correctement conservé – même si le contexte est plus difficile et aléatoire ;

- lorsqu'aucune donnée ou application n'est conservée en local (cas du terminal léger) : l'utilisateur n'a alors besoin que de se connecter au serveur.

Tout dépendra donc de la disponibilité du réseau et des accès aux serveurs.

D'autre part, l'utilisateur a besoin de récupérer son outil de travail : un PC similaire à celui qu'il a perdu, ou bien un terminal léger. Il faut donc conserver un stock de PC prêts à l'usage et assez voisins des PC qu'ils remplacent. Ce type de stock est assez souvent prévu dans les contrats de maintenance améliorée, où il s'agit de remplacer un PC en panne dans un délai rapide que la maintenance standard ne permet pas d'obtenir. Il faut alors bien vérifier que le cas du sinistre est prévu, la particularité dans cette situation étant en effet le nombre important de PC à changer d'un seul coup.

Le PC récupéré doit être conforme aux modèles (*masters*) de l'entreprise : il doit respecter certaines caractéristiques techniques physiques et logicielles, disposer d'un certain nombre d'applications pré-installées et configurées. De plus, sa sécurité doit être prévue en respect des normes de l'entreprise.

Pour récupérer un poste de travail, il est aussi possible de recourir à des portables stockés à l'abri ou de permettre à l'employé de travailler de chez lui avec son ordinateur personnel.

PC portables

Par rapport à ce qui précède, le portable possède un avantage – il peut être conservé à l'abri – et un inconvénient : il n'est pas connecté au réseau en permanence.

Le problème de la sauvegarde individuelle se pose davantage dans le cas des portables, où elle est plus facilement tolérée, pouvant d'ailleurs prendre des formes simples comme la gravure sur DVD ou la clé USB. Afin que le portable bénéficie des facilités de l'entreprise, il est indispensable de le connecter régulièrement pour sauvegarder sur le réseau son contenu et pour mettre à jour son système et ses applications.

D'autre part, en cas de sinistre, le portable a moins de chance d'en être victime (absent ou stocké dans un coffre). Mais s'il est sinistré, récupérer ses données sera plus difficile. Il est donc très important de sensibiliser son titulaire afin qu'il stocke ses données le plus souvent possible sur le réseau de l'entreprise ou sur un média amovible quand il se déplace.

Le PC portable possède une batterie qui le met à l'abri des coupures de courant. En revanche, en cas de stockage prolongé, il faudra penser à la charge et à la bonne santé des batteries.

Enfin, ce type de PC est beaucoup plus sensible au vol, à la perte ou à la destruction durant les déplacements.

Il existe des armoires spéciales pour conserver les PC portables. Certaines sont de véritables coffres forts, résistent au feu et permettent même de charger les batteries. Les solutions les plus évoluées autorisent aussi les connexions réseau

permettant des mises à niveau de logiciel, le tout alors que les PC portables se trouvent dans le coffre.

Travail à domicile

En cas de sinistre, il arrive que l'entreprise demande à ses salariés de travailler depuis leur domicile. L'outil de travail utilisé peut varier :

- cela peut être un PC portable prêté par l'entreprise que le salarié se procure au bureau ou conserve chez lui ;
- cela peut être un PC fixe qui, en général, appartient à l'employé mais sur lequel l'employeur a installé certains logiciels.

Généralement, pour être efficaces, ces PC sont connectés à Internet de diverses manières et peuvent accéder à certains serveurs de l'entreprise. En cas de sinistre, cette solution peut permettre de gagner du temps : l'employé rentre chez lui et accède à des applications d'entreprise ou à des services loués chez un tiers, pour la messagerie par exemple.

Ce type de travail particulier éveille des questions relatives aux équipements de travail à la maison, à la responsabilité et aux coûts, qui doivent être définies clairement à l'avance entre l'employeur et le salarié, voire figurer dans le contrat de travail. Les coûts liés aux communications doivent être pris en compte et l'employeur fournir un service approprié de support technique. Question sécurité, c'est à l'entreprise de prendre les mesures qui s'imposent pour assurer la protection des données utilisées et traitées par le travailleur à distance (achat de logiciel spécifique, mise en place d'un système de sécurité d'accès au serveur de l'entreprise, mode terminal ou client léger, etc.). De son côté, le télétravailleur doit respecter les règles de l'entreprise le concernant : confidentialité, restriction à l'usage des équipements ou outils informatiques, etc.

Les ressources humaines

« Il n'est de richesse que d'homme », dit le proverbe. L'entreprise ne doit donc pas négliger de prendre en considération les ressources humaines dans son approche de la continuité. Cela concerne les employés comme les prestataires externes.

Deux approches différentes sont envisageables, l'employé pouvant être victime d'un sinistre ou, à l'inverse, être de son fait à l'origine d'un sinistre ou d'une interruption d'activité (malveillance ou erreur humaine).

La malveillance

Parmi les actions malveillantes dommageables à la continuité de l'activité, on trouve :

- le départ de personnel provoquant des manques de compétence graves ;

- l'arrêt de travail en production avec ou sans blocage d'éléments importants pour la continuité de l'entreprise ;
- le vandalisme, d'ampleur variable, commis par des éléments intérieurs à l'entreprise ;
- le terrorisme ou sabotage ;
- l'effacement, volontaire ou non, de données, logiciels ou systèmes ;
- le vol de documents importants pour la continuité de l'entreprise ou la sécurité ;
- des saisies de données volontairement fausses, des lancements de programmes inexacts ou avec de mauvais paramètres dans l'intention de nuire ;
- les modifications volontaires de comportement de logiciel, les virus informatiques, etc.

Plus proches de la thématique de la sécurité, ces considérations touchent là à la limite du sujet de cet ouvrage. Des listes plus approfondies de ces menaces sont disponibles auprès des associations professionnelles qui ont développé des approches de la sécurité et des parades (comme le Clusif avec Mehari, par exemple : voir en annexe 1).

En règle générale, la pratique face aux actes de malveillance consiste à :

1. détecter les postes sensibles et connaître les personnes qui les occupent ;
2. accorder des droits d'accès précis et sécurisés pour les employés à ces postes (logons informatiques, accès à des salles, accès à des listings imprimés, etc.) ;
3. suivre et tracer tous les événements ayant lieu sur ces postes, avec des journaux informatiques par exemple, des mains courantes, des enregistrements vidéo (internes et externes) ;
4. mettre en place des contrôles réguliers (par la hiérarchie, la DRH…) ;
5. s'assurer autant que possible que les actions malveillantes éventuelles ne sont pas irrémédiables et peuvent être récupérées (par des sauvegardes et des secours divers) ;
6. enfin , étudier les contrats d'assurance pour vérifier comment la malveillance y est incluse.

Tout ceci doit bien sûr s'effectuer dans le respect de la législation.

L'aide aux victimes

Dans les cas où les ressources humaines sont victimes du sinistre, on pensera alors :

- aux premiers secours, bien évidemment ;
- à l'assistance psychologique à mettre en place ;
- aux aides familiales auprès des proches ;
- aux compétences et remplacements à prévoir ;

- à la communication des événements ;
- à établir des listes précises des victimes ;
- à la fatigue de ceux qui travaillent ou assistent au sauvetage ;
- à déterminer ce que l'on peut faire et ce que l'on doit faire et à demander de l'aide pour couvrir le décalage.

Chapitre 10

Le centre informatique

Avec les divers mouvements de consolidation des matériels informatiques de l'entreprise, le centre informatique se trouve dépositaire d'éléments très importants pour la disponibilité et la continuité des activités.

Le centre informatique lui-même possède une infrastructure particulière qu'il faut choisir et gérer avec soin afin de satisfaire aux objectifs de continuité de l'entreprise.

Choix du site

Idéalement au nombre de trois (primaire, secondaire et distant), les centres informatiques sont localisés sur deux sites : un premier site sur lequel sont organisés les centres primaire et secondaires en « duo » ou « campus » et un deuxième site à distance convenable, sur lequel on prévoit le centre de secours distant.

Cette dualité du premier site est un idéal que n'atteignent que les entreprises ayant un niveau d'exigence très élevé en matière de continuité d'activité. Les autres se contentent d'un site dit principal convenablement fiable selon leurs critères, doublé d'un site distant pour le secours.

Ce deuxième site à distance est considéré comme moins critique que le site principal. Toutefois, ce site distant est en réalité très souvent le site principal d'une autre branche de l'entreprise ou d'une autre société ; il est alors aussi critique que les autres. Le choix du site doit donc dans tous les cas de figure être effectué avec la plus grande attention, à base de critères raisonnés.

L'appréciation des risques présentée dans le chapitre 1 a donné une liste des principaux facteurs à prendre en compte, à laquelle on se reportera. Lors du choix d'un site pour y créer un centre informatique, il est ainsi possible de sélectionner un emplacement permettant de minimiser ces risques. L'approche est tout de même délicate, car il faut trouver des compromis : un site idéalement situé, loin des tremblements de terre et des inondations, s'il est loin de toute

ville agréable et de toute université risque fort de n'attirer aucun employé compétent ! Il faut donc graduer les exigences et peser le pour et le contre de critères potentiellement contradictoires.

Vulnérabilité du site

On se reportera sur ce point au chapitre 1. Néanmoins, lorsqu'il s'agit de choisir une nouvelle implantation, il est intéressant d'évaluer aussi la vulnérabilité des différentes solutions possibles.

Pour un désastre donné, la vulnérabilité d'un site se mesure en pertes financières, mais aussi et surtout en pertes humaines. Sur ce deuxième point, il faut considérer un certain nombre de facteurs, tels que :

- la densité de population dans la zone considérée ;
- la compréhension scientifique du risque ;
- le niveau d'éducation et de sensibilisation du public ;
- l'existence de systèmes d'avertissement, de communication, d'alerte ;
- la disponibilité ou non d'infrastructures de secours et leur degré de préparation ;
- le respect des règles de construction, les pratiques locales ;
- certains facteurs culturels déterminant la réaction du public.

Tous ces points peuvent en effet jouer sur les comportements et donc sur les conséquences du sinistre.

Attractivité du site

Le site envisagé doit attirer des collaborateurs (le site totalement vide étant une vue de l'esprit) et offrir un environnement propice aux activités. Ce sujet sort du thème de cet ouvrage, mais citons néanmoins :

- l'existence de collèges, de lycées, d'universités ou d'écoles d'ingénieurs à proximité ;
- la qualité de vie (voir par exemple les classements faits par certaines revues du genre « les villes où il fait bon vivre ») ;
- l'évolution des populations (en baisse ou en hausse) ;
- la facilité à se loger sur place (à l'hôtel ou en logement fixe) ;
- le droit du travail et la protection sociale (pour les sites à l'étranger) ;
- la connaissance ou non des caractéristiques des lieux (la notion de zone inondable, zone à risque, etc. existe-t-elle sur place ?) et leur suivi dans le temps.

La continuité d'activité est en effet aussi une affaire de compétence et de motivation du personnel.

Climat des affaires

Le site doit se trouver dans un environnement propice aux affaires. Cela concerne aussi bien la situation économique et politique, mais vu sous l'angle de la continuité d'activité, on observe les points suivants :

- la présence de compagnies d'assurance et d'offres de contrats convenables ;
- une fourniture de qualité pour l'électricité, la téléphonie, le réseau ;
- la proximité des points d'accès réseau, ou des points de présence pour la fibre optique à haut débit ;
- la facilité à acquérir un terrain plus vaste que le simple centre informatique ;
- le coût de l'immobilier pour le site et les collaborateurs ;
- la possibilité d'obtenir des offres de services de secours, d'hébergement informatique, de conseil, etc.

En particulier lorsque l'on a choisi l'étranger, ces points peuvent s'avérer déterminants pour la bonne mise en œuvre d'un plan de continuité.

Règles de précaution

À titre de précaution, certaines règles sont généralement admises et respectées pour le choix d'un site, quelle que soit la ville ou le pays :

- être situé à plus d'un kilomètre de toute voie ferrée, autoroute, voie de passage de cargos, usine classée à risque ou usine de traitement des eaux ;
- être situé à plus de cinq kilomètres de tout aéroport ;
- être assez éloigné d'émetteurs radio ou radars puissants (qui normalement n'acceptent rien à proximité) ;
- être à distance « suffisante » d'une centrale nucléaire, à apprécier selon les pays… ;
- ne pas être trop éloigné d'un poste source électrique (moins de cinquante kilomètres), les défauts d'alimentation électrique étant souvent proportionnels à cette distance ;
- se tenir en dehors de toute zone inondable, loin de l'aval d'un barrage ;
- avoir accès facilement à l'eau potable et à de l'eau en général pour refroidir ou éteindre un incendie.

Bien évidemment, si ces règles sont valables lorsqu'on choisit le site, elles peuvent ne plus s'appliquer ultérieurement.

Il est souhaitable, dans la logique du plan de continuité, de déterminer les critères jugés valables par la direction, de leur accorder un certain poids, puis de les évaluer ou faire évaluer. Les notes obtenues permettent alors de départager les sites candidats.

Infrastructure du centre informatique

Le centre informatique accueille des éléments critiques tels que des serveurs, des réseaux, du stockage, etc. Il permet leur fonctionnement mais peut aussi provoquer des pannes diverses et variées dont certaines sont de mode commun (voir le chapitre 7) et donc préjudiciables à la continuité.

Éléments critiques

Les éléments du centre informatique pouvant connaître des pannes préjudiciables à la disponibilité sont nombreux : les contraintes en termes de fiabilité et de sécurité portant dessus sont à étudier soigneusement. On peut citer en particulier :

- la chaîne des alimentations électriques qui doivent être redondantes, protégées et que l'on doit pouvoir couper par sections ;
- les capacités à générer du courant électrique en cas de coupure (batteries, alternateurs, générateurs Diesel ou fioul) doivent être dimensionnées correctement en puissance, qualité de courant et durée de production ;
- la climatisation doit être suffisamment fiable et adaptée aux calories à évacuer et sa maintenance ne doit pas nécessiter l'arrêt général ;
- les éventuels points chauds de la salle doivent être détectés et refroidis localement, la température des éléments sensibles (serveurs) surveillée ;
- les filtrations d'air doivent aussi maintenir le bon taux d'humidité ;
- les systèmes de sécurité d'accès et de surveillance vidéo doivent permettre la traçabilité des accès dans le respect des lois ;
- les systèmes de détection et de sécurité incendie peuvent éviter des dommages importants : leur bon état de fonctionnement doit être vérifié régulièrement ;
- les planchers et faux planchers doivent pouvoir supporter le poids des machines (qui évolue à la hausse) ;
- les canalisations d'eau doivent éviter toutes les zones où une fuite serait catastrophique ;
- les câbles électriques et de réseau SAN, IP, etc. doivent suivre des cheminements distincts ;
- les interventions de maintenance doivent pouvoir se faire en perturbant le moins possible l'ensemble ; dans certains cas, il faut prévoir des bipasses.

En résumé, un centre informatique est un ensemble de technologies diverses qui doit avoir fait l'objet d'une étude d'ingénierie de conception visant à une bonne disponibilité et à une réparabilité aisée.

Référentiels et normalisation

Durant les années 2000-2005, des travaux concourants ont abouti à un ensemble de bonnes pratiques pour la conception et l'aménagement des centres informa-

tiques. Des comités d'utilisateurs ou de normalisation se sont penchés sur le sujet, tels que le *Uptime Institute* aux États-Unis ou la *Telecommunications Industry Association* (TIA), auteur de la norme TIA 942.

Ces travaux ont classé le niveau de service d'un centre informatique en quatre catégories (*tiers* en anglais), du plus faible au plus élevé. Le tableau suivant présente quelques caractéristiques de ces quatre catégories ou classes.

Tableau 10-1 : Les quatre classes du centre informatique, selon le Uptime Institute

Classes	Caractéristiques principales
1	– alimentation électrique sur une voie – refroidissement sur une voie – nombreux points uniques de défaillance – pas de générateur électrique si autonomie électrique de huit minutes – vulnérable aux intempéries – indisponibilité inférieure à 28,8 heures par an
2	– alimentation électrique sur une voie – refroidissement sur une voie – quelques composants redondants – générateur de secours – supporte 24 heures de coupure de courant – quelques critères de choix de site – salle informatique formellement séparée – indisponibilité inférieure à 22 heures par an
3	– alimentation électrique et refroidissement sur plusieurs voies dont une seule active – alimentation et refroidissement redondants – fournisseurs de service doublés – supporte 72 heures de coupure de courant – critères élevés de choix de site – résistance au feu : 1 heure – permet la maintenance à chaud (concurrente) – indisponibilité inférieure à 1,6 heures par an
4	– alimentation électrique et refroidissement sur plusieurs voies actives – composants généralement redondants – tolérance aux pannes – supporte 96 heures de coupure de courant – critères très exigeants de choix de site – résistance au feu d'au moins 2 heures – sécurité physique de haut niveau – équipe de maintenance présente 24h/24 7j/7 – indisponibilité inférieure à 0,4 heure par an

Bien évidemment, un site donné peut se trouver en classe 3 sur un thème et en classe 1 sur un autre. C'est cependant le plus bas (donc 1) qui l'emporte car la

chaîne de disponibilité prend la valeur du maillon le plus faible. Dans la pratique, nombre de fournisseurs ne pouvant prétendre complètement à la classe 4 (car il leur manque certains éléments) mais estimant être meilleurs que la classe 3 qualifient leur centre informatique de « 3+ ».

Il existe certaines différences d'approche et de contenu entre le U*ptime* I*nstitute* et la TIA 942. Pour plus de détails, se référer aux documents cités en annexe 2.

Lorsque l'entreprise a recours à un prestataire externe pour son centre informatique, elle a tout intérêt à spécifier dans son cahier des charges des références aux « classes » définies par ces normes.

Les principaux risques et leur parade

Un centre informatique est exposé, comme tout bâtiment, aux risques habituels que sont l'incendie, l'inondation, la foudre, etc. Le fait qu'il héberge des éléments critiques pour l'activité de l'entreprise et détienne des informations sensibles en stockage exige une démarche orientée dans deux directions :

- un niveau de protection ou de prévention élevé ;
- une capacité réelle à limiter les conséquences.

Lorsqu'on conçoit un centre à partir de zéro, il est possible de jouer sur les deux tableaux, et en particulier sur la prévention. Lorsque le centre existe déjà, en revanche, les menaces sont déjà présentes et il faut alors en limiter les conséquences éventuelles.

Incendie

Le feu, dans un centre informatique ou ses annexes, peut avoir des conséquences graves, dont certaines sont difficiles à percevoir immédiatement.

Dégâts

Les dégâts d'un incendie sont directs et évidents : pertes de stocks et de documents, destruction de biens et de réserves diverses, dommages causés par l'eau nécessaire à l'extinction du feu, locaux devenus impropres à leur usage, etc.

Mais d'autres dommages atteignent le centre informatique de façon beaucoup plus pernicieuse :

- affaiblissement de certaines structures du bâtiment telles que des poutres ou des murs ;
- destruction de cloisons ou vitrages, rendant nulles les isolations de zones à risque ;
- dégâts peu visibles dans les faux planchers, les gaines surélevées de passage de câbles, les systèmes de climatisation… ;
- détérioration importante des isolants des câbles, devenus impropres à leur usage et risquant de provoquer des courts-circuits ;

- problèmes dus aux fumées et émanations toxiques.

En outre, les incendies peuvent avoir des effets indirects qui s'apparentent à des pannes de mode commun : ainsi, si une coupure générale de l'alimentation électrique est requise et que les générateurs Diesel sont interdits de fonctionnement, aucun serveur ne pourra fonctionner. Si, de plus, la connexion réseau vers l'extérieur du site est hors service, ces situations peuvent mettre en danger toute action de reprise sur un site voisin ou éloigné et réduire ainsi à néant toute stratégie de continuité.

Parades

Les parades à mettre en place sont de plusieurs natures. Les listes données ci-après ne prétendent pas être exhaustives mais sont particulièrement adaptées au contexte du centre informatique.

Prévenir

Des actions élémentaires de respect de certaines règles se révèlent très efficaces en termes de prévention :

- ne pas laisser dans une zone à risque des cartons d'emballage, du polystyrène et autre combustible – lorsqu'une machine est déballée, son emballage doit être sorti de la salle et mis en un lieu prévu à cet effet ;
- organiser le stockage des réserves de papier pour imprimantes de manière à ne pas fournir de combustible au feu ;
- respecter les recommandations des constructeurs pour les alimentations électriques des machines et les sections de câblage ;
- inspecter les câbles électriques, changer immédiatement tout câble dénudé, toute connexion noircie ou suspecte ;
- faire respecter les interdictions de fumer (le mégot mal éteint est une cause importante d'incendie) ;
- réglementer l'usage des chauffages électriques d'appoint, des machines à café et de tout autre appareil qui maintient une température élevée ;
- éliminer de la salle informatique et de ses abords tout ce qui peut constituer un combustible ;
- respecter et faire respecter la réglementation en vigueur ;
- faire visiter les locaux par les services incendies (un expert des pompiers, par exemple) pour obtenir un état des lieux et éventuellement connaître les risques du voisinage ;
- séparer les cheminements de câbles conducteurs de courant fort de ceux transmettant du courant faible ;
- passer une fois par an l'aspirateur dans le dessous des faux planchers ;
- inspecter les goulottes de câbles en nettoyant tout ce qui n'a pas à s'y trouver.

Réagir

Dès les premières flammes, il faut réagir. Certaines réactions permettent de réduire les dégâts, voire d'arrêter le feu avant qu'il y ait sinistre. Les actions suivantes peuvent contribuer à encourager les bons comportements :

- mettre en place des extincteurs appropriés aux différentes natures de feux possibles, les garder en bon état par une maintenance régulière et indiquer clairement leur emplacement ;
- former régulièrement le personnel au bon usage des extincteurs avec des exercices pratiques ;
- mettre en place les détecteurs appropriés capables de déclencher l'alarme ;
- concevoir un déclenchement d'alarme correct, capable d'entraîner des actions telles que :
  - fermer des portes coupe-feu,
  - activer des systèmes d'extinction,
  - prévenir les secours,
  - ouvrir les verrous électroniques de portes pour permettre les évacuations,
  - alerter le personnel d'évacuation,
  - éventuellement, arrêter des machines sensibles ;
- s'équiper en systèmes d'extinction qui conviennent à l'environnement d'une salle informatique (gaz neutre non mortel, conforme aux normes) ;
- déterminer les éléments sensibles en cas d'incendie (cassettes, bandes, documents) et prévoir un stockage approprié (coffre ignifugé, par exemple) ;
- poser des affiches et communiquer sur le comportement à adopter en cas d'incendie ;
- faire des exercices d'évacuation du centre ;
- tester les équipements.

Dans tous les cas, la méthode la plus efficace consiste à détecter le plus tôt possible l'incendie, en prévenant des personnes formées qui organisent les actions prévues, tout en ayant sensibilisé le reste des employés.

Dégât des eaux

Sous cette appellation générique, on trouve des sinistres d'importance variable susceptibles d'affecter le centre :

- inondations avec des conséquences pouvant aller jusqu'à rendre un centre totalement inutilisable ;
- pluies importantes avec des ruissellements, des infiltrations de toiture ou de façade provoquant des dommages au bâtiment, aux machines et aux stocks en générant des infiltrations ;
- infiltrations ou fuites provoquant des dégâts que l'on ne découvre pas forcément tout de suite, mais qui détériorent des sous-ensembles du centre ;

- condensations localisées qui rongent des conduites, abîment lentement des revêtements ou des plafonds, provoquent des courts circuits.

Conséquences

Les effets des dégâts des eaux sont directs et indirects, de même que les parades seront immédiates et différées.

- **Effets directs** : la présence de l'eau empêchant toute activité dans le centre, il faut réagir immédiatement en pompant l'eau et en la déversant en contrebas, si c'est possible, ou dans un bac étanche ;
- **Effets indirects** : une fois l'eau évacuée, le centre connaît des moisissures, des courts-circuits, etc. ; il faut assécher les murs, détruire et reconstruire des cloisons, ôter et reposer les tapisseries, les moquettes, le câblage électrique et téléphonique – cela peut prendre plusieurs semaines pendant lesquelles le centre est inutilisable.

Les effets des dégâts des eaux peuvent aller bien au-delà de ce qu'on imagine en première analyse et il n'est pas rare de découvrir, une fois les eaux évacuées, des pannes diverses sur des systèmes qui ont été endommagés par un séjour dans l'eau ou par un simple degré d'humidité trop élevé.

Précautions à prendre

Lorsqu'on peut décider de l'implantation d'un centre, les précautions déjà mentionnées plus haut consistant à éviter toute zone inondable s'imposent. Pour tous les autres cas, il est intéressant d'envisager les solutions suivantes pour la prévention et la réaction en cas de sinistre :

- prévoir des bassins d'expansion situés plus haut que le centre et se fournir en pompes de relevage d'un bon débit ;
- drainer les alentours du centre et en améliorer l'étanchéité ;
- surélever la partie la plus sensible du centre ;
- ne pas faire passer de canalisations d'eau au-dessus d'éléments sensibles ;
- si le centre possède un système de refroidissement à eau, en prévoir la circulation en niveau bas ;
- prévoir des systèmes anti-fuite ou de coupure en cas de fuite sur les canalisations ;
- prévoir des bipasses et des pièges à froid pour pouvoir changer les vannes défectueuses ou certaines pompes sans avoir à tout interrompre ;
- pour tout système (climatiseur, canalisation froide) qui risque l'humidité ou la condensation, prévoir une récupération de l'eau ainsi produite par bac ou lèchefrite ;
- laisser les canalisations apparentes et accessibles de manière à ce qu'on puisse les inspecter facilement.

Par ailleurs, il est important de tenir compte du fait que l'inondation mène la plupart du temps à une coupure électrique. Il est donc judicieux d'avoir conçu le

centre de manière à ce que les systèmes les plus sensibles soient mis hors d'atteinte de l'eau avec une alimentation par batteries et/ou générateur Diesel, eux-mêmes hors d'eau.

Dysfonctionnements électriques

L'alimentation électrique est indispensable pour tous les moyens informatiques du centre. Ses défauts sont ainsi fortement préjudiciables au bon fonctionnement des machines.

Défauts courants

Parmi les défauts courants de l'alimentation électrique, on peut noter :

- les variations de tension, les microcoupures ;
- les parasites ou courants induits (par les ballasts de tubes fluorescents, par exemple) ;
- des perturbations diverses en fréquence ou des défauts dus à des onduleurs de qualité médiocre ;
- les problèmes de références de potentiels multiples et d'électricité statique ;
- la foudre qui génère des courants pouvant avoir des conséquences destructrices à distance.

Les divers équipements réagissent de manière variable à ces défauts. Certains équipements industriels vont d'ailleurs eux-mêmes en générer. Si le centre est voisin d'une usine équipée de machines électriques (gros moteurs électriques, appareils de soudure électrique), il faudra être particulièrement vigilant.

Précautions à prendre

Parmi les précautions utiles à prendre, citons les actions suivantes :

- séparer les matériels sensibles comme les serveurs ou les routeurs de réseau des matériels perturbateurs (moteurs électriques, par exemple) ;
- prévoir des transformateurs ayant la puissance nécessaire ;
- généraliser la mise au neutre ;
- choisir des câbles de qualité et s'assurer que leur pose a été effectuée correctement ;
- prévoir des cheminements de câbles évitant les perturbations émises ;
- séparer le passage des alimentations nominales de celui de l'alimentation de secours (précaution générale : voir les chapitres précédents) ;
- vérifier régulièrement les connexions.

Moyens techniques

Pour améliorer la qualité du courant apporté en salle informatique, il est possible de recourir à des dispositifs tels que des onduleurs ou des moteurs électriques à volant d'inertie doublés de batteries. En général, ces moyens permettent

d'atténuer les défauts du courant d'origine publique et de pallier à certaines coupures de courte durée (dix minutes).

Pour des coupures de plus longue durée, il faut avoir les moyens de générer soi-même du courant, via des générateurs Diesel ou à gaz. Les onduleurs à batterie doivent assurer le relais jusqu'à ce que ceux-ci entrent en action.

Quant à la foudre, elle nécessite une protection technique par paratonnerre en particulier. On utilise aussi les parafoudres pour protéger l'installation électrique et les lignes de transmission de données, la fibre optique étant à préférer dans ce cas.

Enfin, l'électricité statique peut se révéler dangereuse dans le cas des opérateurs intervenant sur les serveurs et touchant des éléments sensibles (cartes mères, processeurs) qui peuvent se trouver gravement endommagés. Il faut régler correctement l'hygrométrie de la salle, poser des revêtements antistatiques au sol et porter des vêtements en textiles ne produisant pas d'électricité.

Pour tous ces moyens techniques concourant à la bonne disponibilité du centre, il faut prévoir une surveillance correcte et un contrat de maintenance permettant la remise en route rapide, incluant des pièces de rechange si nécessaire.

Autres risques

Enfin, un centre informatique est exposé à d'autres risques encore que ceux qui ont été étudiés précédemment.

Défaut de climatisation

La climatisation peut tomber en panne, que ce soit en raison d'une coupure électrique (déjà mentionnée) ou pour des raisons plus particulières, telles que :

- des fuites de liquide réfrigérant ;
- des pannes de ventilateurs ou d'aéro-réfrigérant externe ;
- l'exposition à un rayonnement solaire direct trop élevé.

Dans tous les cas, la température monte et atteint des zones impropres au bon fonctionnement des machines, serveurs, stockage, etc. Les mesures préventives consistent alors à prévoir des redondances des systèmes de climatisation (de type n+1), à doubler les alimentations et à surveiller et maintenir ces systèmes.

En cas de défaillance totale, l'arrêt des machines sensibles ou responsables des plus gros dégagements de chaleur est à prévoir rapidement.

Il existe aussi un risque plus récent d'insuffisance chronique de refroidissement dans certains endroits de la salle informatique où sont concentrés certains serveurs qui dégagent plus de calories que la moyenne. La parade face à ce problème consiste alors à :

- ne pas remplir complètement les racks de machines ;
- disperser dans la salle les machines ou groupes de machines de ce type ;
- prévoir des compléments ponctuels de refroidissement aux points chauds.

Ces technologies, qui concentrent la puissance informatique et donc par la même occasion le dégagement calorifique, peuvent amener à repenser la conception de l'ensemble de la climatisation de la salle ou à aménager une salle particulière.

Intrusions de personnel

L'entrée dans le centre ne doit être réservée qu'au personnel habilité. Il existe en effet différents risques :

- vols de matériel, de sauvegardes ;
- mise sur écoute, pose de bretelles télécom ;
- vandalisme, destructions diverses.

Une protection efficace sera apportée par :

- des mécanismes de contrôle d'accès simples (gardien) ou sophistiqués (identification et authentification par carte, etc.) ;
- la traçabilité des personnes entrant sur le site (nom, prénom, jour, heure, personne visitée) ;
- la difficulté d'accès dans le centre (portes verrouillées, absence de baies vitrées) ;
- une vidéosurveillance des alentours du site ;
- la mise sous protection des éléments sensibles comme les tableaux électriques, les moyens de coupure divers ou les répartiteurs télécom, qui ne doivent pas être accessibles au premier venu ;
- une procédure de contrôle à la sortie des employés emportant du matériel ou des sacs pouvant en contenir.

Pollutions diverses

Normalement, ces aspects ont dû être pris en compte dans le choix du site sur lequel le centre est installé. Cependant, pour les centres situés dans des zones industrielles ou à proximité d'un site industriel, il existe certains risques liés à la pollution :

- émanation de gaz dangereux pour le personnel ou le matériel ;
- poussières de diverses natures ;
- eau impropre à son usage.

Toutes ces atteintes toxiques peuvent se traduire par des problèmes de santé, des dysfonctionnements de matériel, des risques de courts-circuits ou d'incendie, des déclenchements d'alarme intempestifs, etc.

La parade pourra être apportée par :

- des filtrations adaptées ;
- des portes coupe-feu ;
- des clapets dans les gaines de circulation d'air ;
- des zones en légère surpression ;
- une protection des réserves d'eau.

PARTIE IV

La gouvernance de la continuité

Historiquement, les préoccupations de continuité d'activité sont apparues à divers endroits dans l'entreprise et à différents niveaux de son organigramme. Les démarches sont tantôt techniques, tantôt organisationnelles ; elles sont restées partielles, opportunistes et peu coordonnées.

Une prise de conscience au plus haut niveau est en train de s'opérer. Elle pousse les directions générales à considérer la continuité d'activité dans son ensemble et à mettre en place les éléments d'une bonne gouvernance qui sont traités dans les trois chapitres suivants :

- la politique de continuité (chapitre 11), dont l' objectif est de mettre en place une structure ;
- le lancement des actions d'élaboration du PCA et sa maintenance (chapitre 12) ;
- le contrôle ou la vérification de sa bonne exécution (chapitre 13).

Chapitre 11

La politique de continuité

Le mot « politique » – inexactement employé comme traduction de l'anglais *policy* – signifie ici « l'expression d'une volonté » de la direction générale de l'entreprise. Ainsi, ce terme recouvre aussi bien la volonté que l'expression : il s'agit donc d'un document actant des décisions, accompagné d'une communication interne à l'entreprise. Cette politique se traduit dans les faits par la mise en œuvre d'un plan de continuité.

Exprimer une volonté

La politique, en matière de continuité, correspond à une décision de la part de la direction générale de l'entreprise, qui exprime ainsi sa volonté et ses engagements.

La volonté de développer un plan de continuité d'activité est exprimée dans un document émis par la direction générale. Ce document, simple et facile à lire (cinq pages environ), sert de cadre général dans lequel toutes les actions ultérieures en termes de continuité d'activité pourront et devront s'inscrire. Voici un descriptif type de sa structure :

Politique de continuité d'activité

1. Résumé
2. Introduction
3. Conditions d'application
4. Objet
5. Périmètre
6. Décision
7. Bénéfices
8. Responsabilités
9. Références

1. Résumé

Le résumé permet d'annoncer l'essentiel en quelques lignes.

> **Exemples**
>
> « Les directeurs de branche doivent mettre en œuvre un plan de continuité d'activité. »
>
> « Les responsables de groupe doivent montrer qu'ils ont pris en compte l'obligation d'avoir un plan de continuité efficace. »
>
> « Les plans doivent être conçus, publiés et testés pour les activités jugées critiques. »

2. Introduction

L'introduction donne le cadrage général, ainsi qu'une description du contexte.

> **Exemples**
>
> « En termes de continuité d'activité, la société X a réalisé un plan de continuité qui nécessite une adaptation et un élargissement depuis son rachat par la société Y. »
>
> « Ce document exprime l'orientation générale de l'entreprise Z sur les deux ans à venir. »

3. Conditions d'application

Ici sont exprimées les conditions d'application de la politique de continuité : sa date d'entrée en vigueur, sa situation par rapport au passé, etc.

> **Exemples**
>
> « La présente politique s'applique à compter du jj/mm/aaaa. »
>
> « Elle annule le document émis précédemment. »

4. Objet

En fonction de la culture de l'entreprise et des travaux déjà réalisés, on précise ensuite l'objet précis de la politique.

> **Exemples**
>
> « Proposer une structure générale pour les actions de continuité à lancer. »
>
> « Développer des plans de continuité. »
>
> « Améliorer le plan de continuité et en étendre le périmètre. »
>
> « Dégager un budget pour les actions de continuité menées par les directions opérationnelles. »
>
> « Lancer une campagne de test des plans existants. »

5. Périmètre

Une fois l'objet déterminé, la politique précise le périmètre du plan de continuité, avec ses exclusions éventuelles.

> **Exemples**
>
> « Le périmètre est l'ensemble de la SA en France. »
>
> « Les principaux fournisseurs de logistique sont inclus dans le périmètre. »
>
> « Les filiales situées hors de l'Union Européenne ne font pas partie du périmètre. »

6. Décisions

Exprimant clairement et de façon structurée ce qui est décidé par la direction, cette section représente le cœur du document.

> **Exemples**
>
> « Les directeurs d'unités seront les responsables chargés de définir leurs activités critiques et le niveau de continuité désiré. »
>
> « La structure du plan de continuité suivra les modèles fournis par la norme PAS 56. »
>
> « Les directeurs de région mèneront des revues annuelles du plan. »
>
> « Des tests de simulation seront menés une fois par an dans les régions, sous la responsabilité des chefs de zone. »
>
> « Les contrats avec les prestataires devront inclure une clause *ad-hoc*. »

7. Bénéfices attendus

Il s'agit maintenant de justifier la décision. On trouve ici des arguments que l'on peut réutiliser pour expliquer ou justifier la démarche.

> **Exemples**
>
> « Amélioration du service rendu au client. »
>
> « Limitation des conséquences d'un sinistre sur les personnes, les biens et l'environnement. »
>
> « Rendre la reprise du travail plus efficace après un incident de type X. »

8. Responsabilités

La définition des responsabilités est importante pour encourager des comportements bien alignés.

> **Exemples**
>
> « Le responsable de la continuité rendra compte au comité directeur de l'état d'avancement des travaux. »
>
> « Le comité de continuité est dépositaire de la présente politique ; il signalera au comité directeur les éventuels aménagements à y apporter. »
>
> « Les responsables de branche sont responsables de la mise en œuvre du plan dans chacune de leur branche. »

9. Références

On indique ici les éventuelles normes à suivre ou les documents de politique ou directives d'une maison mère, par exemple.

Nommer un comité de pilotage

La direction générale désigne une structure de type « comité de pilotage » (ou COPIL) pour le plan de continuité. Comme la plupart du temps, ce plan n'existe

pas au départ, c'est cette structure qui se voit confier la mise en place ou la création d'un plan de continuité d'activité (PCA) en bonne et due forme.

Parmi les attributions de ce comité, on trouve :

- respecter et faire respecter les orientations de politique définies précédemment ;
- définir les objectifs du projet de mise en œuvre d'un plan de continuité d'activité ;
- fournir le support et les aides nécessaires au bon avancement du projet ;
- suivre l'avancement du projet (ce qui est accompli, ce qui reste à faire, risques encourus) ;
- décider des orientations et réorientations éventuelles du projet ;
- gérer le budget alloué au projet.

Ce comité se réunit régulièrement (toutes les semaines ou tous les quinze jours) et publie un compte rendu.

La responsabilité du projet en lui-même incombe à un directeur de projet qui fait souvent partie du comité de pilotage. Les différents chefs de projet rendant compte à ce directeur peuvent être rattachés à divers services. Il est judicieux d'employer pour ce projet particulier les mêmes structures de projet utilisées habituellement par l'entreprise. Enfin, il est indispensable que ce projet ne soit pas mené uniquement par des personnes sans expérience opérationnelle. Ils peuvent être détachés temporairement mais doivent avoir une bonne connaissance et habitude du terrain.

Chapitre 12

Construire et maintenir le plan de continuité

Suite à une décision de la direction générale, l'entreprise doit construire son plan de continuité en mode projet sous la maîtrise d'un comité de pilotage. Des actions de sensibilisation des employés l'accompagnent.

Une fois le plan de continuité mis en œuvre, la vie continue, l'entreprise évolue, les hommes changent. Or, pour être efficace, le PCA doit toujours rester d'actualité. C'est le but de la maintenance du plan.

Lancement du projet de PCA

Le projet de PCA doit être lancé par le comité de pilotage (COPIL) créé dans le cadre de la note de politique.

Un brin de cérémonial (du type réunion de lancement) est souvent utile pour marquer les esprits. Les opérationnels et les responsables d'unités doivent en effet savoir pertinemment qu'ils vont être mis à contribution et comprendre précisément ce que l'on attend d'eux.

> **Quiproquo au CoDir : l'informatique ne peut décider seule !**
>
> La société Méding lance un projet de PCA en France.
>
> Son approche part des équipes informatiques de production (au sens « exploitation »). À partir de modèles de questionnaires établis par sa maison mère dans un pays d'Europe, certains des responsables d'exploitation informatique établissent des questions précises sur les serveurs, avec différents critères de réponse. Ils demandent alors à des responsables de développement informatique de remplir les fameux questionnaires, ce qu'ils font sans trop se poser de questions.
>
> On obtient finalement des informations sur les temps possibles d'interruption des serveurs Uranus, Neptune et Saturne.
>
> En comité de direction (CoDir), le responsable du PCA félicite les responsables métiers d'avoir répondu aussi vite. Ceux-ci écarquillent les yeux, car bien que responsables de leur processus, personne n'est jamais venu les questionner sur la sensibilité au sinistre de leurs activités.

> Intrigué, le responsable du PCA enquête et découvre que personne n'a jamais demandé quoi que ce soit aux responsables d'activités et que pour eux, d'ailleurs, Uranus, Neptune et Saturne ne sont que des planètes !
>
> Ce quiproquo permet donc de recommencer l'opération selon une meilleure manière de faire : repartir des processus, observer les temps d'arrêt admissibles, puis traduire cela en termes informatiques. Le résultat constaté est alors fort différent : autres matériels, autres contraintes...
>
> **Moralité :** le personnel du service informatique ne peut et ne doit pas deviner à la place des opérationnels, alors que ces derniers ne connaissent pas l'effet de leurs demandes sur l'informatique – ce qui est somme toute normal ! Il faut donc veiller à consulter les responsables opérationnels au même titre que les techniciens.

Concernant la planification de projet et le reporting, il est conseillé d'employer les méthodes usuelles dans l'entreprise. En effet, mieux vaut sur ces points éviter d'apporter trop de nouveauté.

Formation et sensibilisation

Afin d'éviter bien des mésaventures sur un projet unique dans l'histoire de l'entreprise, il est bon d'avoir mis en place un programme de formation et de sensibilisation.

Ce programme pourra comporter plusieurs sessions allant de la sensibilisation générale à des formations plus approfondies destinées aux chefs de projets.

Formation des chefs de projet

Une session de formation pour chefs de projet peut comporter les aspects suivants :

Objectifs

- Donner aux participants des connaissances de base permettant de comprendre les approches et les enjeux de la continuité d'activité (CA).
- Permettre aux responsables d'expliquer et d'initialiser correctement une démarche CA dans l'entreprise.
- Fournir une méthode pour aborder la CA en entreprise et aboutir à la réalisation d'un PCA.

Contenu

- **Introduction** : développement d'un PCA (étapes importantes, documents types, principaux concepts, définitions).
- **Construction du PCA :**
  - *Maîtrise du risque* : quels sont les principaux risques et comment les aborder ; comment mesurer et approcher le risque ; comment le diminuer ?

  - *Analyse d'impact sur les activités* : que l'entreprise doit-elle craindre ; quelles sont les activités critiques ?
  - *Développement d'une stratégie de continuité* : quelles sont les options disponibles ; lesquelles étudie-t-on ; comment choisir ?
  - *Développement d'un* PCA : contenu du plan, travaux à effectuer, attribution des missions, ceci afin d'aboutir à un plan réalisable ; présentation de listes types utiles.
  - *Test du plan* : comment s'assurer que tout fonctionne ; quels types de tests effectuer ?
  - *Maintenance du* PCA : que faut-il surveiller ; comment mettre à jour le plan ?
- **Gouvernance de la CA :**
  - document de politique générale ;
  - comité de pilotage ;
  - projet de développement ;
  - formation et sensibilisation ;
  - lois et règlements à prendre en compte ;
  - associations utiles.
- **Conclusion :** « demain, je commence par quoi ? »

Résultat

À la fin de la formation, le participant a acquis une compréhension des enjeux et une vision claire des actions à mettre en place en premier lieu. Il peut avoir accès à des outils en ligne pour initialiser sa démarche.

Sensibilisation générale

Les sessions de sensibilisation peuvent être organisées pour toucher le maximum de personnel. Elles doivent faire passer des messages simples et durer tout au plus une demi-journée.

Certaines entreprises organisent ces sessions régulièrement à dates fixes sur une période : tous les lundis après-midi pendant deux mois, par exemple.

Coordination

Le projet d'élaboration du PCA touche bien des aspects de l'entreprise. Les travaux qu'il met en œuvre interfèrent à maints endroits avec d'autres activités appartenant à d'autres projets en cours.

Il est donc important de garder une vue globale et cohérente de l'ensemble. À cet effet, un rôle de surveillance doit être dévolu à un comité directeur dans l'entreprise, afin de détecter les besoins en coordination et de procéder aux arbitrages nécessaires.

Par ailleurs, de par sa nature transverse, la continuité d'activité nécessite d'entreprendre des actions communes ou tout au moins coordonnées avec des

organismes locaux ou nationaux, avec des directives internes ou externes, avec des prestataires ou confrères impliqués, etc. Le rôle de coordination est donc fondamental.

Le projet de mise en œuvre du PCA

À la suite d'une décision de la direction générale, l'entreprise est donc tenue de mettre en œuvre un plan de continuité d'activité (PCA). C'est un projet à part entière, essentiel pour l'entreprise.

Ce projet de mise en œuvre du PCA suit les principaux jalons indiqués dans cet ouvrage du chapitre 1 au chapitre 5 : appréciation des risques, analyse d'impact sur les affaires, développement d'une stratégie de continuité, politique et cadrage du plan, attribution des différentes missions et planification des activités. Ces jalons peuvent servir à bon escient au découpage du projet en différentes phases. En effet, ils se prêtent bien à une planification des actions, avec des charges attribuées et des livrables clairs. La plupart des livrables sont illustrés dans les chapitres cités.

Concernant les choix techniques nécessaires à l'élaboration de la stratégie de continuité, on peut cette fois s'appuyer sur les chapitres de la troisième partie de cet ouvrage. Quant au test du PCA, qui vient un peu plus tard dans le projet, la procédure et les enjeux sont décrits dans le chapitre 6.

Pour les sociétés qui possèdent déjà un PCA et qui veulent l'améliorer, le projet d'amélioration peut commencer par une campagne de tests. Les actions d'amélioration des défauts ainsi révélés constituent alors les étapes suivantes.

Le rôle de contrôle exercé par la direction générale ou le comité de pilotage est capital. Il faut en effet vérifier régulièrement :

- le degré d'avancement du projet d'établissement du PCA sur ses principales étapes ;
- les frais engagés et les charges consommées ;
- l'évaluation du reste à faire ;
- les principaux problèmes rencontrés ;
- les actions correctives entreprises.

Si tout se déroule bien selon ce schéma, l'entreprise devrait, à la fin du projet, disposer d'un PCA conforme à ses orientations.

Maintenance du PCA

La politique exprimée par la direction générale a donc permis de lancer le projet de réalisation du PCA, qui a été mené à bien. Il faut alors le maintenir en ordre

de fonctionnement. Cet aspect devra être nécessairement mentionné dans la politique.

En effet, lorsque l'entreprise dispose d'un PCA opérationnel, il lui faut malgré tout faire face à diverses perturbations :

- les menaces et les risques évoluent ;
- les activités de l'entreprise changent ;
- l'entreprise elle-même subit des transformations, déménage, rachète des filiales ou se fait racheter ;
- la technologie offre des possibilités nouvelles ;
- les processus de l'entreprise se modifient ;
- les personnels évoluent ; certains partent, d'autres arrivent ;
- les fournisseurs et les clients ne sont plus les mêmes.

Tout ceci fait que le PCA initial devient erroné en partie et inapplicable en l'état. Il faut donc le modifier, l'adapter et s'assurer qu'il demeure valable malgré tout. C'est le rôle du processus de maintenance du PCA, qui s'effectue au travers d'une gestion des changements.

Un processus difficile

La gestion des changements est un exercice difficile dans bien des domaines, et d'autant plus dans la continuité d'activité.

Gérer les changements suppose en effet que quelqu'un soit tenu au courant de tout ce qui a changé et le traduise dans une modification du PCA. Mission impossible ! Les changements surviennent de toute part et sont souvent effectués par les opérationnels sur le terrain qui n'en avertissent pas forcément le gestionnaire des changements du PCA. Or celui-ci ne peut les découvrir tout seul et, par conséquent, encore moins en tenir compte. Une discipline de fer est nécessaire pour que les opérationnels préviennent systématiquement le gestionnaire lors d'un changement, et hormis les transfomations évidentes telles qu'un déménagement de site, dans la plupart des cas, aucune certitude n'existe.

C'est pour cette raison que nombre de changements sont en fait découverts lors des tests. Ceux-ci constatent en effet des inexactitudes dues à des changements non répercutés.

Faut-il pour autant ne rien faire ? Non, bien sûr, mais l'important est de rester pragmatique. Avant tout, il faut nommer un responsable de la continuité d'activité en charge de la maintenance du plan.

Veille des changements

Certains changements peuvent être découverts au moins partiellement par un responsable de la continuité (RC), dans trois domaines :

- **les mutations de personnel** : certains spécialistes changent de poste, quittent l'entreprise ou sont promus ; certains responsables changent, dans l'entreprise comme chez les fournisseurs employés pour la continuité ;
- **les évolutions technologiques** : des solutions techniques nouvelles sont mises en œuvre, tandis que les anciens systèmes sont abandonnés. Ces changements ne sont hélas pas facile à détecter dans leur totalité ;
- **l'évolution de l'organisation des processus et des activités de l'entreprise** : ce qui était critique au départ peut l'être moins et inversement. Ces modifications peuvent être prises en compte.

Le RC doit donc mettre en place un système de veille ou de détection. Cela peut se faire de plusieurs manières :

- en observant ce qui se passe, en consultant les annonces internes, en suivant les mutations, les projets, etc. ;
- en contactant les chefs de projets et en les sensibilisant à l'importance de la communication de ce type d'informations ;
- en émettant des circulaires pour rappeler certains éléments importants, faire circuler des listes et demander vérification ;
- en se faisant régulièrement confirmer par les responsables d'activité ce qui est critique ou non, les différents délais de reprise, etc. ;
- en demandant l'accès à des outils de gestion de configuration où certains changements sont détectables ;
- en demandant à être mis en copie lors de la création de nouveaux projets, etc. ;
- en traînant du côté de la machine à café…

Il est intéressant de mettre à ce poste un responsable reconnu et charismatique. Il s'agit parfois d'un responsable de groupe, voire du coordonnateur du PCA (voir le chapitre 4).

> **Important**
>
> Le devoir de rendre compte en cas de changement ayant un impact sur le PCA est un message essentiel à faire passer lors des sessions de sensibilisation.

Politique de test nécessaire

La source la plus évidente pour identifier les changements est le résultat des tests. Il peut d'ailleurs être intéressant d'y chercher les changements que l'on aurait pu découvrir sans test, uniquement en ayant averti le responsable de la gestion des changements du PCA, ceci afin d'améliorer la procédure de communication à ce sujet. Il existe aussi des situations où les tests font apparaître des besoins de changements autres que dans le PCA proprement dit – dans les comportements, par exemple.

Étant donnée son importance cruciale pour le maintien en état opérationnel du PCA, une politique de test est elle-aussi nécessaire. Elle doit prévoir les types de

tests, leur fréquence et leur ordonnancement dans le calendrier. Les aspects pratiques de mise en œuvre des tests sont détaillés dans le chapitre 6, et seuls les points de politique et d'organisation sont donc présentés ici.

Types de tests

Il est important de bien organiser les tests de manière à optimiser le rapport entre test et résultats et à éviter de se retrouver dans des situations bloquantes.

> **Exemple : Où sont les bandes ?**
>
> La société DFD a réalisé sur le papier un PCA sommaire. Elle n'a aucune culture de test de PCA. Elle décide de réaliser sur trois jours un test en simulation, avec réelle mise en œuvre d'un ensemble de serveurs de secours sur un site distant chez un prestataire.
>
> Pour ce test ambitieux, la société réserve un support grand système et Unix de haut niveau chez ledit prestataire. Ces spécialistes coûteux sont réservés pour trois jours fermes.
>
> Le premier jour, à H0, il faut aller chercher les cassettes de sauvegarde dans le lieu où elles sont conservées. Petit cafouillage : qui doit y aller ? Où est-ce exactement ? Après deux heures de discussion (H+2), deux techniciens partent en voiture sur le fameux site de conservation des cartouches de bandes. Arrivés sur place : problème ! Personne ne veut les accepter. On n'entre en effet pas comme dans un moulin sur ce site sécurisé, exercice de test ou pas ! Le compteur tourne... Au bout d'une heure et après échanges de fax, ils peuvent enfin accéder aux lieux (H+3).
>
> Arrivés enfin si près du but, autre problème : parmi toutes ces armoires, laquelle est la bonne ? Où sont les clés ? Qui peut renseigner ? Et dans l'armoire : quelles sont les cassettes à reprendre ? Toutes ? Cela ne tiendra jamais dans la voiture ! Quelques-unes ? Lesquelles ? Nous sommes déjà à H+4. Le problème est enfin résolu à H+5, il ne reste plus qu'à trouver la route pour se rendre sur le site de secours, ce qui n'a pu se faire sans le téléphone portable et les collègues...
>
> Pendant ce temps là, les experts systèmes sont facturés au prix fort, quasi à ne rien faire.
>
> **Moralité** : avant de se lancer dans un test de grande ampleur, vérifions les listes, établissons qui fait quoi, allons voir sur place comment cela se présente, notons les noms de ceux qui détiennent les informations... En bref, préférons d'abord des tests de type *checklist* ou *walk-through*.

Il existe une certaine logique à respecter dans la démarche de test, qui doit être progressive. Pour une société peu entraînée en la matière, il faut considérer les points suivants :

- commencer par de petits tests bien ciblés sur un problème concret et un périmètre restreint (voir l'exemple précédent de la recherche des sauvegardes, que l'on peut tester à part) ;
- organiser plusieurs petits tests de ce type assez rapprochés (tous les mois) un peu partout dans la société ;
- augmenter progressivement l'importance des tests et le périmètre concerné ;
- capitaliser à chaque fois en tirant des conclusions pédagogiques des tests et en modifiant les documents du PCA aux points nécessaires ;

- utiliser éventuellement des cas réels vécus pour organiser une session de formation ;
- prouver par l'exemple que tout ce processus est bénéfique : le même test qui a pris quatre heures avec des difficultés sera refait le mois suivant en une heure, une fois les difficultés aplanies ;
- éventuellement, faire des tests gigognes (le test 3 cumulant les tests 1 et 2), afin de montrer une progression.

Il est intéressant de développer ces aspects et de les suivre au cours de l'année par une communication auprès des comités de direction, des départements, etc.

Fréquence des tests

Il est courant de considérer que la fréquence et l'ambition des tests sont inversement liées. Plus la fréquence est élevée, moindre est l'ambition en termes de contenu, de périmètre et de coût.

La sensibilité au besoin de test est variable selon les entreprises, les cultures et le caractère des équipes dirigeantes. Certaines sociétés organisent un test très important tous les ans, un test moyen tous les six mois, et de petits tests de type *check-list* tous les mois. D'autres sont moins exigeantes et font des *check-lists* tous les six mois et des tests plus ambitieux tous les deux ans, voire plus. Il existe aussi une proportion non nulle de sociétés qui ne testent rien ou font juste sonner les alarmes incendie. Ne rien tester revient à constater l'absence de PCA ou à programmer sa mort. En effet, aucun PCA non testé n'est viable à moyen terme.

Par conséquent, il est important de maintenir un climat, non pas de test, mais de préparation au sinistre. Cela passe notamment par la réalisation de tests concernant un petit périmètre mais fréquents.

Les tests mensuels

On peut organiser tous les mois des tests assez légers et peu perturbateurs permettant de vérifier certains points précis, comme l'exactitude des listes ou l'actualité des divers documents. Le chapitre 6 présente cela en détail.

Ces exercices de test, peu exigeants en ressources et peu coûteux, ne mobilisent qu'une partie des groupes (voir le chapitre 4) et des spécialistes impliqués dans la continuité d'activité.

Les tests trimestriels

Chaque trimestre, on peut pratiquer des exercices un peu plus larges et plus complexes que les précédents, permettant de passer en revue certains points particuliers sur lesquels subsistent encore des doutes : déroulement des opérations du PCA suite à la découverte du sinistre, communication en cas de sinistre, clauses des contrats de service, mise en place des groupes dont les membres ne se connaissent pas, activation du centre de crise, etc.

Il est important d'impliquer dans ces tests le personnel qui serait impliqué en situation réelle, en faisant appel à des responsables hiérarchiques opérationnels.

Les tests semi-annuels

Moins fréquents, plus ambitieux et plus onéreux, ces tests peuvent recourir à la simulation en la combinant avec les démarches de revue et de *check-list* des tests précédents. Ils permettent par exemple de vérifier l'ensemble du PCA en simulant un sinistre sur un périmètre raisonnable, ou encore de simuler la disparition de certaines activités critiques et leur reconstruction sur un site de secours dans les délais impartis. On peut, à ce stade, effectuer en simulation ou en parallèle un ensemble de tests qui a été auparavant correctement effectué en *check-list* ou *walk-through* ou, pour une thématique donnée, passer en revue le PCA complet pour détecter ce qui risque de bloquer (accès sécurisés, autorisations de connexions, mots de passes, etc. pour la sécurité, par exemple).

Ces tests ne pourront être organisés que si les tests moins ambitieux qui précèdent ont été menés à bien, suivis des actions correctives nécessaires. Procéder ainsi permet en effet de découvrir assez tôt et de corriger par anticipation certains points de blocage qui auraient faussé un exercice de plus grande ampleur.

Le test annuel

Prévu pour passer en revue l'ensemble du PCA en simulation ou en interruption partielle ou totale, ce test est le plus complet que l'on puisse pratiquer.

Peu d'entreprises testent l'ensemble de leur PCA, depuis l'expression des besoins sur le site de secours jusqu'au retour sur le site primaire et au bilan. Il est évident que la faisabilité d'un tel test dépend également beaucoup des moyens que la société consacre à cette activité. En outre, l'organisation de tests de cette ampleur implique souvent clients et fournisseurs et, dans certains cas, certaines sociétés alertent aussi la presse pour créer un événement.

Dans la même optique, il est également intéressant de faire participer l'entreprise à des tests organisés par les autorités ou autres acteurs simulant par exemple un accident nucléaire ou une explosion d'usine grandeur nature.

Vue d'ensemble des tests

La diversité des tests est telle que cela nécessite un minimum de ligne directrice, afin de mettre en évidence leur intérêt. Les apports réels en termes de formation et d'amélioration du PCA doivent être soulignés. La publication d'un document pluriannuel annonçant les tests par l'entité responsable du PCA prend alors tout son sens, œuvrant à la bonne compréhension de la politique de continuité de l'entreprise.

Ce document permet en effet de présenter une situation en évolution, en partant de tests simples et réguliers pour aboutir à des tests annuels plus complexes.

Prise en compte des conclusions d'audits

Afin d'évaluer la mise en œuvre de la politique de continuité de l'entreprise, la réalisation d'audits est indispensable. Des détails sur ce sujet sont donnés dans le chapitre 13. Les audits produisent des résultats dont il faut absolument tenir compte, car ceux-ci vont avoir un impact non négligeable sur le PCA.

L'audit permet en effet de constater plusieurs types d'anomalies :

- des écarts entre la politique de l'entreprise et la réalité ;
- des différences entre ce qui est écrit dans le PCA et la réalité du terrain ;
- des risques non couverts.

Ces constatations vont entraîner des modifications dans le PCA, permettant d'assurer sa bonne maintenance.

En outre, l'apparition imminente de normes internationales dans le domaine de la continuité d'activité va permettre de donner aux audits le rôle essentiel de faire apparaître certains besoins de mise en conformité, eux-aussi sources de modifications du plan (voir en annexe 1).

Changements dans l'entreprise, résultats des tests, conclusions d'audits – tous ces aspects devront être pris en compte pour modifier le plan de continuité en vue de le maintenir d'actualité et de l'améliorer.

Gestion des changements du plan

Au cours des différentes procédures décrites précédemment (veille des changements, tests, audits), l'ensemble des besoins de modifications dans le plan de continuité est ainsi collecté. Ces besoins vont se traduire en demande de changements.

On entre alors dans un processus classique de gestion des changements, portant sur un ensemble de prescriptions et de documents. Les principales étapes en sont :

1. collecter et classer les différentes demandes de changements en fonction des chapitres du plan sur lesquels elles portent ;
2. faire analyser et valider ces demandes par les différents responsables concernés, à savoir les personnes en charge des sections correspondantes du plan de continuité, certains responsables d'activités ou des chefs de groupes (voir le chapitre 4) ;
3. attribuer les modifications aux entités concernées et les faire réaliser en mode « brouillon » ;
4. vérifier l'ensemble des modifications effectuées en « brouillon » pour y détecter d'éventuelles incohérences ou des difficultés de mise en œuvre ;
5. après d'éventuelles corrections, faire un dernier tour de révision pour obtenir les approbations de tous les responsables concernés ;
6. intégrer les modifications définitives dans le plan de continuité en respectant la gestion de version et les règles de mise à jour en place – cela peut se

faire sur un système documentaire centralisé ou sur des copies décentralisées qui seront mises à jour chacune par leurs responsables en suivant une procédure coordonnée ;

7. avertir les opérationnels des changements du plan.

Cas particulier : Mise à jour des listes

Parmi les défauts détectés dans le plan et nécessitant une modification, on retrouve souvent le problème des listes de matériel, de personnel, etc., qui devraient rendre compte des mouvements de machines et de personnels, mais qui, de fait, ne sont souvent pas tenues à jour.

Pour ce type de modifications, plutôt que d'employer la procédure de gestion des changements décrite ici, il convient d'adopter une gestion particulière de type « gestion de configuration » plus proche du terrain. Ces listes devront donc être mises à jour régulièrement, au fur et à mesure des évolutions. Il est important d'accorder le plus grand soin à ce processus.

Chapitre 13

Le système de contrôle

Pour toute orientation émanant de la direction générale, il convient de s'assurer que la réalité du terrain s'y conforme : c'est alors qu'intervient le contrôle. Toute politique s'accompagne d'une vérification de son exécution, et donc d'un système de contrôle.

En ce qui concerne le PCA, la pratique est encore nouvelle pour bien des entreprises. Néanmoins, des démarches fondées sur les référentiels et les bonnes pratiques qu'ils présentent se mettent peu à peu en place.

Objectifs

La démarche de contrôle de la continuité d'activité permet d'apporter des réponses aux deux questions suivantes :

- la volonté de la direction générale est-elle bien traduite sur le terrain ?
- par quels moyens la direction générale peut-elle faire passer les inflexions de sa politique dans les faits ?

Définir une structure de référence

La première chose à faire est de définir un cadre de travail qui va servir de référence indiscutée. Cela peut être une norme, un ensemble de pratiques jugées bonnes, un référentiel métier, etc.

Dans le domaine de la continuité d'activité, les référentiels existants proviennent actuellement plutôt du monde anglo-saxon. Ce sont des normes comme celles du *Disaster Recovery Institute* (USA) ou du *British Standard Institute* (Royaume Uni). L'AFNOR a elle aussi entamé des travaux sur ce sujet. L'annexe 1 fait le point sur ces normes.

Rien n'empêche cependant une société de se construire son propre référentiel, même s'il existe de bonnes raisons prêchant en faveur d'un référentiel externe.

- Cela permet de couper court à toute discussion, en invoquant l'argument suivant : « nous suivons la référence du marché ».
- Cela facilite les comparaisons entre plusieurs sociétés.

- En contexte international ou dans le cadre d'un groupe de sociétés de cultures diverses, cela permet d'avoir une approche neutre.
- Lors de fusions d'entreprises, cela facilite l'unification.

Par décision de la direction générale, la société doit donc se construire ou, de préférence, se choisir un référentiel et le conserver.

Ce référentiel est généralement structuré en grands chapitres, comme le montre l'exemple de structure suivante :

Référentiel de continuité d'activité N° 1

1. Maîtrise des risques
2. Analyse d'impact sur les activités
3. Stratégie de continuité
4. Plan de continuité
5. Test du plan
6. Gouvernance de la continuité

Voici un autre exemple :

Référentiel de continuité d'activité N° 2

1. Connaissance des risques et des impacts
2. Stratégie de continuité
3. Affectation des responsabilités
4. Définition du planning
5. Test du plan

Il apparaît dans ces exemples que la structure choisie, en cinq à sept points, décline toutes les actions nécessaires pour prétendre avoir une véritable mise en œuvre de la continuité en entreprise.

Déterminer les objectifs

La direction générale détermine alors, dans le cadre choisi, les objectifs qu'elle veut atteindre, sous la forme d'instructions. Ces instructions détaillent les titres de chapitre du référentiel choisi.

Les encadrés qui suivent donnent des exemples.

Pour la maîtrise du risque :

Objectifs

1. Documenter le cadrage de la démarche
2. Identifier les menaces et les risques
3. Faire la liste des biens exposés
4. Analyser les options possibles
5. Faire une préconisation documentée

Pour l'analyse d'impact sur les activités :

Objectifs
1. Documenter le cadrage de la démarche
2. Analyser les processus d'activité
3. Déterminer les configurations concernées
4. Déterminer les processus critiques et leurs paramètres
5. Élaborer une stratégie documentée

Pour le plan de continuité :

Objectifs
1. Documenter le cadrage de la démarche
2. Définir ce qu'est un sinistre
3. Préciser les périmètres
4. Définir les groupes et leurs responsabilités
5. Mettre en place un centre de gestion de crise
6. Établir un planning répartissant les activités en différentes étapes
7. Établir un plan de communication
8. Établir un plan d'affectation
9. Mettre en place un système de documentation

Pour les tests du plan :

Objectifs
1. Documenter le cadrage de la démarche
2. Expliquer les objectifs des campagnes de tests
3. Décrire les types de tests prévus et leurs impacts
4. Préconiser des moyens pour les tests
5. Formaliser le suivi des tests
6. Documenter les conclusions

Comme on le voit sur ces exemples, ces objectifs sont tout à la fois suffisamment généraux pour être universels dans leur application et suffisamment précis pour orienter l'entreprise dans une direction choisie. Très importants pour l'entreprise, ils sont valables à long terme (au moins trois ans) et s'appliquent à toutes les variantes organisationnelles ou géographiques que l'entreprise connaît.

Décliner les objectifs

Les chapitres du référentiel choisi ont été, dans un premier temps, détaillés en objectifs à atteindre. Dans un second temps, ces objectifs sont déclinés pour

tenir compte des spécificités locales et détaillés plus finement pour être plus précis.

Il existe plusieurs manières de procéder. Le plus souvent, il est intéressant de traduire l'objectif en quelques questions (entre trois et sept) qui pourront être posées à la direction locale, ou sur lesquels un auditeur pourra s'appuyer pour son évaluation.

Voici deux exemples :

Chapitre N° 1 « Maîtrise du risque »

Objectif N° 2 « Identifier les menaces et les risques »

Q1. Les critères de sélection sont-ils précisés ?
Q2. Les découpages réalisés sont-ils approuvés ?
Q3. Les responsables d'entité concernés sont-ils impliqués ?
Q4. Les exclusions éventuelles sont-elles mentionnées ?
Q5. Les techniques d'analyse sont-elles décrites ?
Q6. Les sources d'information sont-elles citées ?

Chapitre N° 3 « Stratégie de continuité »

Objectif N° 1 « Identifier les besoins de reprise »

Q1. Dispose-t-on d'un rappel des analyses précédentes ?
Q2. Les exigences des processus critiques sont-elles exprimées ?
Q3. La liste des besoins de reprise est-elle fournie ?
Q4. Les besoins sont-ils segmentés par nature ?
Q5. Les besoins communs sont-ils identifiés ?

On obtient ainsi une vingtaine de questions par chapitre, c'est-à-dire cent vingt à cent cinquante questions pour l'ensemble de la politique de continuité. La formulation de ces questions est parfois délicate. En effet, la réponse ne doit pas laisser une grande marge à l'interprétation mais pouvoir, au contraire, s'appuyer sur des faits constatables. Certaines sociétés de conseil peuvent fournir une assistance appréciable sur ce sujet assez délicat.

Évaluer le plan

À partir de ces questions, il va enfin être possible d'obtenir des réponses. Il existe plusieurs manières de procéder :

- confier les questionnaires aux responsables des entités concernées et leur demander de répondre – c'est ce qu'on appelle « l'auto-évaluation » ;

- demander à un observateur interne à l'entreprise (auditeur interne) de se forger une opinion et de remplir les questionnaires ;
- faire appel à un évaluateur externe à l'entreprise ;
- employer les trois méthodes précédentes à la fois.

L'évaluation proprement dite peut elle aussi prendre plusieurs formes :

- une réponse binaire : « oui » ou « non » ;
- une échelle de graduation telle que : « pas d'accord », « moyennement d'accord », « plutôt d'accord » ou « tout à fait d'accord » ;
- une note de 0 (mauvais) à 5 (excellent).

Il est intéressant de faire évaluer les mêmes points par des personnes différentes et de constater les écarts éventuels.

Les réponses collectées permettent de produire différents schémas au pouvoir explicatif variable. Certaines sociétés de conseil fournissent des grilles d'analyse et des modèles très explicites.

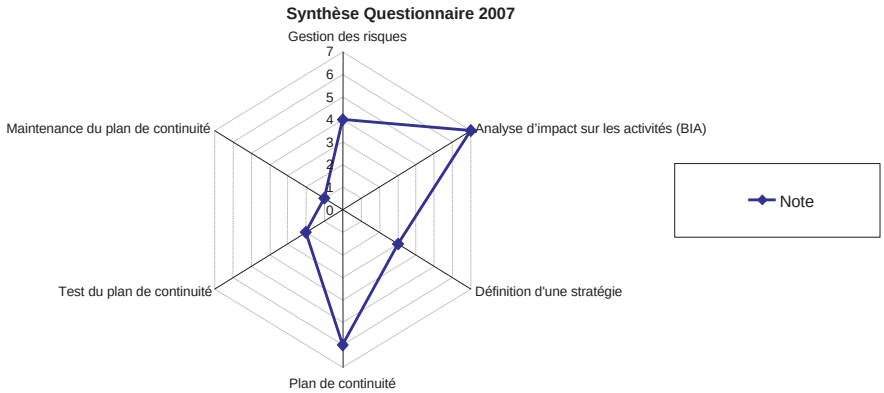


Figure 13-1 : Évaluation d'une entreprise sur des critères multiples

Tirer les conclusions

Grâce à cette analyse, la direction générale dispose d'une photographie de l'existant. La plupart du temps, lorsque cette image émane des responsables opérationnels eux-mêmes, cet état des lieux est très intéressant. Il permet en effet de déterminer les points forts et les points faibles de l'entreprise selon le point de vue des opérationnels.

La direction générale, de son côté, peut souhaiter que l'entreprise obtienne au moins une note palier sur certains domaines. Elle peut fixer une note cible à

atteindre, modulée selon les têtes de chapitre de sa stratégie. Cela peut s'exprimer sur le schéma suivant :

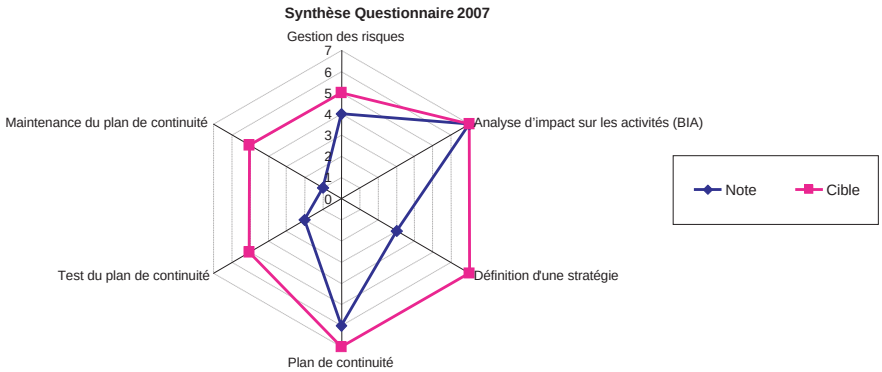


Figure 13-2 : Les objectifs par rapport à l'évaluation

La comparaison entre les souhaits exprimés par la direction générale et ce qui ressort des réponses aux questionnaires permet de faire apparaître les points ou les thèmes pour lesquels des améliorations sont nécessaires. Là encore, l'appel à une société de conseil peut apporter une aide précieuse .

Recommencer

L'ensemble de ces opérations doit être effectué à nouveau régulièrement, par exemple tous les ans. Recommencer l'exercice permet en effet de :

- constater et mesurer les progrès ;
- éviter de s'endormir sur ses lauriers ;
- modifier éventuellement les orientations, les instructions, les questions… ;
- faire varier les niveaux d'exigence demandés ;
- modifier le périmètre de l'exercice.

Il est également possible d'y ajouter des orientations sortant un peu du cadre de la continuité d'activité, en matière de sécurité ou de qualité par exemple. Mais cela sort du cadre de cet ouvrage.

Annexe 1

Normes et bonnes pratiques

Aucune norme internationale ne s'est encore imposée de manière indiscutable dans le domaine de la continuité d'activité. Certains référentiels présentent cependant des démarches intéressantes.

Par ailleurs, certaines normes traitant d'autres thématiques connexes (la sécurité, par exemple) incluent un chapitre ou un paragraphe concernant la continuité, et nombre de travaux sur ce thème sont réalisés actuellement au sein des divers organismes de normalisation.

Les normes internationales

Les normes concernant la continuité d'activité sont essentiellement d'origine américaine ou britannique. Elles consistent généralement à décrire les « meilleures pratiques » (*best practices*, en anglais) issues de l'expérience des professionnels du sujet abordé.

Normes de type « bonnes pratiques »

Le terme « norme » peut en soi prêter à confusion. Il ne s'agit en effet pas ici de normes industrielles donnant précisément les cotes d'une pièce à respecter absolument, mais plutôt de lignes de conduite. Ces normes sont des ensembles de recommandations émises sur des manières de faire par une association de professionnels cooptés. Ces associations, qui participent également à différents degrés aux travaux de normalisation dans leur pays et à l'ISO (Organisation internationale de normalisation), se donnent en général trois objectifs :

1. partager et accumuler les expériences pour décrire par écrit ce qui fonctionne le mieux sous forme d'un corpus de bonnes pratiques ;
2. former des professionnels à ces bonnes pratiques et décerner des certificats ou des attestations de formation gradués par niveaux ;
3. faire la promotion de ces professionnels certifiés en assurant ainsi une sensibilisation du marché aux enjeux de la continuité.

Parmi ces associations se consacrant à la continuité d'activité, deux organismes se distinguent :

- Le **DRII** (*Disaster Recovery Institute International* ou « organisation internationale pour la reprise après sinistre »), pionnier d'origine américaine, est très actif depuis 1988.
- Le **BCI** (*Business Continuity Institute* ou « organisme pour la continuité d'activité »), créé en 1994 et d'origine britannique, est un contributeur important auprès de l'organisme de normalisation britannique, le BSI (*British Standard Institute*), et de l'organisation internationale de normalisation ISO.

La base de connaissance du DRII

En 1997, le DRI International a publié une base de connaissances collectées et formalisées par ses soins en matière de continuité. Son ambition est de présenter en dix points ce que tout responsable de la continuité doit maîtriser. Ces dix points sont :

1. le démarrage et la gestion du projet de continuité ;
2. l'évaluation et la maîtrise du risque ;
3. l'analyse d'impact sur les activités ;
4. le développement d'une stratégie de continuité ;
5. les interventions d'urgence ;
6. la mise en place d'un plan de continuité ;
7. les programmes de sensibilisation et de formation ;
8. la maintenance et les tests du plan de continuité ;
9. la communication de crise ;
10. la coordination avec les autorités.

Cette somme est internationalement reconnue.

La norme BS 25999

Le *British Standard Intitute* (BSI), entité de normalisation britannique (équivalent de l'AFNOR en France), a émis récemment une norme sur le sujet de la continuité : la BS 25999. Cette norme britannique est à l'heure actuelle la plus avancée sur le thème de la continuité d'activité et mérite toutes les attentions, pour plusieurs raisons.

- Elle concentre en son sein tout un ensemble de travaux et d'expériences pratiques de première importance.
- Son rayonnement va bien au-delà du Royaume-Uni : son influence se fait sentir dans une cinquantaine de pays.
- L'ISO a jusqu'à présent repris bon nombre de normes de type « bonnes pratiques » du BSI pour en faire des normes ISO, sans quasiment les modifier.

BS 25999-1 et BS 25999-2

Comme pour les autres normes récentes du BSI de type « bonnes pratiques », la norme BS 25999 est scindée en deux parties :

- la **BS 25999-1** est le code de bonnes pratiques en tant que tel concernant la mise en œuvre de la continuité dans l'entreprise ;
- la **BS 25999-2** (à venir) donne des recommandations nécessaires à ces réalisations et à la préparation aux audits.

Les six points de la BS 25999-1

La norme britannique BS25999-1 préconise une démarche en six points :

1. **Comprendre l'organisation de l'entreprise** – Il s'agit tout autant de connaître les risques auxquels l'entreprise est exposée que ses activités critiques. Cela correspond assez bien aux chapitres 1 et 2 du présent ouvrage.
2. **Déterminer les options de continuité** – Cela consiste à choisir, parmi les différentes options possibles, ce que l'entreprise fera en cas de sinistre et à lister les besoins en termes d'équipements, de sites, de secours, de compétences… Cela correspond peu ou prou au chapitre 3 du présent ouvrage.
3. **Développer et mettre en œuvre une réponse** – Il s'agit ici de développer le plan de continuité et d'attribuer les rôles et responsabilités. Cela correspond aux chapitres 4 et 5 du présent ouvrage.
4. **Introduire la continuité d'activité dans la culture de l'entreprise** – Ce point consiste à organiser des formations, à sensibiliser les employés et à décrire les aspects touchant à la continuité au sein des postes de travail.
5. **Tester, maintenir et auditer** – Il s'agit ici de tout ce qui concerne les tests, exercices, maintenances et audits, correspondant aux chapitres 6, 12, et 13 de cet ouvrage.
6. **Piloter le programme de continuité d'activité** – On aborde ici la gestion de l'ensemble des actions décrites précédemment et la responsabilité de la continuité (voir les chapitres 11 et 13).

Les cinq premiers points se succèdent, telles les phases d'un projet. Le dernier point doit être une préoccupation permanente de l'équipe en charge de la continuité.

Travaux de l'ISO

Actuellement, l'Organisation internationale de normalisation (ISO – *International Organization for Standardization*) ne semble pas considérer la continuité d'activité comme un thème à part, mais plutôt comme une préoccupation commune à plusieurs thèmes et éclatée sous diverses rubriques. On peut citer en particulier les normes consacrées à la sécurité de l'information de la famille ISO 27000 et les guides de préparation aux sinistres.

Cette approche semble en effet poser problème au sein de l'ISO, car lors de chaque approfondissement des thèmes de la continuité d'activité, des difficultés de rédaction surgissent.

La norme sécurité ISO 27002

Cette norme présente une série de préconisations concrètes pour assurer la sécurité de l'information. Elle compte neuf chapitres traitant des différents domaines concernés par la sécurité.

Le chapitre 14 de la norme ISO 27002 traite de la « gestion du plan de continuité de l'activité » sur deux pages environs. Autant dire que le problème n'est abordé que de très haut et uniquement à travers les aspects informatiques.

L'ISO est en train de refondre les normes de cette famille 27000 et un numéro a été réservé pour les aspects « continuité d'activité » du système d'information et des télécommunications : l'ISO 27031. À l'heure actuelle, les travaux sur cette portion de norme semblent hésitants, faisant sentir l'influence de la montée en puissance des normes purement consacrées à la continuité. À quoi bon, en effet, traiter de continuité dans une norme sur la sécurité alors que, par ailleurs, des organismes comme la BSI étudient la continuité en tant que telle ?

La spécification ISO/PAS 22399

Un exemple supplémentaire de la situation actuelle à l'ISO et de l'éclatement des approches de la continuité apparaît avec la « spécification disponible publiquement » ou PAS (P*ublicly Available Specification*) ISO/PAS 22399:2007, qui aborde la S*écurité sociétale – Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle*.

Cette PAS s'appuie, quant à elle, sur des contributions de type « bonnes pratiques » émanant des cinq organismes de normalisation nationaux d'Australie, d'Israël, du Japon, du Royaume-Uni et des États-Unis. Son influence sur les travaux en entreprise est faible.

La situation en France

En France, trois organismes montrent un intérêt particulier pour la continuité d'activité : il s'agit de l'AFNOR, du Club de la Continuité d'Activité et du forum tripartite (ou *Joint Forum*).

Travaux de l'AFNOR

L'AFNOR a publié une norme BP Z74-700 dans la catégorie des bonnes pratiques. Celle-ci se consacre cependant essentiellement aux activités de reprise après sinistre (correspondant aux chapitres 4 et 5 de cet ouvrage).

La norme AFNOR est tournée vers les problèmes de perte d'exploitation, de plan de reprise d'activité (PRA) et aborde peu la maîtrise des risques.

L'AFNOR travaille aussi à un glossaire.

Le Club de la Continuité d'Activité (CCA)

Créé en 2007 en France, ce club a pour ambition de faciliter et promouvoir le partage d'expérience entre ses membres. Il a lancé des groupes de travail sur des sujets aussi divers que la pandémie grippale, les contraintes réglementaires et les « concepts et vocabulaire » de la continuité en français.

Ce club gère aussi un wiki de travail accessible au grand public.

Le forum tripartite ou *Joint Forum*

En collaboration avec la Banque de France et diverses institutions, un document intitulé P*rincipes directeurs en matière de continuité d'activité* a été publié en 2006. Ce document préconise un certain nombre de principes dont cet ouvrage d'ailleurs se fait le reflet.

On consultera le site web indiqué en Annexe 2 pour plus de détails.

Les approches connexes

Des organismes autres que ceux de normalisation réalisent eux aussi des documents de préconisations ou de bonnes pratiques. Certains d'entre eux agissent dans un périmètre qui recoupe en partie la continuité d'activité. En voici quelques-uns qui méritent l'attention.

ITIL

L'ITIL est un ensemble de pratiques et de recommandations permettant de gérer la production informatique de services. Dans sa version 2, ce référentiel est constitué de dix livres. L'un de ceux-ci, intitulé F*ourniture des services*, comprend cinq processus, dont un dénommé G*estion de la continuité de service*.

La continuité du service est ainsi traitée comme un thème parmi plusieurs dizaines d'autres. L'apparition de la version 3 de l'ITIL, encore plus ambitieuse et plus riche, n'a fait que diluer encore la préoccupation de « continuité d'activité ». En réalité, la pratique de l'ITIL dans les sociétés qui le mettent en application a généralement fait peu de cas de ce processus en particulier.

En revanche, il est important de souligner qu'une bonne mise en œuvre *à la façon* ITIL de la gestion des configurations, des changements, des incidents et des problèmes concourt assurément à une continuité d'activité efficace.

Mehari

Le Clusif (Club de la sécurité de l'information français) a développé ces dernières années une approche originale d'évaluation des risques liés à la sécurité de l'information. Mehari fournit gratuitement (sous licence publique) un ensemble structuré de méthodes, d'outils et des bases de connaissance pour :

- analyser les enjeux majeurs de l'entreprise en matière de sécurité, en étudiant les dysfonctionnements principaux et leur gravité ;
- étudier les vulnérabilités, c'est-à-dire identifier les faiblesses et les défauts des mesures de sécurité ;
- réduire la gravité des risques en travaillant en parallèle sur les causes et les conséquences ;
- piloter la sécurité de l'information, avec des objectifs, des indicateurs et des plans d'actions.

Cette approche française est dotée de divers outils et tableaux disponibles en licence libre. Bien que restant cantonnée aux risques encourus par le système d'information, elle propose malgré tout un tour d'horizon intéressant.

NFPA 1600

L'association de protection contre l'incendie NFPA (*National Fire Protection Association*) a été créée en 1896 aux États-Unis. Sa mission est de réfléchir et préconiser des approches techniquement fondées pour réduire les problèmes dus au feu et autres risques.

En janvier 2000, la NFPA a publié la norme NFPA 1600 proposant un ensemble commun de critères pour gérer les catastrophes, les situations de secours et les programmes de continuité. C'est une norme américaine ANSI (*American National Standards Institution*). NFPA 1600 présente un nombre important de documents listant des bonnes pratiques dans des domaines aussi variés que la politique de continuité, les divers comités de programme, la manière d'identifier et de classer les risques et les menaces, la planification des actions, la coordination, la communication, la logistique, la formation, l'éducation du public, etc.

Annexe 2

Sources d'information

Dans une démarche de mise en place du plan de continuité, il est utile de disposer d'informations neutres, sûres et à jour.

Voici quelques organismes susceptibles d'en fournir.

Organismes francophones

- AFNOR (Association française de normalisation) – www.afnor.org
- Club de la Continuité d'Activité (CCA) – www.clubpca.eu
- Clusif (Club de la Sécurité de l'Information Français) – www.clusif.asso.fr
- Forum tripartite avec la Banque de France – www.banque-france.fr
- Haut Comité Français pour la Défense Civile (HCFDC) – www.hcfdc.org
- Institut National de l'Environnement Industriel et des Risques INERIS) – www.ineris.fr
- Institut d'Études et de Recherche pour la Sécurité des Entreprises (IERSE) – www.ierse.fr
- Institut National des Hautes Études de Sécurité –www.inhes.interieur.gouv.fr
- Ministère de l'Écologie – www.ecologie.gouv.fr et www.vigicrues.ecologie.gouv.fr

Organismes anglophones

- Business Continuity Planners Association (BCPA) –www.bcpa.org
- Disaster Recovery Institute International (DRII) –www.drii.org
- Business Continuity Institute (BCI) – www.thebci.org
- British Standard Institute (BSI) – www.bsi-global.com
- Business Continuity Management Information eXchange (BCMIX) – http://BCMIX.collectivex.com
- Association of Insurance and Risk Managers – www.airmic.com
- United Nations Environment Programme (UNEP) www.unep.org
- Incident.com – www.incident.com
- ISO (International Organization for Standardization) – www.iso.org

- National Fire Protection Agency (NSPA) – www.nfpa.org
- Uptime Institute – http://uptimeinstitute.org
- Telecommunications Industry Association (TIA) – www.tiaonline.org

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Management de la Continuité d'activité

L'auteur

Ingénieur informatique diplômé de Centrale et de l'Université de Berkeley, **Emmanuel Besluau** a occupé de nombreux postes à responsabilités dans de grands groupes de différents secteurs, notamment bancaire et de services (IBM, Sligos-Carte Bancaire, Atos-Infogérance...). Aujourd'hui consultant associé au Duquesne Group, il écrit périodiquement dans la presse informatique et intervient en tant qu'expert reconnu auprès de DSI sur des sujets comme la continuité de service, les architectures techniques des centres informatiques, les bonnes pratiques de production de service (ITIL, sécurité, etc.). Il est membre actif du Club de la Continuité d'Activité.

François Tête est Président du Club de la Continuité d'Activité (CCA).

www.clubpca.eu

À qui s'adresse ce livre ?

- Aux responsables risque ou continuité (RSSI, RPCA...) et à leurs équipes
- Aux chefs de projet chargés de mettre en place un PCA
- Aux DG et chefs d'entreprise souhaitant aborder le MCA
- À tous les responsables métier préoccupés par la continuité de leur activité
- Aux DSI et responsables techniques ayant à faire des choix de systèmes
- Aux auditeurs dans le domaine des technologies de l'information
- Aux professionnels de la sécurité ou d'ITIL désirant approfondir le volet continuité

À l'heure où le système d'information (SI) est au cœur des processus, une panne informatique de seulement trois jours suffit à paralyser durablement toute entreprise non préparée. Si la prévention des risques et la sécurité font l'objet de préoccupations croissantes, les responsables négligent trop souvent de se prémunir contre les **conséquences** d'éventuels désastres. Or le **management de la continuité d'activité (MCA)** offre des solutions efficaces pour renforcer la résistance de l'entreprise et du SI face aux crises de toute nature (inondation, incendie, pannes, malveillance...).

Proposant une démarche à la fois organisationnelle et technique, ce guide complet et documenté décrit pas à pas la mise en œuvre concrète d'un **plan de continuité d'activité (PCA)** solide et opérationnel. Il s'appuie sur des **études de cas** réels issues de la longue expérience de l'auteur pour fournir une méthodologie efficace et une revue des solutions possibles (plan de reprise, sites de secours, continuité de service, outils de sauvegarde, architectures du SI, tests et audits, etc.) enrichies de recommandations pratiques et de documents types, sans oublier d'aborder les principes de **gouvernance** et la **normalisation** en cours.

Au sommaire