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.

Enfin, ce n'est qu'une fois ces actions réalisées que l'entreprise aura une meilleure connaissance des scénarios de sinistre dits « résiduels », qui demeurent encore possibles et serviront de contexte pour la suite.

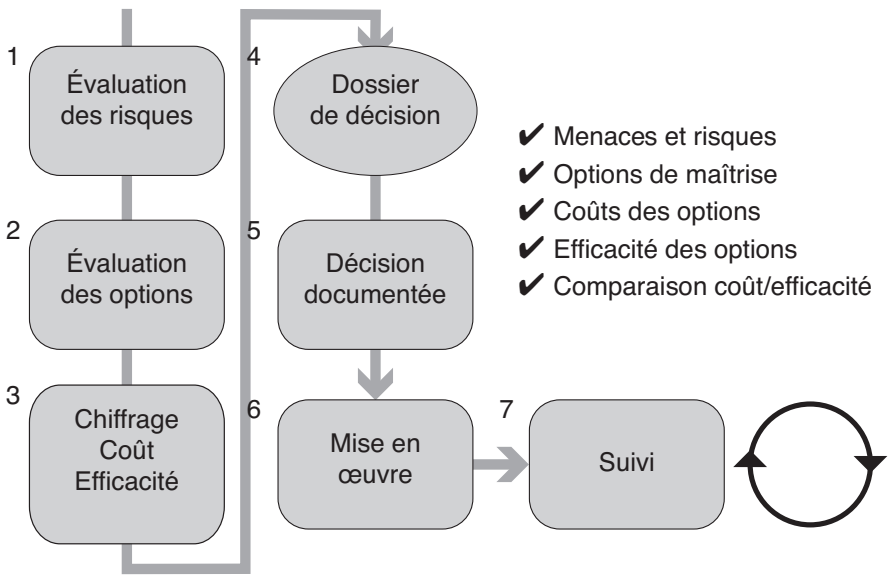

Figure 1-1 : Synoptique de la démarche de maîtrise des risques

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 33).

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 33).

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'occurrences 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 » est illustrée par le tableau 1-2.

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 représenté par le tableau 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.

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.

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

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 raisonnements 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*).

Il faut noter à ce sujet que les valorisations qualitatives sont souvent les plus faciles à réaliser rapidement dans les entreprises qui n'ont pas forcément une culture du chiffre. La plupart du temps, il vaut mieux un chiffrage rapide par ce moyen qu'aucun chiffrage du tout par difficulté à « donner un montant ».

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 A*nnualized* R*ate of* T*hreat 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 informatique, 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 1-2 donne un exemple de suivi des crues de la Loire.

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.).

www.vigicrues.ecologie.gouv.fr

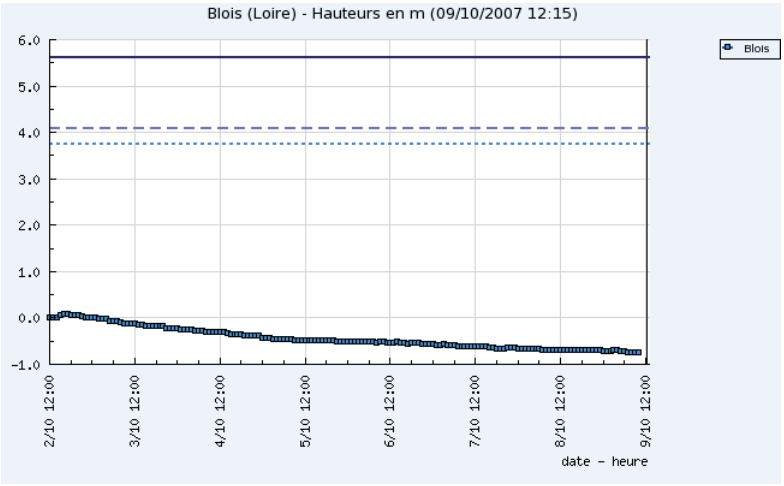

Figure 1-2 : Les crues de la Loire constatées à Blois

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.

Enfin, il est également possible de donner des estimations de type « fréquent », « peu fréquent », « très rare » ou des chiffrages équivalents (3, 2 ou 1) pour accélérer les études. Cela suppose souvent d'interroger des personnes d'expérience dans l'entreprise.

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.

Il et aussi possible de noter ces éléments sur un schéma cartésien et de réaliser ce qu'on appelle souvent une « cartographie des risques ».

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 la moyenne des pertes annuelles 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 Impact Expectancy* ou AIE) est calculée à partir de la valorisation qualitative de ces impacts (SIE ou S*ingle Impact Expectancy*), 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 la moyenne des impacts annualisés

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.

Cartographie des risques

Disposant de chiffres mesurant les impacts et les probabilités, il est possible de réaliser un schéma cartésien avec :

- en ordonnée, les impacts ou pertes ;
- en abscisse, les probabilités.

On obtient alors un schéma tel que celui-ci :

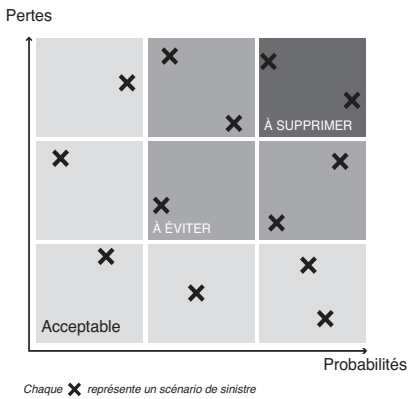

Figure 1-3 : Cartographie des risques

Il est clair que les événements qui se situent en haut à droite (donc probables et de fort impact) sont ceux que l'on veut éliminer en priorité.

De manière similaire, 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.

Ces approches graphiques sont faciles à réaliser quand on dispose des chiffres et très utiles en réunion pour facilement situer les enjeux.

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**
Batchs 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 *batchs 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 batchs de nuit non terminés).
- Du point de vue de l'informatique, deux événements sont plus menaçants que les autres, tous départements confondus : les batchs 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 batchs 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 batchs 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.

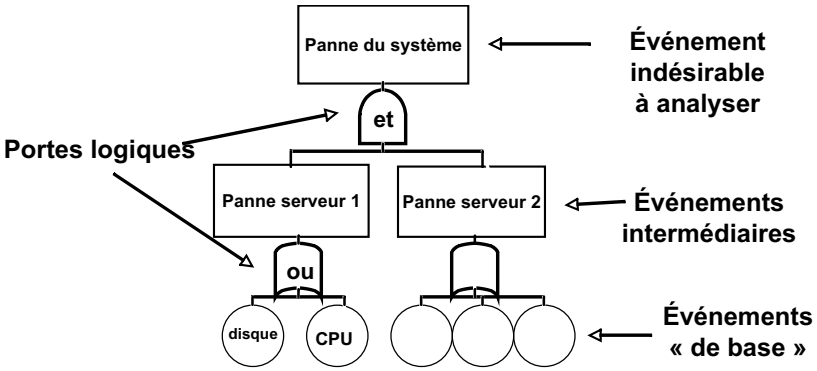

Figure 1-4 : Exemple simplifié d'un arbre de défaillance

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 coûts, 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 33) 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 20), 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.

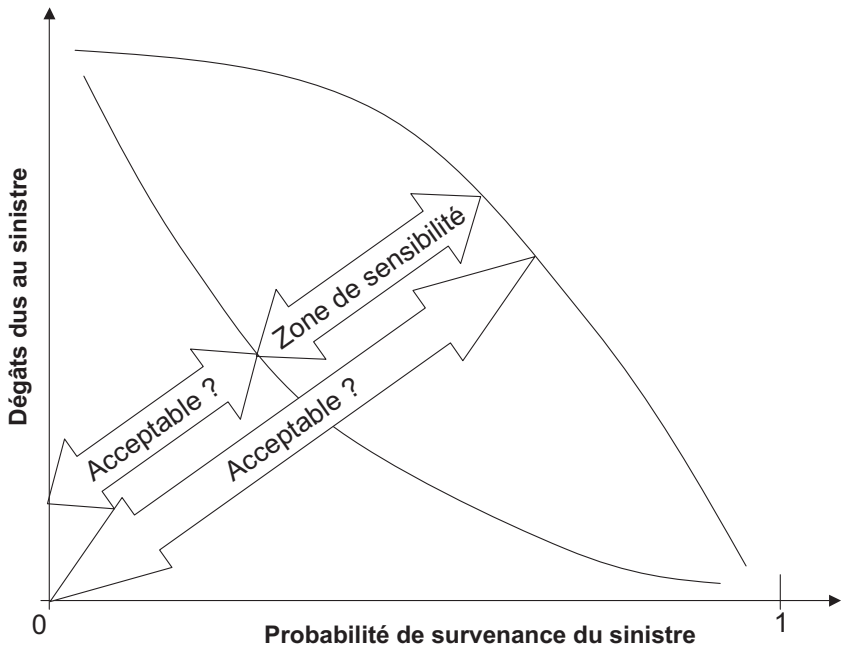

Figure 1-5 : Zone d'aversion variable au risque

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

Vocabulaire

On notera avec le sourire que les Anglo-Saxons préfèrent parler de *risk appetite*, donc d'appétit du risque en lieu et place de l'aversion au risque, renversant ainsi la vision !