

**Yves Métayer
Laurence Hirsch**

Premiers pas dans le management des risques

Premiers pas
dans le
management
des **risques**

**Yves Métayer
Laurence Hirsch**

Premiers pas dans le management des risques

© AFNOR, 2007
ISBN : 978-2-12-465102-3

Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, des pages publiées dans le présent ouvrage, faite sans l'autorisation de l'éditeur est illicite et constitue une contrefaçon. Seules sont autorisées, d'une part, les reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective et, d'autre part, les analyses et courtes citations justifiées par le caractère scientifique ou d'information de l'œuvre dans laquelle elles sont incorporées (Loi du 1^{er} juillet 1992 – art. L 122-4 et L 122-5, et Code pénal art. 425).

AFNOR – 11, rue Francis de Pressensé, 93571 La Plaine Saint-Denis Cedex

Tél. : +33 (0)1 41 62 80 00 – www.afnor.org

Sommaire

Introduction	VII
---------------------------	------------

Partie 0 **Présentation générale**

1	À qui est destiné cet ouvrage	3
1.1	Pour les décideurs : un ouvrage global	3
1.2	Pour les décideurs, les acteurs directs du management des risques : un ouvrage pratique	4
1.3	Pour les décideurs, les acteurs directs du management des risques et les « apprenants » : un ouvrage pédagogique.	6
2	Notion de risque	9
2.1	Il n'y a risque que s'il y a menace et cible.....	9
2.2	Le risque et la vie sont indissociables.....	11
2.3	Le b.a.-ba du management des risques : la criticité et le diagramme de Farmer	10
2.4	Le principe de précaution	12
2.5	<i>Errare humanum est, perseverare diabolicum</i>	12
2.6	Les grandes catastrophes sont la résultante de petits risques non maîtrisés	13

Partie I

Les risques : les définir et les comprendre

3	Fiabilité humaine	17
3.1	L'homme au milieu des processus.....	18
3.2	L'opérateur humain présente quelques caractéristiques singulières.....	19
3.3	Les relations homme-machine.....	22
3.4	Stabilité et instabilité	29
3.5	Notion de crise.....	30
4	Fonctionnement d'une entreprise	33
4.1	Modélisation d'une entreprise	33
4.2	Les trois domaines de fonctionnement (plus un).....	37
4.3	Le management.....	39
4.4	Qualité et risques	44

Partie II

Les risques : comment les maîtriser

5	Management des risques	47
5.1	Management, maîtrise, gestion des risques	47
5.2	Maîtrise des risques : notions élémentaires	48
5.3	Maîtrise des risques : identification.....	50
5.4	Maîtrise des risques : évaluation et caractérisation	52
5.5	Management des risques : le rôle des dirigeants	54
6	Les familles de risques	61
6.1	Risques processus	62
6.2	Risques projet	72
6.3	Risques humains	82
6.4	Risques financiers.....	86
6.5	Risques clients.....	93
6.6	Risques ressources internes et externes	98
6.7	Risques juridiques.....	105
6.8	Risques environnementaux.....	109
6.9	Risques éthiques	114
	Conclusion	125
	Annexes	127
	Bibliographie	133

Introduction

Écrit par un retraité et par une étudiante, nous avons essayé de « jouer la diversité » pour proposer cet ouvrage conçu, nous l'espérons, pour des publics également assez divers. Nous avons pensé aux décideurs, pressés et soucieux d'avoir une vue globale, aux experts et professionnels, impliqués et soucieux d'assumer au mieux leurs responsabilités, aux étudiants, enfin, curieux et soucieux de faire leurs premiers pas en entreprise dans les meilleures conditions possibles.

Nous avons aussi essayé d'en rendre la lecture fluide, y compris en y insérant des clins d'œil que ceux qui ne les partageront pas voudront bien nous pardonner.

Notre ambition est que vous preniez autant de plaisir et d'intérêt à le lire que nous à le concevoir et à l'écrire.

Les auteurs

Partie 0

Présentation générale

1

À qui est destiné cet ouvrage

1.1 Pour les décideurs : un ouvrage global

Il n'est pas excessivement caricatural de dire que deux choses, et seulement deux, préoccupent les dirigeants d'entreprise :

- la faillite de leur entreprise ou de leur groupe ;
- aller en prison avant la retraite.

Ces soucis suffisent largement à occuper leurs journées et même souvent leurs nuits.

Les méthodes qui permettent de maîtriser ces risques ont été développées au gré de la perception qu'ont eue les dirigeants des risques qu'ils couraient ou faisaient courir à leur entreprise. Ces méthodes, quand elles ont été dignes de passer à la postérité par le biais du papier imprimé, ont donc été la matière première d'ouvrages dont on peut deviner, dès la lecture du sommaire, par qui ils ont été écrits et dans quel domaine l'auteur exerçait son activité.

Or les dirigeants ont besoin d'un ouvrage leur permettant de « comprendre » en peu de temps. Pour pouvoir travailler et dormir tranquilles, ils doivent également être certains que l'ensemble des collaborateurs de leur entreprise, et aussi leurs partenaires, sont convenablement imprégnés d'une « culture risques » commune, partagée et suffisante.

1.1.1 L'entreprise est un tout : on gagne ou on perd ensemble

Le management des risques est une discipline parfaitement transverse à l'entreprise. Ceux qui font courir les risques ne sont pas forcément (et même pas souvent...) ceux qui en subissent les conséquences. Un risque, pour peu qu'il soit important, est la plupart du temps le résultat de dangers dont la parade est entre des mains différentes. Les signaux ne sont pas toujours perçus par ceux qui vont les subir.

Bref, comme dans une équipe sportive, c'est presque toujours ensemble que les composantes de l'entreprise gagnent ou perdent la partie.

1.1.2 Manager une entreprise, c'est maîtriser ses risques

En ce qui concerne les risques internes, c'est évident et n'appelle pas de commentaire. En ce qui concerne les risques externes aussi, bien sûr, mais avec deux différences fondamentales : d'une part on peut – doit – se reposer sur les autres pour maîtriser certains risques, d'autre part on peut être frappé d'un sentiment d'impuissance. À un président de compagnie aérienne qui vantait la performance de son entreprise, on a demandé : « Monsieur le Président, comment faites-vous pour réussir si bien, alors que les risques les plus importants qui vous menacent sont l'encombrement du ciel aérien et la météo, deux éléments sur lesquels vous ne pouvez absolument rien ? »... et la réponse a été : « c'est justement parce que c'est impossible que nous savons faire, et que nous sommes les meilleurs ! ».

Bref, c'est parce que l'entreprise sait déployer une politique de maîtrise des risques efficace, et pour les risques de toutes natures, qu'elle réussit durablement.

1.2 Pour les décideurs, les acteurs directs du management des risques : un ouvrage pratique

1.2.1 Une discipline qui s'apprend, mais pas à l'école

On ne naît pas *risk manager*, on n'est pas non plus formé spécifiquement à cela. On le devient le plus souvent par hasard et par la nécessité de l'entreprise. Comme l'auteur en a fait l'expérience lui-même, il n'existe pas une « bible » du management des risques. Il n'y a pas eu dans l'histoire des risques un personnage tel que Deming ou Shiba dans le domaine de la qualité. Il n'y a donc pas d'ouvrage global – ou plutôt il n'y en avait pas jusqu'à une période

récente – qui permette d’acquérir la conviction raisonnable qu’on n’est pas passé à côté de quelque chose d’essentiel.

Pourtant, les « professeurs de risques » ne manquent pas : tous parfaitement convaincus qu’ils ont fait le tour du problème, et que leur méthode est la seule et la bonne. Loin de nous l’idée de proclamer qu’il n’en est pas de sérieux : mais notre souci est d’aider ceux qui vont devoir choisir, à le faire en toute connaissance de cause, à l’abri des jargons et des modes.

Cet ouvrage est donc aussi destiné aux « acteurs directs » au début de leur carrière, et aussi de temps en temps au cours de celle-ci, s’ils éprouvent le besoin de « recalcr » leurs connaissances. Il se doit donc d’être pratique, simple, d’accès facile et non séquentiel.

1.2.2 Une discipline globale et de tous les instants

On vient de dire plus haut que le management des risques était l’affaire de tous. Ce qui signifie qu’il est souhaitable que tout le monde, dans l’entreprise, s’en préoccupe, et si possible de la même façon. Mais c’est également l’affaire de tout : toutes les ressources de l’entreprise, et pas seulement les ressources humaines, tous les processus, toutes ses parties prenantes, sont cibles des dangers qui les guettent et causes des risques qu’ils font courir aux autres.

C’est enfin l’affaire de tout le temps. Comme on le verra par la suite, les approches actuelles ont tendance à privilégier l’amélioration, certes, mais de façon discontinue : le but de cet ouvrage est d’initier une démarche beaucoup plus permanente et progressive. Avec moins de douleur ? Peut-être. En tout cas avec plus d’efficacité, nous l’espérons.

1.2.3 Risques et qualité : un même combat

On vient déjà, sans encore l’expliquer, de parler « d’amélioration continue », de « parties prenantes »... c’est le vocabulaire de la qualité. Cette communauté de vocabulaire révèle une analogie presque complète avec les méthodes et outils développés pour la qualité. C’est un point sur lequel il conviendra de s’appuyer si l’entreprise a lancé de telles démarches. C’est aussi, pour celles qui ne l’ont pas (encore !) fait, une autre façon d’entrer dans de telles démarches. Façon présentant des avantages et des inconvénients, qui devront être évalués à la lumière de la culture et de la stratégie de l’entreprise.

1.3 Pour les décideurs, les acteurs directs du management des risques et les « apprenants » : un ouvrage pédagogique

1.3.1 Tout le monde devrait savoir faire

Les deux « cibles » évoquées plus haut sont évidemment aussi des apprenants ; il faut y ajouter tous ceux qui ont besoin d'avoir des notions simples et pratiques sur le management des risques. Pour ne citer que deux grandes catégories, il y a les étudiants, et puis l'immense groupe que représentent les collaborateurs de l'entreprise concernés par une démarche MDR (management des risques), sans appartenir à la catégorie des « acteurs directs » évoqués précédemment.

Ces « apprenants » ont besoin d'un ouvrage qui présente deux caractéristiques particulières : il doit être assez « généraliste » (plutôt qu'exhaustif) pour permettre d'aborder les risques quels que soient leur nature et le contexte, et pédagogique, c'est-à-dire permettre aux lecteurs d'assimiler des principes simples, voire des images mentales performantes.

1.3.2 Assimiler des invariants simples

Les invariants sont présentés dans les premiers chapitres. Ils s'appliquent à tous les types de risques, et constituent ainsi la base des méthodologies du management des risques. *A priori*, ils ne font pas appel à des connaissances particulières, sauf à ce vieux bon sens qui, parfois, fait défaut.

Mais qu'on ne s'y trompe pas : ils sont aussi l'ossature d'une culture « risques » pour l'entreprise. En effet, quelle culture peut durablement imprégner un corps social si une langue commune n'y est pas pratiquée ? Comment agir vite, et sûrement, si un certain nombre de réflexes – y compris la mise en œuvre d'outils – ne sont pas présents chez toutes les parties prenantes, et en premier lieu les collaborateurs ?

1.3.3 Être capable d'esprit critique

La première illusion d'optique à laquelle le *risk manager* est confronté est l'apparent paradoxe entre la rigueur des méthodes ou outils proposés, et la nécessité récurrente de faire des approximations, voire des impasses. Quand on analyse un grand nombre, certains se focalisent sur les deux derniers chiffres et d'autres sur les deux premiers...

La raison en est tout simplement que le management des risques n'est pas une science exacte ! Et comme toutes les sciences « molles » (sans donner le moins du monde une valeur péjorative à ce mot), la discrimination entre le vrai et le faux, le négligeable et l'important, le fait et la perception, est particulièrement difficile. Il est donc particulièrement difficile d'y voir clair dans les affirmations, les méthodes et les outils du genre « couteau suisse », et de savoir à qui faire confiance parmi ceux qui les défendent parce que cela correspond à leurs enjeux souvent un peu trop personnels.

2

Notion de risque

2.1 Il n'y a risque que s'il y a menace et cible

C'est évident, mais on l'oublie : la pire des menaces n'est rien si... elle n'est une menace pour personne.

Au passage, notons que nous avons préféré « menace » à « danger », pour une raison importante : on peut transformer une menace en opportunité, pas un danger. Mais nous n'irons pas, comme certains auteurs, jusqu'à écrire qu'au-delà des risques « négatifs », qui correspondent au sens habituel du terme, il existe des risques « positifs », que l'on peut manager de la même façon. Ce point de vue est séduisant, mais en théorie seulement. En pratique il se heurte, précisément, au bon sens, et oblige(rait) les parties prenantes de l'entreprise à une gymnastique intellectuelle peu efficiente, voire dangereuse.

Pour en revenir au sujet, cette coïncidence nécessaire de la menace et de la cible fournit la première façon de maîtriser un risque, et souvent la plus simple et la plus efficace. Plutôt que d'essayer de l'éliminer ou de minorer la menace ou ses effets, il suffit de soustraire la cible : pour ne pas se faire fracasser le crâne par un pot de fleurs, il est plus astucieux de s'éloigner du balcon que de prendre un casque !

Pour illustrer ces propos, le schéma simple ci-dessous (Figure 2.1) montre que le management d'un risque passe par la diminution de la zone de recouvrement entre la cible que représente le système, et la menace.

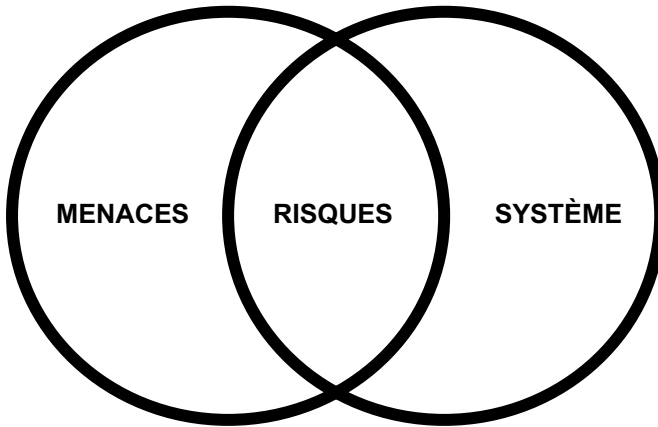


Figure 2.1 Naissance d'un risque

2.2 Le risque et la vie sont indissociables

« Qui ne risque rien n'a rien », pour ne citer qu'un de nos proverbes les plus courants : il est bien dans notre culture d'admettre cela. Les Gaulois d'Astérix, qui ne craignent aucun danger, et qui ne courent donc aucun risque, n'ont peur que de la chute du ciel. Plus récemment, des scientifiques ont fait circuler l'idée que la vie humaine va devenir (médicalement et théoriquement) infinie : parmi les nombreuses questions qu'une telle situation posera(it), il en est une majeure : la seule façon de mourir serait un accident, et donc plus personne ne prendrait le moindre risque !

Autre brève de comptoir, il est bien connu que si on prend moins de risques, la vie n'est pas forcément plus longue, mais elle le paraît...

2.3 Le b.a.-ba du management des risques : la criticité et le diagramme de Farmer

De façon totalement générale, un risque (après avoir été identifié, ce qui est l'objet du chapitre 5.3) se déplace dans un espace à deux dimensions :

- la probabilité de son occurrence ;
- la gravité de ses effets.

Ce qui permet de définir sa **criticité**, nombre obtenu en faisant le produit de la probabilité par la gravité. Ce sont les trois paramètres essentiels qui définissent un risque, ou plus précisément qui servent à sa **caractérisation**. On verra au chapitre 5 qu'il ne s'agit pas toujours d'une simple multiplication entre des nombres faciles à calculer...

La « caractérisation » des risques, puis leur « hiérarchisation » passent alors toujours par une cartographie qui se présente comme le schéma ci-dessous (Figure 2.2). Les zones d'acceptabilité figurées grossièrement sur le schéma sont affinées afin d'en déduire, comme on le verra plus loin, le plan d'action de maîtrise des risques.

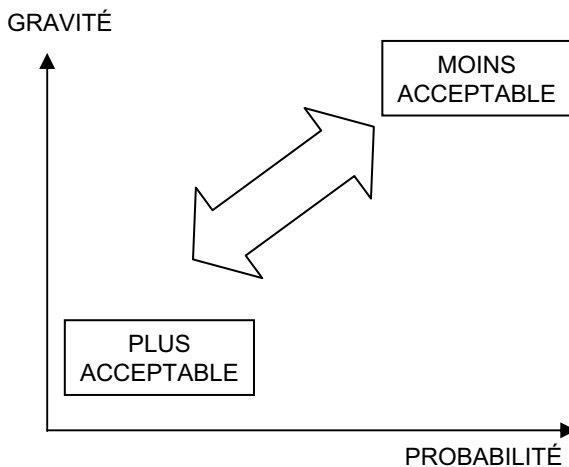


Figure 2.2 La cartographie des risques : diagramme de Farmer

2.4 Le principe de précaution

Il faut traiter les risques, mais on ne peut pas traiter tous les risques, au moins simultanément. On sait bien que les ressources sont limitées. La tendance naturelle est donc de tracer une ligne diagonale – ou une hyperbole pour ceux qui veulent croire qu'ils ont trouvé la façon absolue de calculer la criticité (nous exprimons plus loin notre point de vue sur ce point).

Il « suffit » de décider qu'on va commencer par traiter les risques dont la criticité est la plus grande. Ils se situent en haut et à droite (Figure 2.3). On s'arrêtera sur le trait qu'on aura tracé.

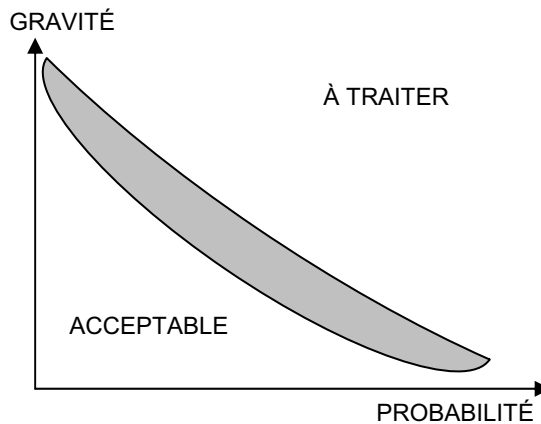


Figure 2.3 Zone d'acceptabilité d'un risque

Simple ? Pas tant que cela... Tout cela n'est pas connu avec précision : quelle doit être la largeur du trait ? Le tracer très étroit est malhonnête ; le tracer trop large est lâche – et surtout inefficace.

Appliquer le principe de précaution, c'est tracer une zone tellement large qu'elle couvre toute la surface du graphique. Le lecteur choisira pour qualifier cette attitude un des adjectifs du paragraphe précédent... à moins qu'il ne lui en vienne un autre à l'esprit.

2.5 *Errare humanum est, perseverare diabolicum*

« Se tromper est humain, persévérer est diabolique » : tout le monde a entendu ce proverbe, quelquefois connu sous une forme plus moderne « on n'a pas le droit de faire deux fois la même bêtise ».

Cette idée a deux conséquences majeures quand on parle de maîtrise des risques :

- Une menace mal connue peut générer un risque estimé acceptable tant qu’aucune cible n’a été touchée, et le même risque devient inacceptable dès l’instant où l’événement s’est produit... « plus jamais ça ».
- Le niveau d’exigence des parties prenantes est, comme l’entropie de l’univers, appelé à croître indéfiniment : l’entreprise est donc absolument obligée de faire croître la performance de son système de maîtrise des risques au moins aussi vite que l’exigence de ses parties prenantes. Sauf cas particulier – et sans doute assez rare – d’une entreprise qui saurait tout naturellement « auto générer » son progrès de façon suffisamment anticipative, tout le monde est donc condamné, de gré ou de force, à mettre en place un système d’amélioration continue formalisé.

2.6 Les grandes catastrophes sont la résultante de petits risques non maîtrisés

Chère lectrice, cher lecteur, combien faites-vous de vraies bêtises par an ? Nous entendons par là des erreurs ou fautes ayant des conséquences significatives ou graves sur vous ou votre entourage. Sauf si vous êtes un cas très particulier, vous allez répondre « plus de 1 – moins de 100 – entre 2 et 10 ». Faites l’expérience en groupe !

Traduit en d’autres termes, ceci signifie que, chaque jour de votre (notre) vie, nous avons – très approximativement – une « chance » sur 100 de faire une erreur d’importance.

Et combien de « chances » estimez-vous avoir, d’être pris dans un accident d’avion, de vivre de près l’explosion d’une centrale nucléaire ou d’une usine chimique, ou encore de ne pas revenir vivant de votre travail ? Vous aurez de la peine, sauf si vous vous êtes déjà penché sur la question, à répondre par un nombre. Ce genre d’événement n’est certes pas impossible, puisqu’il s’est déjà produit. Mais ailleurs, avec d’autres. Quant aux accidents du même genre qui n’ont pas encore eu lieu, encore plus difficile...

Traduit dans les mêmes termes que plus haut, cela signifie que vous estimez que la probabilité de ce qu’on appelle une catastrophe est égale à une « chance » sur un million, ou encore moins. Vous avez raison ! Pour simplifier – nous demandons pardon aux experts des statistiques – cela signifie donc qu’il faut la conjonction de 4, 5, 6 erreurs indépendantes pour provoquer une catastrophe.

Conséquence (apparemment !) optimiste, il suffit donc de maîtriser une seule de la série d'erreurs, en d'autres termes d'en maîtriser le risque, pour éviter la catastrophe (nous parlerons ensuite de crise, mais cela revient au même).

Facile !

Mais quel risque ? C'est l'objet des premiers chapitres de ce livre.

Et comment ? C'est l'objet des suivants.

Partie I

Les risques : les définir et les comprendre

3

Fiabilité humaine

L'homme est faillible, c'est une évidence, mais pendant longtemps cette idée a été taboue dans les entreprises. C'est là le résultat de décennies d'évolution des mentalités, et il n'est pas sans liens étroits avec la culture de la société dans laquelle l'entreprise est insérée. On ne réagit pas à l'erreur de la même façon au Japon et en Europe, en Europe anglo-saxonne et en Europe latine, à Troudorf-le-Haut et à Troudorf-le-Bas. Pour ne citer que quelques exemples caricaturaux, les idées qui suivent trouvent encore preneur, voire propagateur :

- si l'employé fait une erreur, il faut le punir ;
- si l'employé fait une erreur, ce n'est pas sa faute mais celle de l'entreprise, du patron, des clients, à « pas d'chance »... ;
- l'employé ne peut pas faire d'erreur, et son entreprise – plus souvent son administration – ne peut donc pas en avoir fait non plus.

La performance de la machine humaine, en particulier en situation complexe, et les développements associés pour une meilleure connaissance de l'interface homme-machine, sont donc des disciplines dont le développement et la diffusion sont assez récents.

Le chapitre qui suit est très largement inspiré d'un ouvrage qui a fait référence dès sa parution : « Catastrophes ? Non merci ! », dont on trouvera les caractéristiques en bibliographie. Que ses auteurs veuillent bien, si ce modeste ouvrage tombe entre leurs mains, pardonner l'imperfection des lignes qui suivent.

3.1 L'homme au milieu des processus

L'homme communique intensément avec son environnement, et ceci par des médias très variés :

- en réception : ses 5 sens (+ le 6^e pour certains), les instruments qu'il lit, les procédures qu'il connaît ou qu'il découvre ;
- en émission : il agit, conçoit ou fait agir des automatismes, écrit ou impose des procédures.

Et tout ceci dans un champ de contraintes issues de ses paramètres personnels et de son environnement (Figure 3.1).

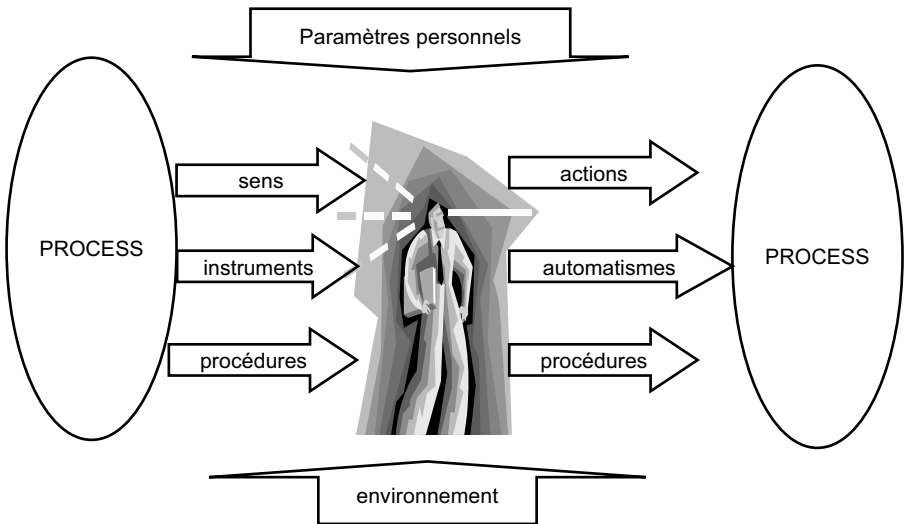


Figure 3.1 L'homme au centre des processus

Oublier l'un de ces aspects, quand on regarde fonctionner la machine humaine, expose son raisonnement ou ses actes à des lacunes.

Or cette machine est loin, très loin, de fonctionner comme un automate (en bon état). Ses performances, comme on va le voir plus loin, sont à la fois médiocres et très supérieures à celles d'un automate.

3.2 L'opérateur humain présente quelques caractéristiques singulières

Nous n'entrerons pas dans le débat des différences de comportement selon les sexes : quelques ouvrages, dont certains ont connu une large diffusion – et c'est tant mieux – ont contribué à répandre quelques idées intéressantes sur ce vaste et vital sujet. Mais nous nous plaçons ici dans une entreprise qui ne pratique aucune sorte de ségrégation, il nous faut donc descendre de notre planète, et à la fois bien entendre et savoir lire une carte routière...

3.2.1 Il fonctionne en canal unique

L'homme fonctionne de façon quasi mono tâche, du moins dans son action consciente. Sans atteindre le cas, assez grave pour un tel personnage, d'un président qui ne pouvait pas à la fois descendre un escalier et mâcher du chewing-gum sans rater une marche, il y a un peu de cela dans notre fonctionnement. Une information n'est reçue que si elle veut être entendue : crier plus fort n'est pas forcément suffisant pour se faire entendre, bien au contraire.

Dans son fonctionnement un peu plus inconscient, l'homme est un peu plus multitâche : il peut quand même prendre des notes en écoutant, ou conduire en parlant. Mais les « couches » dans lesquelles ces tâches s'exécutent sont étanches, et passer de l'une à l'autre constitue une perturbation.

L'homme peut également avoir un comportement totalement réflexe. Il est alors proche de l'automate : il réagit de façon prévisible (encore que...) et ceci lui demande peu d'énergie. Repasser au conscient demande donc un effort qui peut être douloureux.

3.2.2 Il s'adapte à la charge de travail

L'homme est une machine à vitesse variable, et cette vitesse peut atteindre des valeurs très élevées. Bien mieux, la vitesse à laquelle il doit travailler le conduit à augmenter sa performance... pendant un certain temps. Mais au risque de générer de plus en plus d'erreurs. Et au prix, surtout d'une fatigue qui croît et qui ne se résorbe ensuite que très lentement.

Inversement, l'homme peut fonctionner à vitesse réduite – en veille. Mais, et c'est un paradoxe, cela le fatigue aussi, et contribue tôt ou tard à diminuer sa performance. Bref l'homme n'est pas une machine car il est animé par quelque chose de bien plus subtil qu'une prise électrique ou un animal de trait.

3.2.3 Il a besoin d'informations pour fonctionner

Rien de pire pour un cerveau de ne pas recevoir d'information. Et même d'informations qui évoluent : la perception d'une information – tout à fait réelle et significative – mais qui ne bouge pas (feu rouge, écran immobile...) le lasse vite et il ne perçoit plus l'information, ni éventuellement ses changements. Inversement il est attiré par ce qui bouge même si ce qui est immobile est plus important – même s'il en est conscient. Qui n'a pas vécu cela à un carrefour un soir d'été...

Dans un autre domaine, qui n'est pas celui traité ici, on n'a pas trouvé mieux que l'isolement pour démoraliser un prisonnier... ou un cadre dont on veut se débarrasser.

3.2.4 Il est capable d'anticipation

À partir de situations qu'il reconnaît, ou bien grâce à un raisonnement qu'il a appris à faire, l'homme peut anticiper l'évolution des informations qu'il reçoit. Ceci est évidemment un grand avantage sur la machine – qui essaie d'ailleurs de l'imiter grâce aux algorithmes de plus en plus sophistiqués soutenus par des puissances de calcul et de stockage de données de plus en plus importantes. En effet, cette capacité d'anticipation compense le fait qu'il fonctionne en canal unique : il peut alors se consacrer à d'autres tâches.

C'est aussi une faiblesse si cette capacité est mal maîtrisée : elle conduit forcément à une perte de vigilance qui peut être très lourde de conséquences si la situation n'évolue pas comme l'opérateur l'a prévue, et/ou si les informations qu'il a choisies pour sa veille ne sont pas pertinentes.

3.2.5 Il estime mal les risques

L'homme est un optimiste incorrigible. Si cette caractéristique – pas toujours reconnue – est plutôt une bonne chose dans la vie en couple et en société, il induit une augmentation des risques qu'il doit maîtriser ou fait courir, et ceci d'autant plus qu'il est sous stress.

Comme on l'a déjà vu rapidement, et qu'on le verra plus en détail dans le chapitre 6, on ne maîtrise bien les risques que si on sait en évaluer probabilité et gravité. Sans évaluation correcte, pas de traitement correct, et donc des erreurs d'autant plus gênantes qu'elles mettent l'opérateur dans une sorte de spirale qui l'entraîne dans un stress toujours plus grand et dans de nouvelles erreurs toujours plus graves.

Ce fait a des conséquences tout à fait majeures quand on traite de maîtrise des risques : plus on s'éloigne du domaine de fonctionnement normal, pour aller vers l'incident ou l'accident, plus la perception de la gravité se détériore. Autrement dit, plus la situation est grave, complexe, mal reconnue, peu fréquente, et plus il faut donner à l'opérateur des informations formalisées, simples et claires !

Si ce modeste ouvrage pouvait conforter cette idée dans l'esprit du lecteur, nous aurions la faiblesse de penser qu'il n'aurait pas totalement gaspillé son temps en le lisant.

3.2.6 Les différents types d'erreur

On peut répartir les erreurs en six catégories. Comme toute classification, elle est insuffisante et réductrice, mais elle nous semble permettre de ne rien oublier de trop important :

- Erreur de perception : information masquée, perdue dans une foule d'autres, pas assez « violente » pour attirer l'attention... Qui n'a pas ignoré un ami perdu dans une foule ?
- Erreur de décodage et de représentation : non-compréhension ou interprétation erronée d'un signal, d'un symbole... Qui ne s'est jamais brûlé les mains avec un mitigeur aux symboles trop « esthétiques » ?
- Non-respect d'un mode opératoire ou d'une réglementation : volontaire ou non... Qui n'a pas franchi un « stop » un peu vite en l'absence de toute circulation ?
- Erreur de communication : un mot pour un autre, une phrase dite trop vite... Qui ne s'est pas disputé sur un malentendu ?
- Non-prise de décision en temps voulu : « il aurait fallu »... Qui n'a pas regretté le mot qu'il fallait dire, le geste qu'il fallait faire ?
- Action mal séquencée ou mal dosée : inversion de l'ordre des gestes à faire, efforts trop ou pas assez importants... Qui n'a pas cassé un jouet en le sollicitant un peu trop ?

3.3 Les relations homme-machine

3.3.1 Les interfaces

Nous avons vu – ou plutôt effleuré – dans le chapitre précédent ce qui peut se passer dans le cerveau d'un bipède plantigrade de type homo sapiens qui fait une erreur. Nous avons vu au début du même chapitre que l'homme est au centre des processus. Il joue donc un rôle d'interface, et il nous semble possible de proposer sans grande démonstration l'idée que les risques naissent surtout aux interfaces. D'où leur importance.

On en distingue plusieurs types :

- Les informations que l'homme reçoit d'un système : conception de l'instrument, emplacement, clarté de l'échelle, pertinence du paramètre mesuré, etc.
- Les informations et les ordres que l'opérateur envoie vers le système : conception du « levier » de l'action, emplacement, effort à fournir, mais aussi clarté de la relation entre le geste et l'effet attendu.
- Les échanges entre les hommes : précision des mots, exactitude de la relation entre le mot et le fait, et bien entendu différence de langues...
- L'action et la perception des boucles de contrôle : exactitude de la relation entre le geste et l'effet produit, perception claire de la relation entre le phénomène et le paramètre mesuré...
- La gestion des piles d'actions : procédures explicites ou implicites, habitudes...
- La gestion des modèles : représentation mentale du système piloté, ainsi que et surtout, le cas échéant, l'appréciation de son état de dégradation.

3.3.2 Quelques principes (apparemment) simples

Ce n'est pas ici le lieu de rédiger un traité d'ergonomie, mais nous citerons quelques principes issus de notre expérience et de la littérature spécialisée (*cf.* bibliographie en fin d'ouvrage) qui nous semblent susceptibles de guider les choix et l'élaboration des plans de maîtrise de risques :

- mettre à disposition des informations exactes et pertinentes vis-à-vis du phénomène qu'on veut illustrer ; des informations simples et sans ambiguïté possible ;
- fournir toutes les informations utiles, et seulement les informations utiles ;

- fournir des informations permettant la prévision, l'anticipation, et le recoupement avec d'autres informations élaborées de façon indépendante ;
- simplifier au maximum les modes opératoires, et d'autant plus s'ils doivent être utilisés sous stress ;
- concevoir des modes opératoires « auto-pardonnants », c'est-à-dire permettant de guider l'opérateur même s'il se trompe de chemin, ou si l'itinéraire doit varier de façon dérangeante ;
- étudier de façon exhaustive, réaliste, si possible en situation réelle, les commandes et les effets de ces commandes.

3.3.3 Documentation et système d'information

Nous vivons à l'ère de l'information, c'est bien connu et on dit que c'est nouveau. Soit. Ce qui n'est pas nouveau, en revanche, c'est que nous sommes toujours dans la civilisation de l'écrit. Internet n'a fait, curieusement, que renforcer ce fait tout en changeant le support et souvent, hélas, la forme. Nous parlerons donc dans ce qui suit de « documentation » en faisant abstraction du système d'information associé : l'objet est plus important que le support, et plus simple à appréhender.

La documentation qui contient, peu ou prou, le savoir-faire d'une entreprise est un élément essentiel de sa robustesse. Nous avons prélevé sur un site Internet prestigieux (*cf.* bibliographie en fin d'ouvrage) les caractéristiques qui définissent la qualité d'une documentation :

- définition des responsabilités ;
- cycle de vie et état des documents ;
- présentation et structure de la documentation ;
- outils de gestion de la documentation ;
- classement de la documentation.

Parfait ! Tout ce qui est cité est en effet essentiel... Mais révélateur ! Rien sur le contenu, comme si les rédacteurs n'avaient besoin que de feuilles de style et d'organigrammes...

Il n'est pas là non plus question de rédiger un manuel du parfait petit documentaliste. Quelques principes simples cependant :

- La documentation doit être accessible par tous ceux qui en ont besoin, au bon moment et à l'endroit où ils sont.

- Elle doit être la plus simple possible ; comme disait un artiste célèbre : « la perfection, ce n'est pas quand il n'y a plus rien à ajouter, c'est quand il n'y a plus rien à enlever ».
- Elle doit être adaptée à celui qui l'utilise : langage, mots, pictogrammes... Trois coups de peinture sur un plancher valent mieux qu'une note décrivant un itinéraire !
- Elle doit être exacte, et donc mise à jour aussi souvent que les évolutions du contexte le rendent nécessaire.
- Elle doit être adaptée aux circonstances : on n'écrit pas de la même façon pour un opérateur tranquille et un opérateur sous stress.
- Elle ne doit pas être culpabilisante – on a vu plus haut que les modes opératoires doivent être « auto-pardonnants ».
- Elle doit garantir sa propre traçabilité (mise à jour, diffusion...) et permettre la traçabilité des actes et des événements.
- Elle doit respecter les lois et règlements en vigueur.

Pour revenir au système d'information, en une phrase, nous dirons simplement qu'il a pour rôle de permettre à la documentation de respecter les principes ci-dessus, et ceux que nous n'avons pas cités parce qu'ils lui sont plus intrinsèques (fiabilité, etc.).

3.3.4 Les modes opératoires

Ce qui précède a des conséquences importantes sur la structure des documents d'action, ou « modes opératoires » ou encore « procédures ». La première de ces conséquences est qu'il n'est pas possible de rédiger des modes opératoires de type « couteau suisse » qui feraient face à toutes les situations :

- les modes opératoires relatifs au fonctionnement normal peuvent aussi couvrir le domaine incidentel ;
- les modes opératoires relatifs aux domaines incidentel et accidentel peuvent être regroupés sous le vocable « plan d'urgence » ;
- les modes opératoires du domaine accidentel peuvent être identifiés comme tout ou partie des « plans de sauvegarde » ;
- les plans de sauvegarde peuvent, ou non, déborder vers les événements qu'on a définis comme « hors plan » parce que trop improbables... ou, malheureusement, parce qu'impossibles *a priori* à imaginer, décrire et traiter.

La figure ci-après (Figure 3.2) illustre un empilement possible des documents.

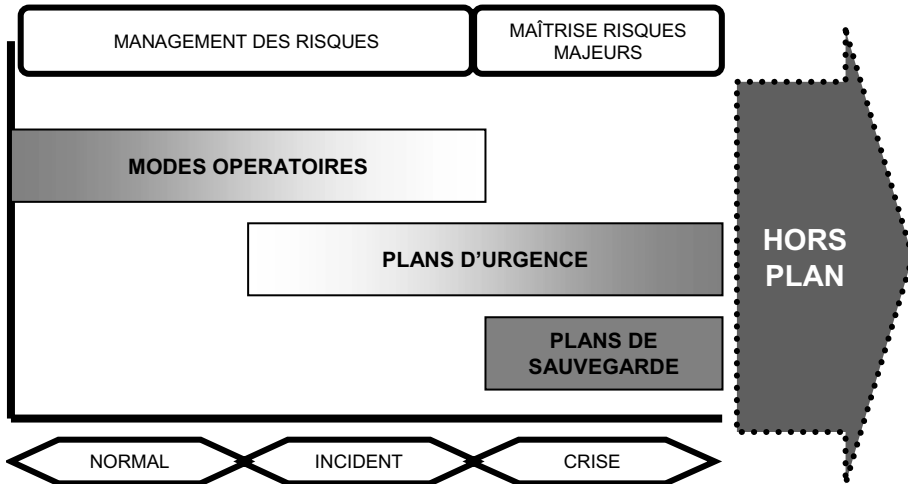


Figure 3.2 La structure documentaire des modes opératoires

Tout ceci est à définir en fonction de la culture et de l'activité de l'entreprise. Quelques constantes cependant : les dispositions qu'ils contiennent doivent être :

- cohérentes entre elles, et en particulier contenir toutes les passerelles fiables nécessaires au passage d'un document à l'autre,
- non redondantes, et *a fortiori* non contradictoires,
- connues et assimilées par les collaborateurs en charge de les appliquer, ce qui suppose :
 - une pression permanente pour faire vivre les modes opératoires courants, trop souvent relégués au placard au bénéfice du savoir-faire, voire des « petits carnets » ;
 - de la formation et des exercices périodiques pour les modes opératoires relatifs aux situations rares.

3.3.5 La redondance

La redondance est une notion essentielle à la maîtrise des risques. Qui n'a pas, la veille d'un examen, placé deux réveils près de son lit ?

En effet, comme le disent les statisticiens, doubler le matériel revient à multiplier entre elles les probabilités d'occurrence de leurs défaillances. Ce qui permet, en général, de ramener la probabilité résultante à une valeur tellement faible que le risque est acceptable.

On définit le niveau de redondance comme suit : la différence entre le nombre de matériels disponibles et le nombre de matériels requis pour assurer une fonction. La plupart du temps, une redondance de niveau 1 est largement suffisante. Mais cela se complique un peu dès qu'on approfondit...

Ne serait-ce que parce qu'un matériel s'entretient, et que pendant ce temps-là il est généralement indisponible... Pour continuer à disposer de la redondance, ce n'est pas 2, mais 3 actionneurs qu'il faudra installer. Sans oublier de les tester : il faut vérifier non seulement l'état des matériels de sauvegarde qui ne fonctionnent pas en temps normal, mais aussi les performances de ceux qui fonctionnent, et qui peuvent se dégrader.

Mais surtout faut-il que les matériels redondants ne risquent aucune défaillance simultanée – on dit de « mode commun ». Cela conduit à des dispositions constructives (ne pas les mettre dans le même local, ne pas les alimenter par la même source d'énergie, etc.) et même de conception (principes de fonctionnement différents, constructeurs différents, etc.). La chasse à la redondance parfaite est un sport de haut niveau et les exemples d'erreurs magistrales de conception sont légion, même dans des installations réputées pour leur sophistication.

Ce qui précède n'aurait pas sa place dans ce paragraphe si on ne finissait par aborder le sujet : la redondance humaine. C'est d'ailleurs la base même de la qualité à ses débuts : mettre un contrôleur partout (y compris pour contrôler le contrôleur et le contrôleur du contrôleur).

On peut facilement transposer. Là où un homme est nécessaire, on en met deux. Quand il est indisponible, quelle qu'en soit la raison, on en met trois. Mais l'indépendance des perceptions et des actions est infiniment plus difficile à assurer qu'avec des réveils, des moteurs ou des pompes ! Et surtout, contrairement à une pompe, un opérateur a horreur qu'on doute de sa capacité à pomper...

La redondance humaine est donc un sport à plus haut niveau encore. Elle passe par un certain nombre de bonnes pratiques :

- afficher la transparence la plus parfaite sur les conditions dans lesquelles elle s'exerce ;

- privilégier « l'auto redondance », c'est-à-dire la capacité de l'homme à se contrôler lui-même ;
- privilégier les contrôles en cours de processus, afin de minimiser les coûts des dysfonctionnements ;
- porter une attention particulière aux interfaces entre les processus et aux interfaces avec les clients (ce qui peut être contradictoire avec ce qui précède) ;
- rechercher l'indépendance des opérateurs par des formations différenciées, des entraînements différents, l'usage de modes opératoires différents, de systèmes d'information indépendants ;
- donner une valeur positive à l'erreur et organiser le retour d'expérience.

Quel que soit le type de redondance, deux petits bémols s'imposent. D'une part, même si la redondance constitue indéniablement une des principales bonnes pratiques pour minimiser les risques de défaillances des processus opérationnels ou des ressources humaines, il faut être vigilant : sans aller jusqu'à dire que « trop de redondance tue la redondance », il faut savoir en apprécier la valeur ajoutée. Mettre en place des dispositifs redondants n'est pas sans conséquence financière et peut faire grimper l'indicateur des Coûts d'Obtention de la Qualité (COQ). Il faut donc éviter une démarche de surqualité qui irait à l'encontre de l'amélioration de la performance de l'entreprise. D'autre part, trop de redondance peut entraîner des effets pervers, comme le relâchement de la vigilance des opérateurs, voire leur démotivation.

Là encore, les exemples d'accidents dus à une redondance inexistante ou insuffisante sont très nombreux. Parmi eux, l'accident de la centrale nucléaire de *Three Mile Island*¹ est certainement l'un des événements qui ont le plus fait progresser la connaissance de ces phénomènes et la façon de les traiter, à la fois sur le plan matériel ou sur le plan humain.

3.3.6 L'approche par états

Approche par cause, approche par conséquences, tout cela est bel et bon... dans le calme feutré d'un bureau, avec sous la main toutes les données nécessaires – ou bien le temps pour les acquérir.

1. *Three Mile Island*, aux États-unis, est connue pour l'accident nucléaire survenu le 28 mars 1979, en raison d'un enchaînement d'événements mêlant défaillances mécaniques, erreurs humaines, défauts de conception... À la suite de cet accident, les exploitants de centrales nucléaires ont mis au point des procédures de conduite accidentelle visant à renforcer la sûreté, notamment « l'approche par état », toujours en vigueur.

Si on se retrouve dans une situation grave et complexe, le stress monte, et rien ne garantit que les analyses qui auront été faites dans la sérénité s'avéreront pertinentes et compréhensibles dans le tumulte du moment – aussi bien faites soient-elles.

On n'explique pas autrement les errements des opérateurs lors d'accidents complexes tels que celui de *Three Mile Island*. Ce n'est donc pas un hasard si c'est dans le nucléaire que s'est développée, à la suite de cet événement (qui, 25 ans après, apporte encore des enseignements !) une autre façon de voir les choses : l'approche par états.

L'idée est simplissime : peu importe ce qui nous a amenés là, peu importe comment et surtout pourquoi – d'autant que ce « pourquoi » serait traumatisant et qu'il est donc inutile de le laisser contribuer à augmenter le stress ambiant. Ce qui est important, c'est de faire un bilan rapide, simple, sans impasse, de la situation, et d'en déduire quels modes opératoires mettre en œuvre pour revenir à une situation moins dégradée.

Ceci passe aussi, bien entendu, et longtemps avant, par la sérénité d'un bureau : au niveau de la conception des matériels, il aura fallu mettre en place – voire inventer – puis valider les matériels et les modes opératoires nécessaires pour que ce bilan soit possible et que l'action soit sûre.

3.3.7 Le rôle du management

Un chef est un homme comme les autres mais, c'est bien connu, il reste chef même dans sa salle de bains...

Pour parler plus sérieusement, le rôle du management vu de l'interface homme-machine est à la fois secondaire et primordial. Il n'est pas différent de ce qui pourrait être écrit à propos de n'importe quelle démarche de progrès.

Avant l'événement, il peut se résumer en trois axes :

- promouvoir, par ses actes, son attitude, une « culture risques » dans l'entreprise ;
- donner les moyens nécessaires à ceux qui ont en charge le déploiement des démarches correspondantes ;
- piloter le bouclage de ces démarches, et par là valider ses propres actions.

Ceci est à raccorder à la schématisation décrite plus loin au paragraphe 4.3.

Pendant l'événement :

- assurer sa fonction, ce qui signifie essentiellement être présent dans l'organisation et à l'extérieur, en particulier devant les médias s'il y a lieu ;
- n'assurer **que** sa fonction, c'est-à-dire f... la paix à ceux qui sont en charge de l'action, que l'on a choisis, formés, et à qui on a délégué les pouvoirs nécessaires.

Un exemple simple : dans un magasin la veille de Noël, quand les vendeurs sont débordés et que la panique guette, le rôle de patron est :

- d'être au contact des clients mécontents ;
- éventuellement d'aider ses caissières à faire des paquets.

Surtout pas de donner des ordres à la place des chefs de rayon, ni de tenter une réorganisation à chaud !

Après l'événement :

- piloter le retour d'expérience et garantir la mise en œuvre des actions correctives ;
- reconstituer les conditions nécessaires au retour à la normale, y compris en donnant les moyens nécessaires ;
- panser les plaies, rassurer ceux qui ont fait des erreurs, remercier ceux qui ont beaucoup donné, et même – ce qui ne tombe pas sous le sens – compenser les frustrations de ceux qui n'ont pas eu l'occasion d'être impliqués dans l'action.

3.4 Stabilité et instabilité

La notion de stabilité/instabilité est complètement sous jacente à l'étude des risques majeurs. On parle aussi parfois de « spirale descendante », ce qui revient à peu près au même.

Un objet, un organisme, sont stables si une perturbation qui les affecte est suivie de leur part d'une réaction ou d'un repositionnement vers l'état normal. Ils deviennent instables, en général à la suite d'une ou plusieurs « premières » perturbations, quand au contraire ils s'éloignent de cet état normal.

C'est le cas du bateau qui « prend » une première vague, ce qui provoque de la gîte qui va favoriser sa submersion par les suivantes. Sur le plan humain, c'est le cas de l'opérateur qui « pète les plombs » alors qu'il est déjà sous stress,

quand survient une nouvelle perturbation, sous la forme d'un nouvel événement, de l'intervention malencontreuse d'un tiers, etc.

On peut parfois, et heureusement, contrarier une instabilité, en général par une action rapide et qui ne tombe pas forcément sous le sens – un contre pied en quelque sorte. Il existe quelques exemples fameux dans le domaine médiatique, comme celui du président d'un grand pays, en fort mauvaise posture suite à des accusations de corruption, et qui a retourné l'opinion en direct à la télévision en « avouant » qu'il avait gardé par-devers lui, une fois, un petit chien.

Malheureusement, le plus souvent, une telle réaction est impossible ; la seule issue est alors d'attendre d'avoir touché le fond pour redonner le coup de pied salvateur – quand le fond est ferme et qu'il reste assez de force.

C'est une solution, et c'est évidemment la pire : la meilleure est de faire ce qu'il faut pour résister aux perturbations, c'est-à-dire... à maîtriser les risques.

3.5 Notion de crise

Tout le monde sait ce qu'est une crise... surtout quand on le dit. Quand est-ce qu'une crise commence ? Quand finit-elle ? Qui « décide » qu'on est en crise ? Tout cela est flou, et ne s'éclaircit, la plupart du temps, qu'après le passage des historiens.

Savoir cela est pourtant strictement indispensable, car si on ne sait pas ce qu'est une crise, on sait quelles en sont les conséquences : l'organisation (les processus) ne fonctionne plus. Ce n'est pas un hasard si ce paragraphe suit celui traitant de stabilité : on est en crise quand la stabilité de l'entreprise est compromise. Une définition pour en cacher une autre, certes, mais elle illustre une idée importante : en crise, le naufrage est possible, voire certain, si une nouvelle perturbation se superpose à celle qui a provoqué la crise.

Les définitions de la crise qu'on trouve dans la littérature sont la plupart du temps influencées par le point de vue de l'auteur – nous ne prétendons pas échapper à cette règle. Citons Patrick Lagadec (*cf.* bibliographie en fin d'ouvrage) :

« Crise : une situation où de multiples organisations, aux prises avec des problèmes critiques, soumises à de fortes pressions externes, d'âpres tensions internes, se trouvent brutalement et pour une longue durée sur le devant de la scène, projetées aussi les unes contre les autres... le tout dans une société de communication de masse, c'est-à-dire en direct, avec l'assurance de faire la « une » des médias sur une longue période ».

Si nous avons cité cette définition, c'est parce qu'elle émane d'un expert qui fait référence, et aussi parce qu'elle correspond globalement à l'idée qu'en a le public. Nous n'avons pas la prétention d'en formuler une critique, mais le lecteur aura senti que cette définition de la crise fait la part un peu trop belle à l'aspect médiatique. Elle suppose aussi une constance des médias dans leurs sujets de préoccupation qui ne saute pas aux yeux : c'est le moins qu'on puisse dire, et ceux qui « gèrent » les crises le savent bien et savent donc aussi « jouer » avec.

Pour illustrer un peu plus notre propos, nous proposons une liste des crises possibles, avec les réserves d'usage sur ce genre de compilation :

- agression criminelle (sabotage, terrorisme, espionnage, attaque sur les personnes...) ;
- agression économique (boycott, OPA...) ;
- dissémination malveillante d'informations et de produits (contrefaçon, rumeurs...) ;
- accident industriel (pollution, accident de transport...) ;
- catastrophe naturelle (incendie, inondation, tremblement de terre...) ;
- défaillance des sites de production (panne générale, défauts produits majeurs, destruction du site, déménagement...) ;
- crise juridique (mise en examen d'un homme clé, fraude, procès médiatisé...) ;
- crise sociale (grèves, plans sociaux, violence sur le lieu de travail, occupation de locaux...) ;
- crise humaine (accident grave, décès, fuite de dirigeant...) ;
- crise réglementaire (nouvelle loi ou réglementation...) ;
- crise concurrentielle (rupture technologique, survenance d'un nouveau concurrent puissant...).

Ceci dit, les crises se suivent, ne se ressemblent pas, mais présentent des analogies dans la façon de les traiter. Les points communs sont évoqués dans les paragraphes relatifs au management de crise. En complément, chaque paragraphe intitulé « méthodes et bonnes pratiques pour revenir au fonctionnement normal » du chapitre 6 devrait répondre aux attentes du lecteur quant au « comment » réagir selon le type de crise.

Une autre notion doit intervenir ici : celle de la « crise réplique » (ou « crise rebond »). À l'image d'un tremblement de terre, on doit toujours s'attendre à une deuxième crise, conséquence plus ou moins directe de la première. Comme des répliques de séisme, le problème est qu'on ne sait pas ni où ni quand l'événement va avoir lieu. Deux exemples très connus : quand l'Erika a fait naufrage, il n'était pas évident que les retombées seraient plus pour Total que pour l'armateur ! Et lors de l'accident de Tchernobyl, personne ne se serait douté qu'une crise franco-française toucherait ultérieurement ceux dont on a prétendu (à tort) qu'ils affirmaient avoir arrêté le nuage à nos frontières...

4

Fonctionnement d'une entreprise

4.1 Modélisation d'une entreprise

4.1.1 Pourquoi des modèles ?

Cet ouvrage a pour ambition de permettre à ses lecteurs de traiter l'ensemble des risques d'une entreprise. Il est donc nécessaire de mettre à leur disposition un ensemble d'outils, méthodes et concepts, permettant de garantir que la démarche n'oubliera pas de point important... sans hélas espérer prétendre à l'exhaustivité.

Pour ce faire, on adoptera (et ceci est un parti pris des rédacteurs) un modèle qui a fait ses preuves et ne connaît guère de concurrents : le modèle EFQM et ses méthodes associées.

En amont, il faut également proposer une façon de représenter une organisation permettant au lecteur de situer une démarche management des risques dans le contexte le plus général de la stratégie de l'entreprise.

4.1.2 Le modèle d'organisation de l'entreprise

Une entreprise est souvent représentée par des « couches » formant une pyramide, mais nous préférons le schéma suivant (Figure 4.1).

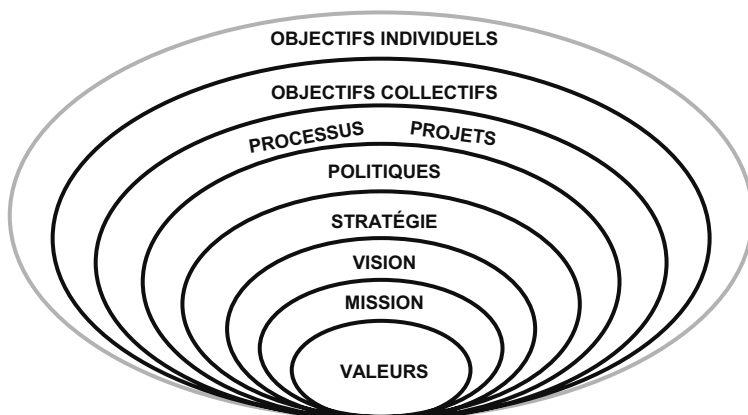


Figure 4.1 Modélisation d'une entreprise

Une entreprise repose sur un « empilement » de concepts qui se complètent et interfèrent :

- Les valeurs : quasi intangibles, elles sont le ciment intime qui fédère tous les collaborateurs, à tous les niveaux. Elles sont choisies, clarifiées par le plus haut dirigeant, et ne souffrent guère de débat car elles sont positives et valorisantes.
- La mission : quasi pérenne également, sauf changement très fort dû, en général, à un bouleversement du contexte.
- La vision : en général émise sur le moyen terme (3 à 5 ans), elle est imaginée par le plus haut dirigeant et décrit en termes simples et généralement ambitieux ce que sera l'entreprise au bout de ce laps de temps.
- La stratégie : c'est l'ensemble des choix que fait la Direction (cette fois de manière collective) et qui vont permettre d'atteindre la vision, quels que soient les aléas qui pourront survenir sur le chemin.
- Les politiques : en application de la stratégie, elles rassemblent dans une poignée de domaines (RH, qualité, achats, etc.) les choix, cohérents avec la stratégie, qui permettront à l'ensemble des managers de prendre leurs décisions en toute connaissance de cause.

- Les processus et les projets : ces politiques s'appliqueront à ce qui constitue l'essence même de l'activité (de toutes les activités de l'entreprise) : les processus et les projets. Nous avons pris le parti de séparer les deux concepts, parce qu'un projet, par définition, n'est pas répétable, au contraire d'un processus. Les outils et méthodes permettant d'en garantir la performance ne sont donc pas les mêmes.
- Les objectifs : les projets et les processus sont instrumentés par des indicateurs, qui sont raccordés à des objectifs – toujours liés à ce qui précède naturellement. Les objectifs collectifs sont déclinés en objectifs individuels.

Tout ceci se déploie : l'ensemble des collaborateurs de l'entreprise a à connaître et à comprendre la vision, la stratégie, les politiques, et naturellement les objectifs. Entre le maçon qui déclare « Je construis une cathédrale » et celui qui dit « Je transporte une pierre », il y a toute la différence entre une entreprise où le déploiement est effectif, et une entreprise où il ne l'est pas.

Cela se déploie également vers les autres parties prenantes de l'entreprise – à une légère réserve près pour la stratégie, dans certains cas.

4.1.3 Mesure et management de la performance

Il n'est pas dans notre intention ici de donner une idée complète de la façon de manager la performance de l'entreprise. C'est un problème largement non résolu, malgré l'existence de nombreux ouvrages sur le sujet, ainsi que de nombreuses études, méthodes et outils. Mais nous insisterons sur la nécessité de la mesurer, car il n'y a pas de progrès sans mesure. Même si cela revient à enfoncer des portes que l'on croit largement ouvertes, nous insisterons juste sur l'idée qu'on ne pilote pas une petite entreprise avec la trésorerie, et une grande avec le cours de l'action. Est-ce si évident pour tout le monde ?

La plupart du temps, on attend une certaine croissance de la performance. De plus en plus souvent, c'est même une question de survie. Mais il y a croissance et croissance. Pour schématiser – et introduire du même coup quelques termes de vocabulaire utilisés par la suite – nous distinguerons trois types de croissance :

- Le progrès naturel. Il repose sur la bonne volonté et la compétence des membres de l'entreprise, dirigeants et non-dirigeants. Ce type de croissance n'est pas garanti, et ne saurait entraîner des taux de croissance supérieurs à quelques pour-cent par an... dans les cas les plus défavorables, ce taux de croissance peut être négatif, présage de la disparition de l'entreprise à terme. En revanche, ce type de management de la croissance ne coûte quasiment rien.

- L'amélioration continue. Elle le résultat d'actions volontaristes, appelées globalement « démarches de progrès ». Là aussi les méthodes et outils abondent, mais il est des cas où le savoir-faire intuitif des dirigeants suffit à initier de tels mouvements. Les résultats sont garantis à la condition expresse que les démarches soient menées à leur terme, et s'enchaînent les unes avec les autres au fil de temps : comme tout produit vivant, une démarche a un cycle de vie qui se termine par son obsolescence et sa disparition. Tout l'art du dirigeant est de sentir ce qu'il doit faire, et quand il doit le faire. On peut attendre de telles actions de gains de quelques pour-cent par an. L'investissement est également de quelques pour-cent des forces vives, ce sont donc des opérations rentables dès les premières années. En dessous 1 %, on gaspille ses forces et son argent car les résultats ne sont pas au rendez-vous.
- La rupture. Elle est souvent le fruit de la nécessité, en particulier de modifications brutales de l'environnement. Personne n'aime les changements rapides (sauf les bébés mouillés, dit-on). Il s'agit donc d'opérations violentes, qui ne peuvent se justifier que si on en attend des sauts de performance à deux chiffres. L'investissement à prévoir peut également atteindre les deux chiffres. Comme il important, il a pour conséquence une dégradation temporaire de la performance qu'il faut savoir anticiper et supporter à un moment délicat. Comme précédemment, une démarche de rupture a un cycle de vie, plus court que celui d'une démarche de progrès il faut donc aussi accompagner sa fin de vie en lançant au bon moment une démarche plus douce.

4.1.4 Le modèle de la gestion de la performance : le modèle d'Excellence de l'EFQM

Le modèle EFQM (*European Foundation for Quality Management*) est un outil permettant de représenter l'entreprise de façon complète, selon 9 « éclairages » appelés « critères » (Figure 4.2).

Les critères situés à gauche concernent les moyens que l'entreprise déploie pour assurer sa performance actuelle, mais aussi pour garantir son développement futur. Les critères situés à droite permettent d'évaluer la performance de l'entreprise vis-à-vis de l'ensemble de ses partenaires, appelés « parties prenantes ».

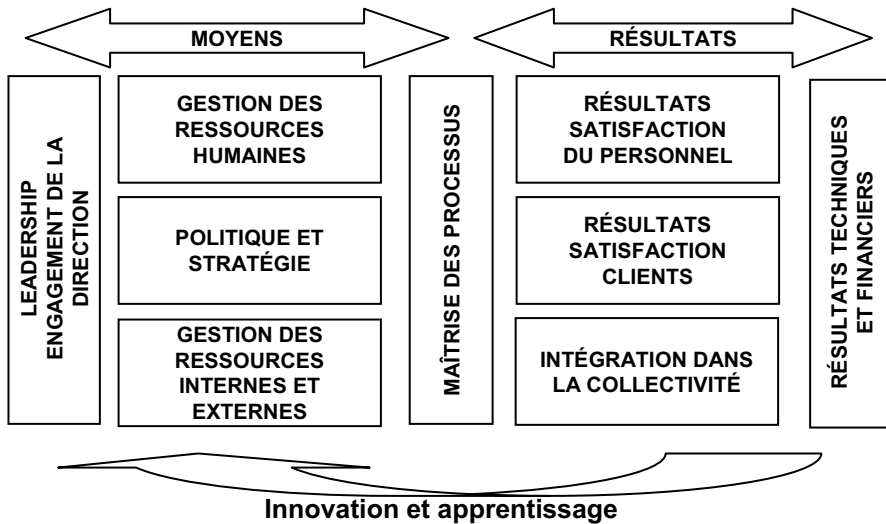


Figure 4.2 Le modèle d'Excellence de l'EFQM

La boucle de retour « innovation et apprentissage » met en lumière la nécessité de cohérence entre les résultats et les moyens, ainsi que le rôle fondamental de l'amélioration continue des processus et des connaissances.

On verra plus loin que le management des risques porte en interne sur les objets englobés par les critères « moyens », alors que le management des risques vis-à-vis de l'externe s'ordonne très facilement selon les critères « résultats ».

En amont de cet outil, l'EFQM a émis ses « Concepts fondamentaux pour l'Excellence », qui donnent du sens au modèle. En aval, le modèle EFQM a permis la mise au point de méthodes d'évaluation et d'autoévaluation. On se reportera pour cela utilement aux ouvrages publiés en France par l'AFNOR, représentant national de l'EFQM, qui font la part belle, quoique pas toujours de façon très évidente, à la façon dont l'entreprise manage ses risques.

4.2 Les trois domaines de fonctionnement (plus un)

On ne peut pas considérer une entreprise comme un organisme qui avancerait par saccades : la vie n'est pas immobile, elle n'est même pas une succession de photos, elle est plutôt un film, un *continuum* d'évènements et de réactions. Comme tout être vivant, elle évolue sans cesse dans un espace à multiples dimensions.

Mais il faut bien simplifier... Nous proposons donc de représenter l'entreprise comme un objet qui se situe à tout moment dans l'un des trois domaines de fonctionnement (Figure 4.3).

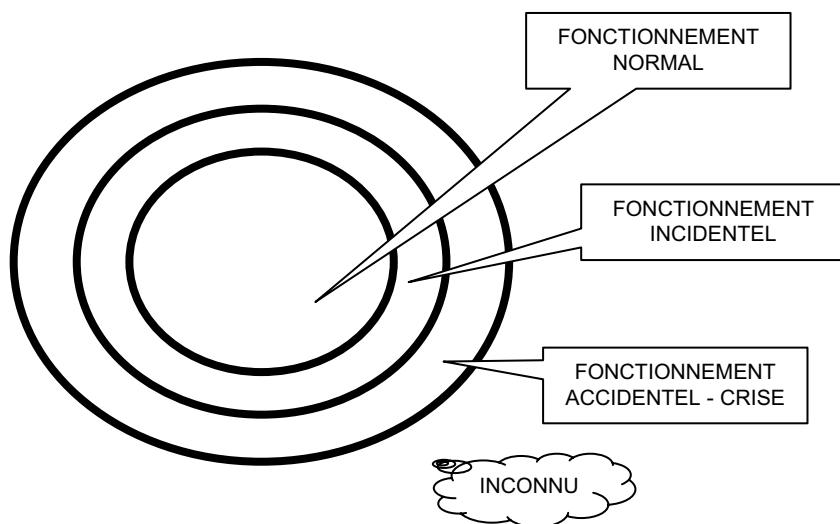


Figure 4.3 Les domaines de fonctionnement

4.2.1 Domaine de fonctionnement normal

C'est celui où « tout baigne »... Les indicateurs sont au vert, l'environnement ne donne aucun signe inquiétant. Le pilotage de l'entreprise est du domaine de la veille. À l'image d'une voiture sur une route déserte et droite, on est dans le pilotage inconscient, et les signaux faibles, en particulier en provenance des dangers ou des cibles, sont mal perçus. La vigilance est donc à organiser. Sans négliger l'anticipation.

Le rôle du management est de tout mettre en œuvre pour ne pas sortir de ce domaine.

4.2.2 Domaine incidentel

L'entreprise est en alerte plus ou moins active ; les indicateurs clignotent, ou passent à l'orange – voire au rouge. Pour reprendre l'image de la conduite automobile, c'est le moment où « il se passe quelque chose » (voyant d'alerte,

franchissement de ligne, bruit...). Les risques sont concrets, le pilotage devient actif, l'anticipation n'est déjà plus possible. C'est le moment de la mobilisation.

Le rôle du management est de tout faire pour revenir au domaine normal... et surtout ne pas aller vers le domaine de crise.

4.2.3 Domaine accidentel

« Rien ne va plus. » Les indicateurs rouges sont tellement nombreux à clignoter que leur exploitation est impossible. Toujours dans l'exemple de l'automobile, c'est la panne bloquante, l'accident... Les risques sont devenus des dangers graves et imminents, mais la confusion et le stress peuvent empêcher de les appréhender correctement. Le pilotage devient réactif : il s'agit de revenir le plus vite possible dans un domaine plus calme. On ne pilote plus avec les processus normaux, les fonctions et les responsabilités ne sont plus les mêmes, au moins temporairement et partiellement.

Le management est tout entier orienté vers la sortie de la crise, et il doit s'organiser autrement pour y réussir. La plupart du temps, il ne peut pas y arriver avec les seuls moyens habituellement à sa disposition. Il doit faire appel à des moyens externes. Parfois même, ces moyens s'imposent d'eux-mêmes.

4.2.4 Et ailleurs...

On aura remarqué que, comme les Trois Mousquetaires, les 3 domaines annoncés sont au nombre de 4. Le dernier est le celui de l'inconnu, aussi bien dans la perception des dangers que dans la lutte pour les éliminer. La sortie du domaine de crise vers l'extérieur du schéma correspond à la (vaste...) zone où l'existence de l'entreprise n'est plus de la compétence naturelle de son management. Ou au moins plus seulement, mais les auteurs ne souhaitent pas entrer dans un débat sur la réalité des miracles...

Il existe cependant des concepts et des méthodes pour traiter ce domaine... à condition qu'on en ait la volonté – ou l'obligation.

4.3 Le management

Le schéma utilisé plus haut (Figure 4.1) permet, en outre, de visualiser de façon simple deux notions importantes pour la suite (Figure 4.4).

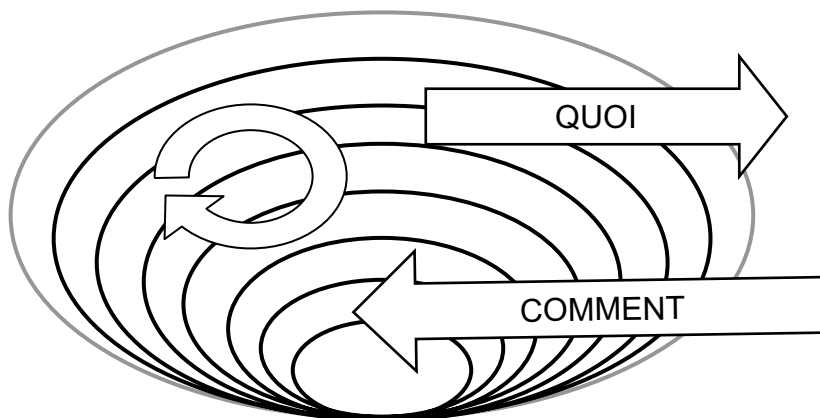


Figure 4.4 Modélisation du management

4.3.1 À quoi sert un manager

Son rôle est (tout simplement ?) d'assurer des bouclages entre les différentes « couches » du schéma ; les hauts dirigeants sont plutôt en charge des bouclages entre la vision, les politiques, etc., tandis que les managers de terrain sont plutôt responsables des bouclages entre objectifs collectifs et individuels. Que d'erreurs majeures de management seraient évitées si chacun avait conscience des « boucles » dont il est responsable, et surtout, surtout, ne s'occupait que de celles-ci...

4.3.2 Qu'est-ce que le management participatif ?

Tout le monde croit savoir ce que c'est, et demeure, bien entendu, convaincu qu'il le met en pratique... L'image que nous proposons traduit simplement le fait que « faire du management participatif », c'est garantir que le QUOI « descend » des valeurs vers les objectifs, et que le « COMMENT » remonte dans l'autre sens. Que d'erreurs seraient aussi évitées, si les managers savaient s'abstenir de saturer leurs collaborateurs avec des « comment » dont ceux-ci n'ont pas besoin... et qu'ils rejettent d'autant plus facilement qu'ils ne sont pas pertinents.

4.3.3 Management et crise

- **Un management particulier**

En cas de crise, telle que nous en avons tenté une définition au chapitre 3.5, le management a non seulement un rôle (encore plus) primordial, mais différent. On ne peut plus du tout parler de management participatif ! Bien que le bon fonctionnement de la chaîne hiérarchique dépende toujours de la confiance que les collaborateurs ont en leurs chefs, et que cette confiance peut découler de leur aptitude à pratiquer, en temps normal, un tel type de management.

Le rôle du management, et en particulier les plus hauts dirigeants, consiste à affronter la tempête depuis la dunette du navire, et pas ailleurs. On distingue trois phases :

- avant : la préparation de l'entreprise à la crise ;
- pendant : la détection de la crise et la prise des mesures appropriées ;
- après : la gestion de l'après crise, et l'évitement de la « crise réplique ».

Dans les paragraphes qui suivent nous n'aborderons que les aspects communs : on retrouvera les autres dans le chapitre sur les familles de risques.

- **Avant la crise**

Gouverner, c'est prévoir ! Plus facile à dire qu'à faire. Il n'empêche qu'il est du rôle du management d'écouter les signes annonciateurs, et de faire passer l'information là où elle doit aller. Question de feeling et/ou d'organisation.

En tout cas il est toujours possible de préparer l'entreprise sous un aspect : faire comprendre aux collaborateurs que l'impossible peut se produire, et que les accidents ne sont pas toujours pour les autres. Dans les grandes entreprises, l'élaboration (participative !) d'un plan « risques majeurs » est toujours opportune. Il est d'ailleurs obligatoire dans certains cas (classement dit « Seveso »).

Un plan risques majeurs ayant, par définition, une probabilité très faible d'être mis en œuvre, des exercices de simulation périodiques sont absolument nécessaires pour le valider, et pour maintenir le niveau de connaissance des collaborateurs. Plus ces exercices seront réalistes, mieux cela vaudra. C'est prendre un risque (raisonné) que de simuler un incendie avec des fumigènes dans une installation industrielle, ou encore de tester un plan d'évacuation par temps de verglas, mais c'est indispensable.

Dans les plus petites, on peut au moins en parler : c'est peut-être éviter un drame très grave que de dire à un livreur de pizza qu'en cas de contestation d'un client violent, il doit immédiatement faire cadeau de son colis, et remonter sur son cyclomoteur !

• **Pendant la crise**

La première et principale décision à prendre est de passer en organisation de crise. Cela ne s'improvise pas et l'aide à cette décision est décrite dans les différents paragraphes du chapitre 6.

Une organisation de crise, quelle qu'elle soit, se fait sur le mode suivant : on constitue quatre postes de commandement, qui reçoivent le pouvoir de piloter l'entreprise dans le cadre des procédures prévues... s'il y en a ; sinon ils sont en charge d'un pilotage de type « cabotage » en zone dense en récifs :

- Le poste « direction » : c'est lui qui décide des phases, prend les décisions majeures et assure l'interface avec l'extérieur. Il est tenu par le plus haut dirigeant ou un de ses très proches collaborateurs, de préférence un opérationnel à un expert.
- Le poste « opérations » : c'est lui qui gère la crise sur le plan pratique, qui décide de la mise en œuvre des moyens et de la conduite des processus, s'il en reste d'opérationnels.
- Le poste « contrôle », dont la tâche est de collecter, en interne et en externe, toutes les mesures et informations permettant aux deux postes précédents de prendre les meilleures décisions possibles.
- Le poste « moyens », qui est chargé d'apporter les moyens en hommes, matériels, méthodes, appuis logistiques ou techniques, nécessaires aux trois précédents.

Les trois derniers postes doivent être tenus par des personnes compétentes. Comme il est nécessaire que cette compétence soit disponible en permanence, cela peut demander des formations *ad hoc* bien plus complètes que ce que les exercices périodiques peuvent apporter – et que chacun a d'ailleurs finalement peu de chance de vivre.

Bien entendu, les moyens nécessaires doivent être prévus et essayés périodiquement s'ils ne sont qu'à cet usage : moyens de communication, moyens de mesure, locaux adaptés, et modes opératoires dûment validés par les exercices. Par exemple, un opérateur téléphonique devra munir ses cadres d'astreinte d'abonnements... d'un concurrent !

Il y a quatre postes, au moins quatre et rien que quatre : l'organisation normale de l'entreprise s'efface devant ces nouveaux pouvoirs, le temps que dure la crise. Bien entendu, la crise peut ne pas être générale, et le domaine d'action des quatre postes limité à tout ou partie de l'entreprise, des processus, etc. et ceci dans la plus grande clarté.

• **Après la crise**

Un risque majeur : l'oubli. Or, bien entendu, c'est tout le contraire qu'il faut faire.

Nous mentionnerons sans insister plus que nécessaire, tant c'est évident, sur la nécessité du retour d'expérience, et donc sur le rôle de la Direction pour l'animer, en tirer les plans d'action et en vérifier le déploiement.

Mais d'autres aspects méritent l'attention :

- Porter un soin particulier aux traumatismes de ceux qui ont vécu la crise, et en tout premier lieu, si c'est le cas, ceux que l'opinion considère comme des « coupables ».
- Ne pas oublier, même si c'est moins important, ceux qui ont été écartés de la crise ; cela génère parfois un sentiment de frustration, celui de ne pas « en avoir été ».
- Vis-à-vis de l'extérieur, communiquer sur les mesures prises pour ne pas connaître à nouveau une telle situation ; action difficile s'il en est, en particulier avec les médias de bas niveau : seuls les trains qui déraillent les intéressent.
- Vis-à-vis des clients, opérer une communication adaptée, témoignant du souci permanent que l'entreprise a eu d'eux en ces temps difficiles.
- Vis-à-vis des autres parties prenantes (collectivité, actionnaires), une attitude analogue doit être envisagée au cas par cas, et strictement adaptée aux inquiétudes spécifiques de telle ou telle partie.
- Vis-à-vis des concurrents aussi ! Certes on ne peut pas tout dire, et à tout le monde. Mais les entreprises œuvrant dans des domaines analogues, employant souvent les mêmes méthodes et les mêmes matériels, seront reconnaissantes d'un tel geste... À charge de revanche. C'est également un exercice délicat, qui ne peut être conçu qu'avec une logique gagnant-gagnant : mais les gains escomptés peuvent s'avérer colossaux. Le truchement d'organismes fédérateurs (chambre de commerce, syndicats professionnels...) peut être une voie moins aléatoire.

4.4 Qualité et risques

Selon les auteurs et ce que les consultants ont à vendre, selon la culture et l'organisation de l'entreprise, « tout est dans les risques » ou « tout est dans la qualité » (ou tout est dans les RH, le financier, la communication, etc.).

Rien de plus radical pour troubler les esprits, et rendre, parfois de façon durable, telle ou telle démarche de progrès vaine et donc inefficace, parfois pour de nombreuses années.

4.4.1 La qualité, c'est les risques

Il est de bon sens de dire que la qualité – ou plutôt l'assurance qualité – traite de la maîtrise des risques clients. Comme QSE (Qualité, Sécurité, Environnement) traite, en plus, des risques environnementaux et humains, et comme le TQM (Management par la qualité totale) traite de l'ensemble des parties prenantes. On peut même avancer, on le verra plus loin, que le développement durable traite des risques que nous faisons courir aux générations futures.

4.4.2 Les risques, c'est de la qualité

Si on parle de maîtrise – voire de management – des risques, on parle d'une démarche de progrès. Il est inconcevable que cette démarche ne soit pas conduite comme une démarche qualité. Le cycle vertueux de la maîtrise des risques n'est autre que la « roue de Deming », soit l'amélioration continue comme expliquée au paragraphe 5.2.2, appliquée aux risques.

Plus globalement, l'art de gérer les risques, de transformer les dangers (menaces dans le vocabulaire *ad hoc*) en opportunité n'est rien d'autre que la qualité mise au service de la stratégie de l'entreprise.

4.4.3 La qualité et les risques, même combat

Outre la communauté de méthodes et d'outils évoqués rapidement plus haut, le management de la qualité et le management des risques ont évidemment tout intérêt à être pilotés de façon homogène. Les discours doivent être cohérents. Ce n'est pas une mauvaise chose que les acteurs soient les mêmes. En tout cas, les managers doivent s'appropriier le tout de façon similaire, synergique. Jusque et avant tout dans leur propre comportement au quotidien.

Partie II

Les risques : comment les maîtriser

5

Management des risques

5.1 Management, maîtrise, gestion des risques

Comme nous n'avons pas l'intention de rentrer dans des débats sémantiques, nous afficherons dès le départ, avec un parti pris que nous ne nierons pas, notre position vis-à-vis de ces trois termes :

- Gestion : mot employé à tort et à travers, et donc vide de sens... Pas particulièrement harmonieux, il véhicule une image plutôt passive et donc à éviter : il n'y a pas loin de la gestion à la digestion, laissons donc tout cela aux gestionnaires.
- Maîtrise : terme positif, parfois presque trop ; nous l'emploierons pour qualifier les actes qui visent à identifier les risques, à les caractériser et à en minimiser les effets et les conséquences. Maîtriser, c'est agir. La maîtrise des risques est l'affaire, avant tout, des acteurs directs qui y sont impliqués. Dans le jargon de la qualité, la maîtrise s'appuie sur des processus opérationnels.
- Management : terme plus large, que nous emploierons pour désigner les actions de management qui ont trait à la maîtrise des risques. Le management des risques, c'est avant tout l'affaire des managers. Toujours dans le vocabulaire de la qualité, le management des risques s'appuie sur des processus de pilotage (ou de management).

On pourra en déduire, sans trop d'abus, que la maîtrise des risques est incluse dans le management des risques. À noter qu'en français nous avons la chance de disposer de ces deux termes : les anglophones n'ont que « management », ce qui nous a permis de lire récemment dans une revue spécialisée un texte dont la traduction mot à mot serait : « le management des risques comporte, entre autres [...]... le management des risques »...

5.2 Maîtrise des risques : notions élémentaires

5.2.1 Probabilité, gravité, criticité

On a vu au chapitre 2 que l'outil élémentaire de la maîtrise des risques est le diagramme dit « de Farmer », dont la forme la plus simple est celle qui a été donnée au paragraphe 2.3.

Il s'agit là d'une représentation purement qualitative. En réalité, on définit la criticité comme le produit de la probabilité par la gravité des effets du risque envisagé. Autrement dit, sous une forme plus mathématique :

$$Cr = P \times G$$

Mais une entreprise, comme tout organisme vivant, sait parfois réagir contre les agressions qui la touchent. On l'illustre par une formule plus complète, comme par exemple celle-ci :

$$Cr = f(Pa, Pd, Pnc, Ge, Pcd)$$

où les paramètres sont les suivants :

- Pa : probabilité d'apparition du risque ;
- Pd : probabilité de non-détection ;
- Pnc : probabilité de non-correction entre détection et effet ;
- Ge : évaluation de la gravité de l'effet ;
- Pce : probabilité de non-compensation de l'effet produit.

5.2.2 Processus élémentaires

Ils découlent d'une autre figure imposée : la boucle vertueuse de l'amélioration continue (ou « roue de Deming ») appliquée à la maîtrise des risques (Figure 5.1).

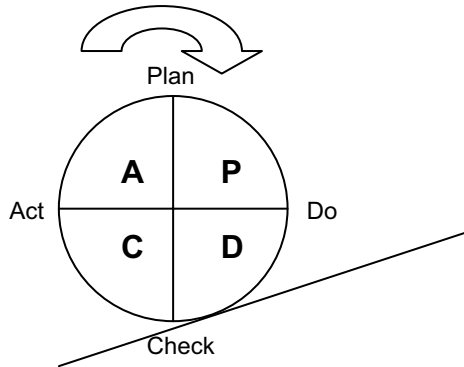


Figure 5.1 La roue de Deming ou la boucle vertueuse de l'amélioration continue

Rappelons les définitions des termes :

- P (*plan*) : planifier, préparer, prévoir ;
- D (*do*) : faire, réaliser, déployer ;
- C (*check*) : mesurer, évaluer, contrôler ;
- A (*act*) : consolider, prendre acte, valider.

Ajoutons quelques commentaires, apparemment frappés du sceau du bon sens, mais qu'il est peut-être utile de (se) rappeler de temps en temps :

- Le A ne veut pas dire « agir » (agir, c'est DO), mais plutôt « acter » : Deming insistait bien sur l'importance de faire le point, et sur le fait que « consolider » n'est pas inéluctable : il n'est pas interdit, bien au contraire, d'abandonner pour faire autrement.
- La flèche montre le sens de rotation de la roue, et une remarque sur l'ordre d'apparition des lettres n'aura d'autre intérêt que celui de vérifier l'attention de l'auditoire. Mais elle signifie aussi, et surtout, que la roue ne tourne pas toute seule : pour qu'elle gravis la pente vertueuse de l'amélioration continue, il faudra d'une façon ou d'une autre lui transférer de l'énergie !

Transposée dans le processus de maîtrise des risques, la boucle de l'amélioration continue prend une allure un peu plus complexe (Figure 5.2).

Ce diagramme met en évidence non pas une seule boucle, mais deux : la « petite », dont le rôle est de garantir l'efficacité de l'action de maîtrise du risque considéré, et la « grande » qui doit garantir que le risque maîtrisé (et qui est donc devenu un « risque résiduel ») ne change pas de nature avec le temps.

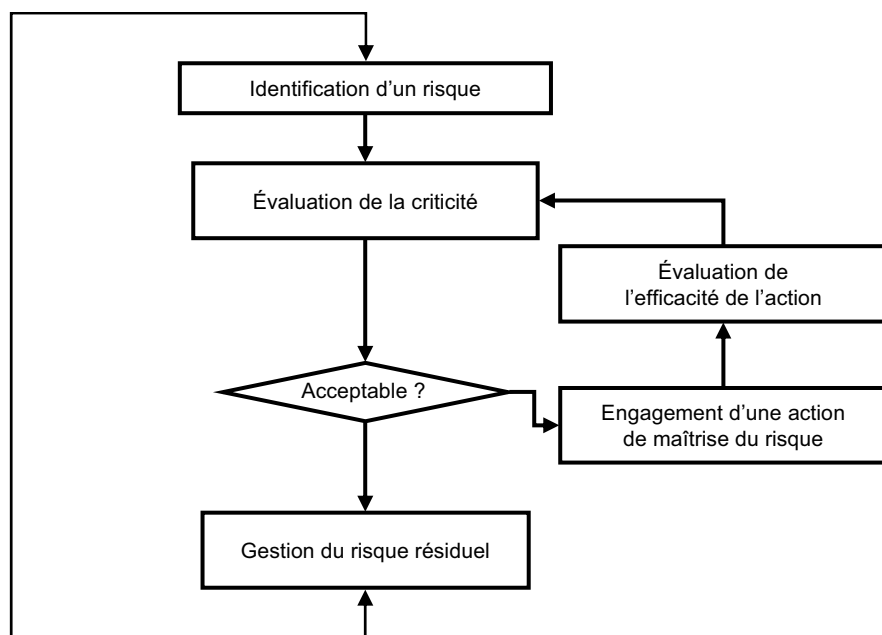


Figure 5.2 La boucle de l'amélioration continue appliquée au processus de maîtrise des risques

Nous allons revenir dans les paragraphes suivants, plus en détail, sur chacune des cases de ce diagramme.

5.3 Maîtrise des risques : identification

Inutile de faire assaut de banalités en proclamant qu'il s'agit d'une phase essentielle ! Ni d'ajouter qu'il faut maîtriser tous les risques pour être tranquille, mais que c'est impossible. Ni souhaitable d'ailleurs.

Il existe trois grandes familles de méthodes pour identifier les risques :

- les méthodes intuitives et empiriques ;
- les méthodes déductives qui partent d'un inventaire des effets (méthodes ascendantes) ;
- les méthodes déductives qui partent des causes (méthodes descendantes).

5.3.1 Les méthodes intuitives et empiriques

Les plus pratiquées sont à base de *brainstorming* (en français : « remue-ménages »). On réunit un groupe de réflexion, dont la composition n'est évidemment pas anodine, et on lui fait « cracher » tous les risques qui viennent à l'idée. Plus l'expression est libre et plus on a de chances de ratisser large. Plus on a aussi la chance de se retrouver devant un tas d'items parmi lesquels il va falloir retrouver ses petits.

Un tri est donc en général indispensable, qui peut être conduit à l'aide d'outils classiques, comme par exemple le diagramme des affinités.

Parmi les méthodes empiriques nous classerons aussi celles qui consistent à se référer à un ou plusieurs ouvrages et à en extraire les risques qui semblent convenir à la situation de l'entreprise. L'empirisme est alors à double niveau : dans le choix de l'ouvrage et dans la façon dont l'auteur a pu, lui-même, constituer ses listes. Celui qui est entre vos mains en ce moment n'échappe pas à cette règle.

Nous citerons enfin les outils tels que les matrices de découverte, qui sont un pas vers un peu plus de rigueur. Le choix des lignes et de colonnes est primordial pour la qualité des résultats. Même si la matrice est insuffisante, elle peut permettre d'éviter certains oublis, et de se poser quelques questions qui ne seraient pas forcément venues à l'esprit.

5.3.2 Les méthodes ascendantes

On part des effets de la menace : le cours de nos actions s'effondre, notre personnel nous quitte, notre chiffre d'affaire s'écroule, le ciel nous tombe sur la tête, etc.

Puis on remonte aux causes (menaces) qui peuvent être à l'origine de cet événement, à l'aide d'un outil tel que l'arbre des causes. Le traitement du risque consiste alors naturellement à travailler sur chaque cause, de façon à réduire la menace et ses effets.

Pour les risques majeurs, dont on a vu qu'ils sont la conséquence de plusieurs causes indépendantes élémentaires, cette démarche est rassurante : on est sûr, en éliminant au moins une des causes, de transformer ce risque majeur en un risque « ordinaire ».

5.3.3 Les méthodes descendantes

Dans ces méthodes, on part des causes : un concurrent apparaît, nos ateliers sont sales, une inondation survient, etc.

Ensuite, on en déduit les effets qui peuvent toucher l'entreprise : perte de chiffre d'affaire, grève du personnel, fuite de clients... On peut utiliser un outil simple comme le 5 M (pour main-d'œuvre, méthode, milieu, matière première, matériel) (Figure 5.3).

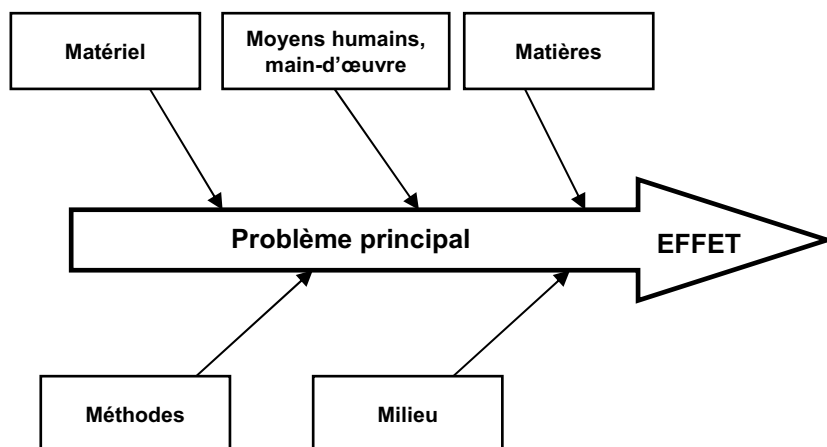


Figure 5.3 Le diagramme « 5 M »

5.3.4 Les méthodes mixtes

On peut – on doit ! – combiner tous les types d'approche. Sur le plan pédagogique, cela permet de toucher du doigt la difficulté de procéder à un inventaire des risques. Sur le plan méthodologique, on va ainsi, naturellement, vers une meilleure exhaustivité.

La combinaison d'un arbre des causes et d'un 5 M porte même un joli nom évocateur : le « diagramme papillon ».

5.4 Maîtrise des risques : évaluation et caractérisation

Il faut donc évaluer la criticité, par exemple à partir d'une des formules du paragraphe 5.2.1. L'essentiel est de ne pas se laisser aveugler par le confort que donne la clarté apparente de la formulation : on ne se déplace pas ici dans un

espace rigoureux à deux dimensions mesurées par un système d'unités cohérentes !

La probabilité est effectivement une grandeur physique qui peut se mesurer en occurrences par événement et/ou par unité de temps. On peut bien entendu utiliser des « vraies » probabilités, dont la forme mathématique est rigoureuse, et exprimée en puissance de 10 : par exemple « 10^{-2} accident mortel par an et pour 10 000 personnes ». C'est bien là une grandeur physique, elle peut se mesurer et sa mesure peut être manipulée dans des opérations mathématiques. Mais il ne faut pas perdre de vue que l'échelle logarithmique qu'elle emploie résulte d'un choix, qui ne sera pas sans conséquence sur le résultat.

La forme peut être beaucoup plus simpliste : une échelle du genre « 4 = très probable, 3 : probable, 2 : peu probable, 1 : improbable, 0 : impossible » peut également se rencontrer.

Quant à la gravité... Par exemple, même dans le cas simple d'un risque financier, il semble naturel d'évaluer la gravité via le montant des sommes mises en jeu... Quoique... une perte de 10 000 € est-elle 1 000 fois plus grave qu'une perte de 10 € (échelle arithmétique) ou bien seulement 4 fois plus grave (échelle logarithmique) ?

Quant aux autres risques... La tentation est bien entendue de tout ramener au coût des effets, ce qui conduit, pour les risques humains par exemple, à évaluer le « prix du mort ». Débat complexe et assez repoussant dans lequel nous n'entrerons pas.

Dans ces conditions, on se contente souvent d'échelles plus qualitatives, du genre « mortel – très grave – grave – peu grave – sans effet »... Tant qu'on en reste à mettre des événements dans des cases, pas de problème : cela suffit souvent. Mais on commence à faire n'importe quoi quand on veut quand même dresser un tableau de calcul, car il faut alors définir une échelle dont tout porte à croire qu'elle sera arbitraire alors que son choix n'est pas sans conséquences sur le résultat.

Beaucoup de questions dans les lignes qui précèdent, et peu de réponses ! Celles-ci dépendent évidemment du contexte de l'entreprise et de la culture ambiante. À défaut d'une solution simple, notre message se bornera à deux conseils qui, eux, prétendent l'être :

- faire très attention au choix des échelles et des mesures, et rester bien conscient des conséquences de ses choix sur la grandeur et la précision des résultats ;

- faire encore plus attention aux outils et méthodes standards que l’on trouve dans les ouvrages ou dans les discours de consultants : ils s’appuient sur des choix qui ne sont pas toujours explicites, et la rigueur apparente du processus proposé peut cacher des biais lourds de conséquences.

5.5 Management des risques : le rôle des dirigeants

5.5.1 Risques et stratégie

Pour ne pas compliquer le schéma, nous avons omis au paragraphe 5.2.2 une troisième boucle, implicite : celle qui passe par les objectifs stratégiques de l’entreprise (Figure 5.4). C’est en fonction de ces objectifs – et donc plus globalement de sa stratégie – que la décision d’accepter ou de maîtriser un risque est pertinente ou ne l’est pas.

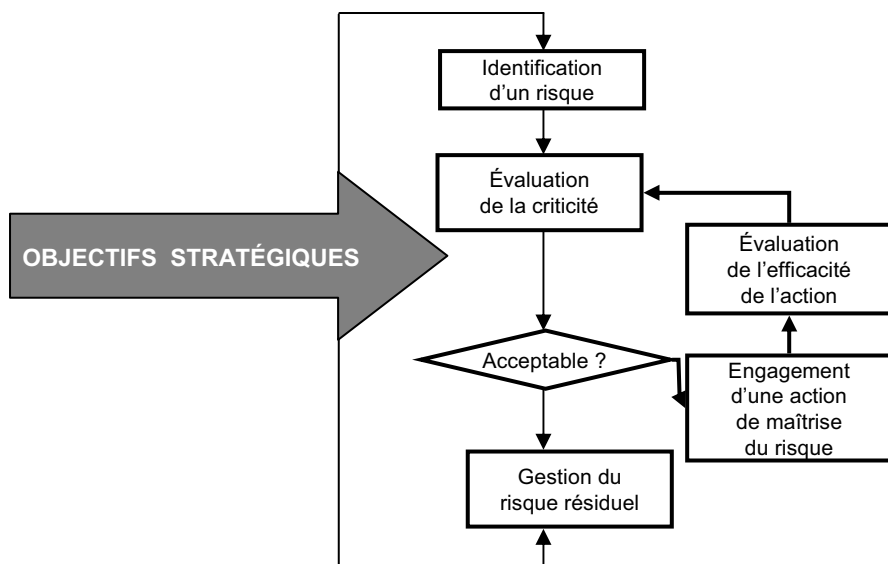


Figure 5.4 Stratégie et management des risques

Ce qui ne veut pas dire, loin de là, que l’entreprise est seule juge : une « bonne » décision prend naturellement en compte les exigences des parties prenantes, à travers, justement, cette stratégie... À condition, évidemment, qu’elle soit bien faite.

Nous sommes bien là dans le domaine du management. Nous allons y rester dans les paragraphes suivants.

5.5.2 Élaboration et validation des politiques

Une des responsabilités majeures de la Direction est l'élaboration des politiques (*cf.* paragraphe 4.1.2), dont la politique « management des risques ».

L'engagement visible est un préalable, mais n'est évidemment pas suffisant. Une politique ne doit pas être – seulement – un acte de foi, et encore moins un programme électoral (comme il en existe quelques-uns...). Elle doit contenir des éléments concrets qui permettront à l'ensemble de l'entreprise de faire les choix qui seront les meilleurs. Elle doit permettre de valider ces choix *a posteriori*, de les peaufiner, voire de les amender à la lumière de l'expérience.

On peut donner ici quelques critères, qui permettront de juger si une politique de management des risques est digne de porter ce nom. Cette politique définit, avant tout, **les niveaux de risques (criticité) acceptables**. Mais bien d'autres critères (communs à toutes les autres politiques d'ailleurs) peuvent être mis en avant :

- la cohérence avec la stratégie ;
- la cohérence avec les stratégies et politiques des autres entreprises du groupe, des partenaires, etc. ;
- les éléments communs à toutes les politiques évoquées ci-dessus ;
- la cohérence et la complémentarité avec les autres démarches de progrès pré-existantes ;
- le respect de la réglementation ;
- le sens global de la démarche (par exemple responsabilité sociale et environnementale) ;
- la clarté et la « déployabilité » de la politique ;
- le bon équilibre entre moyen terme et long terme ;
- l'existence d'indicateurs chiffrés, etc.

Cette « dignité » à porter le nom de politique doit être formelle et visible : c'est pourquoi la Direction élaborera et publiera des critères d'acceptabilité. Une bonne pratique, rencontrée en entreprise, consistait à publier des « balises »

permettant de guider l'élaboration et la validation de la politique. Ces « balises » étaient de trois sortes :

- le « prescrit » : conditions à remplir absolument pour être acceptable ;
- le « recommandé » : les orientations à privilégier, les conseils sur la forme, le fond... ;
- le « proscrit » : ce qui entraînerait le refus de validation.

En tout état de cause, la validation de la politique fait l'objet d'une décision explicite et publique. Puis cette validation déclenche le déploiement de la politique.

5.5.3 Déploiement

Déployer une politique n'est pas chose simple : cela demande beaucoup d'énergie et de persévérance. Un journaliste a écrit : « le problème, avec les managers, c'est qu'ils se désintéressent d'une idée dès qu'ils l'ont comprise ». Jugement un peu sévère, mais pas dénué de vérité : le chemin est très long entre l'assimilation d'une idée par un cerveau, en général performant, et l'intégration de la même idée – sous une forme parfois différente – dans la culture d'un groupe.

Le risque de « vrai-faux déploiement » n'est donc pas nul. Une bonne pratique consiste à organiser ce déploiement en tenant compte de la culture et de la structure de l'entreprise, ainsi que de l'énergie qu'on peut y consacrer.

Schématiquement, il existe quatre types de déploiements, illustrés par la figure 5.5.

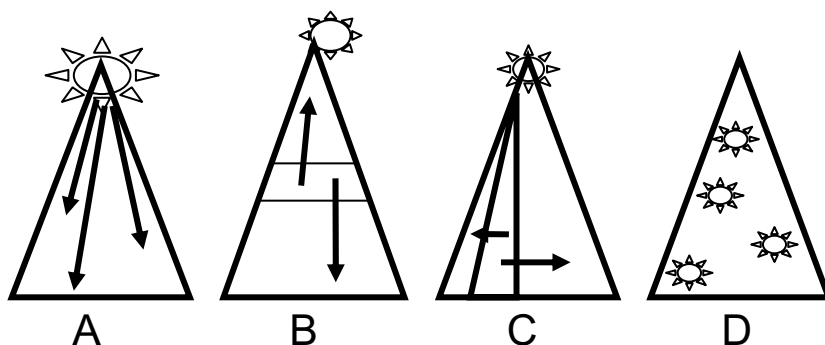


Figure 5.5 Les quatre types de déploiement

- A – le déploiement « *top-down* » : toute l'énergie est dissipée au sommet, et contribue à diffuser la politique partout dans l'entreprise, en même temps, et verticalement.
- B – le déploiement « métiers » : l'énergie est principalement dépensée à un niveau intermédiaire, choisi en fonction de sa pertinence. Un bouclage strict est nécessaire par le sommet, mais c'est son seul rôle et l'énergie qu'il dépense est donc moindre.
- C – le déploiement « expérimental » : la politique est d'abord déployée dans un secteur de l'entreprise (agence, service, usine...) puis, après retour d'expérience, est généralisée. L'énergie est dépensée dans le secteur expérimental et au sommet, mais elle est inférieure à celle du cas A.
- D – le déploiement « nénuphar » : très peu d'énergie au sommet, on laisse faire en espérant qu'un jour le nénuphar couvrira l'étang ; évidemment c'est rarement le cas.

Le type de déploiement à adopter dépend naturellement du contexte. Mais on peut dire sans trop se tromper que le déploiement « *top-down* » a plus de chances de réussir dans les organisations de petite taille, et/ou si le contexte justifie un investissement à court terme qui peut atteindre 10 % des forces vives. Le déploiement « métiers » sera recommandé dans les organisations complexes et diversifiées, comme les groupes composés d'entités très différentes et que ne relie, parfois, que le cours de l'action. Le déploiement « expérimental » est une bonne solution dans les grands organismes composés de nombreuses entités analogues.

Quant au déploiement « nénuphar », jamais, au grand jamais, nous ne l'avons rencontré...

5.5.4 Processus de pilotage

Les paragraphes qui précèdent traitent du rôle majeur des dirigeants : élaborer et déployer les politiques, et en particulier la politique de management des risques. Il nous faut maintenant « boucler la boucle » du schéma du paragraphe 5.5.1.

C'est là un processus de pilotage classique. Le but est d'aboutir à un plan de maîtrise des risques (PMR) qui sera mis en œuvre et dont la mise en œuvre fera l'objet des contrôles adéquats.

Il n'y a là rien de nouveau par rapport aux méthodes de pilotage des autres démarches de progrès. Nous nous bornerons donc seulement à citer quelques bonnes pratiques :

- L'élaboration du PMR se fera sur le mode participatif : c'est une condition essentielle à sa qualité, et en particulier à la pertinence de l'identification et de la caractérisation.
- L'élaboration des actions se fera également sur le mode participatif, afin d'en optimiser le déploiement et l'acceptation.
- Le processus de révision sera piloté de façon exemplaire, via des revues périodiques sur lesquelles une communication adaptée sera faite.
- Les acteurs impliqués et concernés seront formés, condition nécessaire à la qualité du déploiement et à leur motivation.
- Un système de reconnaissance sera mis en place, à moins qu'il n'existe déjà.
- Ce système prendra en compte les succès autant que les échecs ; pour les succès, ce ne sera pas chose facile, puisque cela reviendra à valoriser des non-événements. La pertinence des indicateurs sera alors primordiale : quoiqu'on pense, on peut communiquer sur les trains qui arrivent à l'heure !
- Le système de contrôle mobilisera les équipes et les collaborateurs en charge de cette activité. Ce sera une garantie de professionnalisme. On luttera contre la tentation de mobiliser les experts des domaines concernés, car on ne peut être juge et partie.

La périodicité des contrôles et des revues va cadencer la mise en œuvre du PMR. Loin de nous l'idée d'afficher un quelconque mépris pour cette façon de procéder. Mais on comprendra aisément qu'il s'agit là d'initier un mouvement alternatif. Le risque est donc d'une certaine perte d'efficacité : dans les cas limites (jamais rencontrés, bien entendu, dans la réalité !) on « fait du risque » une fois par an et on l'oublie le reste du temps. La conséquence majeure est que cette façon de procéder ne contribue pas à promouvoir un « esprit risques » dans l'entreprise.

On a vu précédemment que nous proposons de positionner l'entreprise, en permanence, dans un espace à trois domaines : le fonctionnement normal, incidentel, accidentel.

Il s'agit là d'une tout autre conception du management des risques, puisqu'il devient permanent : pour reprendre l'expression du paragraphe précédent, on ne « fait pas du risque » une fois par an, on « baigne dedans » en permanence.

C'est l'esprit dans lequel le chapitre 6, sur les familles de risques, est rédigé, et ceci constitue, nous l'espérons, le principal apport conceptuel de cet ouvrage.

5.5.5 Autres obligations du management

Les autres « obligations » du management sont classiques et ne seront ici évoquées que rapidement :

- L'exemplarité : à la fois dans le traitement des risques et dans le comportement de tous les jours : rien de pire qu'un patron qui entre dans un atelier sans son casque, quand le port de celui-ci est requis.
- La transparence : toute l'efficacité d'une démarche de management des risques repose sur la confiance que les collaborateurs peuvent nourrir vis-à-vis de cette démarche ; rien de pire, là aussi, que la découverte d'un risque majeur caché, comme par exemple une pollution.
- La visibilité de l'engagement personnel : à la fois dans les discours et dans les actes, y compris celui de donner des ressources.

5.5.6 Rôle du management pendant les crises

Pendant les crises, le management change de forme et les managers changent de rôle. Il y faut quelque vertu, et en particulier jouer – encore plus que d'habitude ! – l'équipe plutôt que le pouvoir personnel.

Afin d'éviter les répétitions, le rôle du management avant, pendant et après les crises est développé au paragraphe 4.3.3.

6

Les familles de risques

Le chapitre sur les familles de risques est conçu comme un document à entrées multiples.

On traite d'abord des risques « processus » et « projets ». Comme on a vu au paragraphe 4.1.2, ces deux concepts recouvrent à eux seuls toutes les activités de l'entreprise. Maîtriser les risques des processus et des projets est donc – en théorie – suffisant pour maîtriser tous les risques de l'organisation.

C'est pourquoi ces deux paragraphes sont développés un peu plus longuement que les suivants. C'est une approche qui en vaut une autre, mais ce n'est pas la seule et surtout ce n'est pas la plus intuitive.

C'est pourquoi les paragraphes suivants sont organisés à peu de choses près selon les neuf éclairages fournis par le modèle EFQM (paragraphe 4.1.3).

Quel que soit le paragraphe, la structure détaillée est ensuite la même :

- De quoi parle-t-on : quel domaine ?
- Quels sont les risques dans ce domaine ?
- Comment faire pour les maîtriser en restant dans le fonctionnement normal ?
- Comment sait-on qu'on est dans le domaine incidentel ? Que faire pour revenir au fonctionnement normal ?

- Comment sait-on qu'on est entré dans le domaine accidentel, et comme faire pour en sortir dans les meilleures conditions ?

6.1 Risques processus

6.1.1 Qu'est-ce qu'un processus ?

D'après la norme ISO 9000:2000, un processus est un « ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie ». Il est à noter que le propre d'un processus est d'apporter de la valeur ajoutée au produit ou service transformé.

Cette définition ne manque pas d'aridité, et ne se prête guère, sous cette forme, à un déploiement facile : nous dirons plus simplement que les processus donnent une image de l'ensemble des savoir-faire de l'entreprise. Et qu'il est bon de les identifier, de les décrire, de les munir d'indicateurs, pour les améliorer sans cesse, voire d'en corriger les défauts.

Nous en profiterons pour dénoncer une erreur que font bien des entreprises qui se lancent dans la certification : les processus d'une entreprise (pré) existent, démarche qualité ou pas. À l'occasion d'une démarche de certification, contrairement à ce que certains consultants prétendent, on ne crée pas les processus. *A priori*, sauf anomalie majeure, on ne modifie pas les processus à ce moment-là : c'est autre chose, cela s'appelle du « *reengineering* » (ou « re-conception » de processus). Il s'agit d'une démarche de rupture qu'il est tout à fait inopportun, voire dangereux, de lancer en même temps qu'une certification – qui elle, s'apparente à la recherche de l'amélioration continue.

Un processus permet de réaliser une ou des activités, dans le but de répondre à un objectif de l'organisme, afin de satisfaire un client (interne ou externe), par un ou plusieurs « livrables ».

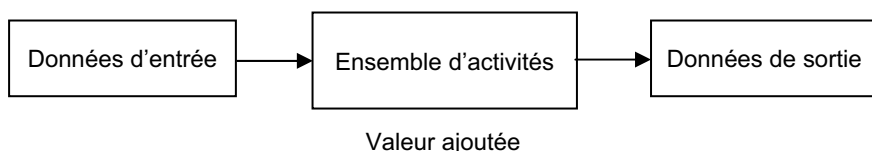


Figure 6.1 Description (très succincte) d'un processus

La description d'un processus passe par les étapes suivantes :

- détermination de l'intitulé du processus ;
- définition du but et de la raison d'être ;
- identification du ou des domaines dans lequel il est mis en œuvre ;
- identification des intervenants ou acteurs ;
- détermination de leurs rôles ;
- détermination des conditions de déclenchement ;
- description chronologique des actions : séquencement ;
- identification des flux d'information : données d'entrées, de sorties ;
- définition des conditions de fin du processus (ainsi est-il absolument bien borné) ;
- établissement des interactions potentielles avec d'autres processus ;
- détermination des outils et documents associés.

Un processus doit :

- Être répétable : le processus peut être répété dans les mêmes conditions et dans le temps. Il peut être suivi et compris par l'ensemble du personnel qui l'exploite ou l'améliore.
- Être mesurable : on s'assure que le produit ou service issu du processus correspond à l'objectif fixé, pour cela on met en place des indicateurs de performance.
- Posséder des interactions avec les autres processus de l'organisme.

Une entreprise est constituée d'un ensemble de processus liés entre eux. Les données de sortie d'un processus « A » correspondent aux données d'entrée d'un processus « B ». Ces interactions sont très importantes puisqu'elles forment les liens entre les différents processus de l'organisme, elles doivent donc être parfaitement identifiées. C'est aux frontières entre les processus, on le verra, que se génèrent souvent les risques.

Un processus est un ensemble d'activités qui sont, en général, **transversales** à l'organisation de l'entreprise. En effet, plusieurs services peuvent intervenir dans la réalisation d'un processus (par exemple : le bureau d'études définit les solutions, le service logistique livre les matériaux, la fabrication produit les solutions...).

Les processus d'un organisme peuvent être répartis en plusieurs catégories :

- **Processus de management d'un organisme** comprenant notamment les processus liés à la planification stratégique, à l'établissement des politiques, à la fixation des objectifs, à la mise en place de la communication, à la mise à disposition des ressources nécessaires et aux revues de direction.
- **Processus de management des ressources** (ou « processus support ») comprenant notamment les processus concourant à la mise à disposition des ressources nécessaires aux processus de réalisation.
- **Processus de réalisation** (ou « processus opérationnels ») comprenant tous les processus qui permettent de fournir les résultats attendus de l'organisme.
- On parle aussi des **processus de mesure, d'analyse et d'amélioration** (ou « processus de pilotage ») nécessaires pour mesurer et recueillir les données utiles à l'analyse des performances et à l'amélioration de l'efficacité et de l'efficience. Ces processus, qui comprennent les processus de mesure, de suivi et d'audit, les actions correctives et préventives, font partie intégrante des processus de management, de management des ressources et de réalisation.

À partir de la cartographie de l'ensemble des processus, il est bon d'identifier les processus clés de l'entreprise. Ce sont les processus qui sont indispensables au bon fonctionnement de l'organisme. Par exemple dans le cas d'un organisme qui fonctionne en « juste à temps », le processus « approvisionnements » est un processus clé. Quand on parle de risques, c'est dans ces processus qu'on trouve, en général, les risques majeurs.

6.1.2 Quels sont les risques qui menacent la performance des processus ?

Un processus est efficace et sûr si ses données de sortie correspondent aux objectifs fixés. On peut mesurer son efficacité grâce aux indicateurs de performance pertinents et judicieusement choisis. On mesure sa « sûreté » en maîtrisant les risques de façon méthodique.

Il existe plusieurs types d'indicateurs : taux, ratios, coûts... Leur choix est essentiel à la performance du processus. Bien plus, c'est l'ensemble des indicateurs mesurant la performance des processus qui constitue la « base de données » avec laquelle on pourra mesurer la performance globale de l'entreprise... et au passage, de son système de management de la qualité.

En tout état de cause, un indicateur et son objectif associé doivent être PAMM (Pertinents, Accessibles, Motivants et Mesurables) ou bien SMART (traduit de l'anglais : Spécifiques, Mesurables, Accessibles, Réalistes et calés dans le Temps).

Comme toujours, le risque n'existe que s'il y a danger et une cible menacée par le danger – en l'occurrence le processus.

Pour garantir les processus contre les risques qui les guettent, les indicateurs doivent donc être placés tout simplement là où les risques sont les plus importants. C'est donc un travail spécifique, mais en général on ne se trompe guère en les plaçant :

- aux interfaces avec les autres processus (entrées/sorties) ;
- aux interfaces avec les parties prenantes ;
- après chaque activité difficile, complexe ou dangereuse.

Les indicateurs peuvent être – doivent être si possible – chiffrés pour être mesurables. Mais un code de couleurs type « vert – orange – rouge » peut également parfaitement faire l'affaire. Cette codification peut également être, de façon implicite ou pas, de façon visible ou pas, reliée à une comparaison arithmétique entre des valeurs et de seuils.

Les méthodes décrites au chapitre 5.3 peuvent être mises en œuvre pour identifier les risques « processus ». À titre d'exemple, ils peuvent l'être aussi via une méthode qui en vaut bien une autre, celle des « 5 M » :

- Méthode :
 - le processus est trop compliqué ;
 - le processus est inutile ;
 - le processus n'est pas bouclé.
- Main-d'œuvre :
 - les ressources humaines sont insuffisantes en nombre ;
 - le personnel n'est pas formé ;
 - le responsable du processus ne maîtrise pas toutes les étapes du processus.
- Matière :
 - les données d'entrée ne sont pas conformes au cahier des charges ;
 - les données de sortie ne sont pas conformes au cahier des charges.

- Moyen :
 - les indicateurs sont mal définis (ils ne permettent pas de vérifier l'adéquation avec les objectifs) ;
 - les interactions avec les autres processus sont mal définies ;
 - les procédures et/ou modes opératoires permettant de réaliser les tâches du processus sont mal définis.
- Milieu :
 - le processus ne dispose pas de l'environnement nécessaire à sa bonne réalisation ;
 - le milieu a changé de façon significative ;
 - le milieu est plus agressif que prévu.

Bien sûr cette liste n'est pas exhaustive, elle doit être approfondie au sein de l'organisme par le groupe de travail qui sera chargé de déterminer les risques liés aux processus.

On peut utiliser pour ce travail toutes les méthodes classiques. En particulier l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) donne de bons résultats. Mais avant de s'y lancer, on ne perdra pas de vue que cette méthode est souvent d'une mise en œuvre souvent assez laborieuse, on ne sait jamais trop où s'arrêter. Dans le cas de l'analyse des risques processus, ce problème n'est pas trop grave puisque, si la cartographie et la description des processus ont été bien faites, le domaine de l'étude est bien délimité.

6.1.3 Le domaine normal

Un processus est efficace (il est dans le domaine « normal ») s'il satisfait les clients (externes ou internes).

• Comment le définir

Le domaine normal est facile à caractériser si les processus ont été décrits : puisqu'ils sont instrumentés, cela signifie tout simplement que tous les indicateurs sont au vert.

La fréquence de la surveillance des indicateurs est évidemment essentielle : elle se fait au jour le jour – ou minute par minute, ou année par année, selon le rythme du processus en question.

Comme on ne vit pas dans un monde stable, quelques indicateurs pourront passer à l'orange sans qu'on sorte du fonctionnement normal ; mais il ne s'agira en aucun cas d'indicateurs concernant des processus clés.

- **Comment y rester : méthodes et bonnes pratiques**

La prévention du risque est le meilleur moyen de minimiser sa réalisation et donc de permettre au processus de rester dans le domaine normal.

Les méthodes sont celles permettant de garantir les processus contre les risques, et découlent donc toutes du management de la qualité, avec des niveaux de sophistication divers. On en citera trois, de complexité croissante.

L'assurance Qualité

L'organisme peut utiliser un certain nombre de méthodes et outils permettant de maintenir et améliorer le niveau de qualité des processus (rappelons que la qualité peut être définie comme un ensemble de caractéristiques permettant de satisfaire les besoins des clients).

Le principe de l'amélioration continue est de détecter les dysfonctionnements dans le but de les éradiquer le plus en amont possible. Ce principe est souvent matérialisé par la roue de Deming (Figure 6.2).

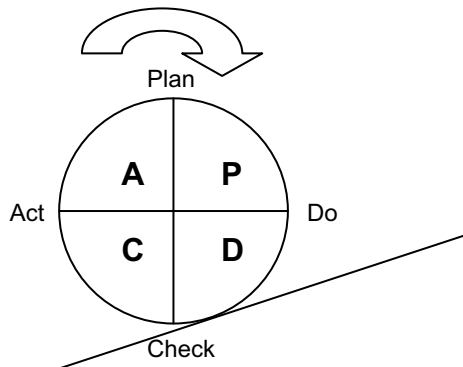


Figure 6.2 La roue de Deming

La roue de l'amélioration continue est caractérisée par un cycle continu en quatre phases, qui se répètent sans cesse :

- *Plan* : on détermine les objectifs à atteindre et on planifie la liste des actions.
- *Do* : on réalise les actions prévues.

- *Check* : on mesure ou évalue l'efficacité des actions réalisées et l'atteinte des objectifs.
- *Act* : à partir de l'analyse de l'efficacité du système, on décide de réagir ou non, et sur quoi.

De façon plus générale, l'entreprise désirant améliorer son mode de fonctionnement, pour réduire les dysfonctionnements et non-conformités, peut se lancer dans une démarche qualité impliquant tout le personnel et les activités de l'organisme. Afin de garantir son niveau d'efficacité, l'organisme peut sanctionner sa démarche qualité par une certification selon un référentiel qualité, avec l'intervention d'un organisme externe qui atteste la conformité au référentiel choisi... ou bien met en évidence ce qui ne l'est pas. Le plus connu est la norme ISO 9001, mais une foule d'autres référentiels existent, tous plus ou moins bâtis sur le même principe (ISO 14001 pour l'environnement, etc.) et plus ou moins spécifiques à un type d'activité (automobile, armement, aviation...). Parmi beaucoup d'autres facteurs clés de succès, mais qui sont communs à toutes les démarches de progrès, on n'en citera que trois, plus spécifiques :

- Le choix du « bon » référentiel, et en particulier le choix entre un référentiel « prêt à porter » ou un référentiel « métier » (voire l'écriture d'un référentiel « maison » – tendance souvent constatée et malheureusement souvent inopportune).
- La décision ou non de faire certifier par tierce partie.
- la constitution d'un « point zéro » à partir duquel on mesurera les progrès effectués. Ce point est essentiel, et le moins facile à atteindre : en effet, le « point 0 » est souvent issu de la base des indicateurs de performance des processus... qu'on n'a pas encore décrits et encore moins instrumentés... Il n'empêche que sans ce travail préalable, pas de mesure, et donc pas de preuve de l'efficacité de la démarche !

Ne pas chercher ces facteurs clés de succès, c'est faire courir des risques importants – voire vitaux – à la démarche, et ceci à court et à long terme.

MSP : Maîtrise Statistique des Procédés

L'efficacité d'un processus peut également être garantie en mettant en place la MSP. Le principe de cette méthode est de suivre l'évolution des données de sortie d'un processus. Des limites de tolérance sont spécifiées par le client. Ainsi on peut mettre en place des actions correctives lorsque l'évolution des données se rapproche des limites de tolérance.

Six Sigma

La méthode Six Sigma est une méthode d'amélioration de la qualité par rupture.

Un processus est caractérisé, d'un point de vue mathématique, par une moyenne et une étendue. Cependant le processus peut, s'il est mal maîtrisé, être décentré par rapport à la moyenne cible et prendre des valeurs se situant en dehors de la zone d'étendue admise. Le principe de la méthode Six sigma est de remédier à ces écarts. Le but est d'obtenir une moyenne de 3 à 4 défauts par million de pièces produites, ou d'actes délivrés au client.

D'où le nom de la méthode, clair pour ceux qui ont quelques notions de statistiques, et totalement rébarbatif pour tous les autres – en général le plus grand nombre. C'est un de ses défauts, auquel on peut ajouter toute une quincaillerie de vocabulaire et d'éléments d'organisation qui en font une opération toujours très lourde... mais très profitable : c'est donc aussi sa principale qualité.

Cette méthode se décompose en cinq phases qui sont :

- Définir : définition et structure du projet.
- Mesurer : mesurer la performance actuelle.
- Analyser : analyser les données du processus sur lequel on va agir.
- Innover- améliorer : définir et mettre en œuvre les solutions.
- Contrôler : vérifier l'amélioration de l'efficacité et « transversaliser » la méthode vers les autres processus de l'organisme.

6.1.4 Le domaine incidentel

Le domaine incidentel est franchi lorsque le processus ne fonctionne plus de manière efficace. Dit autrement, les indicateurs ne sont plus tous au vert.

• Comment le définir : savoir qu'on y est

- un au moins des indicateurs des processus clé n'est pas au vert ;
- un nombre significatif d'indicateurs de l'ensemble des processus n'est pas au vert ;
- un au moins des indicateurs de l'ensemble des processus est au rouge.

On peut aussi disposer d'autres signaux, qui seront d'autant plus pertinents qu'ils se situeront plus en amont dans la conception du processus :

- le dysfonctionnement a un impact sur les données de sortie ;

- un des risques décrits au paragraphe 6.1.2 (milieu, méthodes, etc.) se manifeste de façon évidente.

- **Comment agir : méthodes et bonnes pratiques**

Une situation incidentelle n'implique pas forcément de graves conséquences : on n'est pas (encore) en crise. Une réaction est nécessaire, mais sans oublier d'évaluer la gravité de l'incident et le coût engendré pour y remédier.

Parmi les actions les plus simples :

- revoir le système de pilotage du processus ;
- revoir les indicateurs et mieux estimer leurs qualités (pertinence, etc.) ;
- redéfinir les contrôles : fréquence, méthodes... ;
- etc.

Mais on peut être conduit à :

- redécrire le ou les processus ;
- changer de responsable du ou des processus ;
- augmenter, temporairement ou pas, les contrôles ;
- réétudier les indicateurs et les objectifs ;
- etc.

A priori, toutes ces actions ou réactions seront conduites et mises en œuvre avec les moyens et les ressources courantes de l'entreprise. Il n'y a pas non plus lieu, à ce stade, de rechercher de nouvelles méthodes ou de faire appel à des appuis externes inhabituels.

6.1.5 Le domaine accidentel

Le fonctionnement des processus n'est plus du tout celui qui était désiré, ou courant. On entre en crise. Cette crise peut être générale, ou bien limitée à un domaine, un processus, une partie de l'entreprise. Mais dans le domaine considéré le temps est venu de l'action immédiate.

- **Comment le définir : savoir qu'on y est**

Ce sont les indicateurs qui vont conduire à constater la crise :

- plusieurs indicateurs de processus clé sont au rouge ;
- tous les indicateurs, ou presque, de l'ensemble des processus ne sont plus au vert.

Au contraire du domaine incidentel, il est peu probable que des informations « amont » permettront de définir l'état de crise. Ce seront plutôt des signaux « aval » :

- pertes financières – mouvements anormaux d'actions ;
- pertes importantes de clients – afflux de réclamations ;
- campagne de presse ;
- etc.

• **Comment agir : méthodes et bonnes pratiques**

De façon adaptée à la situation et au domaine de crise, l'organisation à adopter est toujours la même :

- décider et faire savoir qu'on est en crise – définir le domaine ;
- organiser le management selon les schémas décrits au chapitre 4 ;
- prendre rapidement les mesures nécessaires à la sauvegarde de l'entreprise.

L'équipe de crise sera constituée intégralement. Le titulaire du poste « opérationnel » aura des qualités certaines en organisation. En matière de communication, on prendra soin de vérifier en quoi la défaillance des processus peut avoir des causes ou d'effets sur les processus des parties prenantes.

Pour focaliser les propos sur les processus, objets du présent paragraphe, il est plus que probable qu'un remaniement profond des processus, de leur description et de leur management sera rapidement indispensable. Parmi les méthodes :

- pratiquer un *reengineering* complet ou partiel ;
- revoir de façon importante les responsabilités, et en particulier opérer des changements dans les responsables de processus ;
- revoir la description complète des processus de l'entreprise.

Pendant et à la sortie de la crise, il est probable que des supports externes seront nécessaires. Ils peuvent être de nature très diverse selon la situation :

- recours à des conseils externes ;
- appel à des compétences managériales externes de façon temporaire ;
- refonte de l'équipe de direction ;
- opération de formation d'envergure ;
- révision de la stratégie ;
- etc.

Comme pour toute crise, il conviendra d'organiser une sortie « propre » : analyse et retour d'expérience, communication, managements des blessures, des frustrations...

6.2 Risques projet

6.2.1 Qu'est-ce qu'un projet ?

D'après la norme FD X50-118 : « Un projet est un processus unique, qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques incluant les contraintes de délais, de coûts et de ressources ».

L'AFITEP en donne une description beaucoup plus riche, qu'on trouvera en annexe 1.

On glissera ici pudiquement, car là n'est pas le débat, sur la question de savoir si un « processus unique » peut être un processus, alors qu'on a écrit pas ailleurs qu'un processus est nécessairement répétable. On laissera donc les experts et les exégètes en débattre à loisir, pour n'en tirer qu'une idée : un projet ne se manage pas comme un processus ; et on n'en manage donc pas les risques de la même manière.

D'ailleurs, en tant que tel, le projet ne constitue-t-il pas en lui-même un facteur de risque ?

Classiquement on découpe un projet en différentes phases. Chacune relève de risques spécifiques, et ses défaillances constituent un risque majeur pour la suivante :

- phase d'émergence ;
- phase d'avant-projet ;
- phase de développement ;
- phase de réalisation ;
- phase de qualification et réception ;
- phase de déploiement ;
- « service après-vente » ;
- démantèlement – recyclage.

Non moins classiquement, on distingue différents types de projet, pour lesquels les risques ne seront pas tout à fait les mêmes :

- **Projet d'ouvrage** : une seule livraison, un client unique

On appelle projet d'ouvrage un projet qui au final produira une seule unité. Il n'y a donc qu'une seule phase de réalisation, l'équipe projet n'a pas le droit à l'essai : on ne peut pas se permettre de réussir un pont au deuxième coup ! Le risque portera donc essentiellement sur la conduite de projet.

On ne peut donc pas parler d'amélioration continue pour ce genre de projet. Cependant le retour d'expérience aura son utilité mais en sera d'autant plus délicat.

- **Projet de produit** : une série de produits et plusieurs clients

Un projet de produit a pour objectif la mise sur le marché d'un nouveau produit. Le risque portera donc notamment sur le fait de bien cibler le besoin du marché. La conduite de projet est très importante également, mais lorsque le produit est réalisé en grande série, des améliorations peuvent être apportées en cours de réalisation, voire après la livraison. Mais les coûts ne seront pas du tout les mêmes.

6.2.2 Les acteurs d'un projet

On distingue trois catégories d'acteurs dans un projet, et on verra que cette distinction est fondamentale pour la résistance du projet aux risques. On n'insistera jamais assez sur l'importance de les identifier, quel que soit le projet, quelle que soit son importance.

Les fonctions correspondantes empruntent, assez couramment, au vocabulaire de la construction. On reprendra ces termes, mais nous en utiliserons d'autres qui nous semblent plus pertinents, pour autant évidemment que le projet ne soit pas un immeuble... Des experts pourront faire remarquer que ces termes peuvent ne pas avoir le même sens selon les cultures d'entreprise, et ne pas recouvrir exactement les mêmes concepts. C'est vrai et c'est bien là la question. Il conviendra donc de choisir celui qui convient le mieux... voire d'en inventer d'autres !

- **Le Commanditaire** : doté des pouvoirs nécessaires dans l'entreprise, il décide l'engagement du projet. Il a le pouvoir, si nécessaire, de réorienter ou d'arrêter le projet. Parmi ses pouvoirs, il a en particulier celui d'accorder les ressources et celui d'imposer un plan de management des risques.

Dans l'exemple de la maison, c'est le futur occupant ou son représentant (promoteur).

- **Le Pilote stratégique** : désigné par le Commanditaire, son rôle est de prendre les décisions stratégiques du projet et de s'assurer en permanence de la cohérence de celui-ci avec le reste de l'activité de l'entreprise. Il peut, selon les cas, proposer la réorientation du projet ou son arrêt au Commanditaire. Pour ce qui concerne les risques, c'est lui qui approuve la teneur, l'ambition et le pilotage du plan de management des risques.

Dans l'exemple de la maison, c'est l'architecte.

- **Le Pilote opérationnel** : désigné par le Pilote stratégique, il pilote la mise en œuvre du projet jusqu'à sa clôture. Ainsi, il prend toutes les décisions nécessaires à son aboutissement à condition qu'elles ne relèvent pas explicitement du rôle du Pilote stratégique ou du Commanditaire. C'est lui qui élabore le plan de management des risques et le fait appliquer.

Dans l'exemple de la maison, c'est l'entrepreneur.

On emploie également, comme dit plus haut, les termes de « maître d'ouvrage » et « maître d'œuvre », ainsi bien entendu que « chef de projet ».

Un projet ne mobilise pas que trois personnes... Ces fonctions ne sont pas des emplois, et inversement dans les grands projets elles peuvent être assurées par des groupes entiers. Bien plus, tous les partenaires de l'entreprise, internes et externes, doivent être pris en compte. Cette idée est d'autant plus importante qu'un projet peut avoir tendance à s'isoler, ce qui, on le verra par la suite, peut générer des risques importants.

Parmi ces partenaires, en ne citant que les plus importants :

- les sous-traitants ;
- la collectivité dans laquelle le projet va s'insérer ;
- le personnel qui va être concerné, et par voie de conséquence...
 - les services financiers ;
 - le service communication ;
 - le service contrôle/audit ;
 - etc.

6.2.3 Les risques qui menacent un projet

Comme il l'a été dit précédemment, selon sa nature (d'œuvre/de produit) le projet peut comporter des risques dont l'importance n'est pas identique.

Globalement, les risques pour un projet se regroupent dans le triangle classique de la qualité (Figure 6.3).

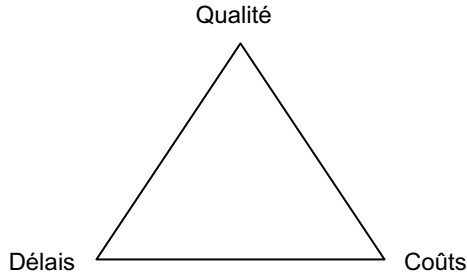


Figure 6.3 Le triangle de la qualité

Et la cible des dangers qui guettent le projet est naturellement constituée, en premier lieu, par le livrable du projet lui-même. Mais cette cible peut-être plus large, jusqu'à l'entreprise elle-même, par exemple dans le cas où le projet est trop ambitieux pour ses moyens.

Nous donnons ci-dessous (Tableau 6.1) quelques idées pour illustrer ce que pourra produire une identification des risques, selon deux axes :

- Identification des risques à partir des composantes du projet : ressources, complexité, types de projet.
- Identification des risques au cours des différentes phases du projet

6.2.4 Le domaine normal

• Comment le définir

Le projet est dans le domaine normal lorsque les objectifs sont atteints, que les livrables sont livrés en temps et heure, que les ressources attribuées sont suffisantes. Bref, être dans le domaine normal, c'est respecter le triptyque coût/qualité/délais.

• Comment y rester : méthodes et bonnes pratiques

Tout repose sur la façon de manager et de conduire le projet. Dans les grandes entreprises, ainsi que dans les entreprises où le « mode projet » est le mode principal de fonctionnement, on aura intérêt à définir un « référentiel de management de projet » adapté et spécifique (mais pas trop quand même, afin que les partenaires externes s'y retrouvent). Dans les autres cas, on adoptera plutôt

Tableau 6.1 L'identification des risques selon les phases du projet

Phase du projet	Ressources humaines	Ressources matérielles/ temporelles	Performance technique
Phase d'émergence			Étude de marché mal ciblée
Phase d'avant-projet	Choix de compétences et fonctions inadaptées à la nature du projet	Besoins budgétaires sous-estimés Choix de technologies à risques	Étude de faisabilité irréaliste
Phase de développement	Tâches réparties inégalement au niveau du groupe	Planning trop optimiste (non respecté) Défaillance de sous-traitants	Analyses fonctionnelles, AMDEC incomplètes
Phase de réalisation	Manque de cohésion au sein du groupe Départ de compétences clés Conditions de travail inadaptées	Mauvaise planification Incompatibilité entre projets au sein de l'entreprise	Livrables non conformes au cahier des charges (CDC) Nombre excessif de sous-traitants
Phase de qualification et réception	Manque de compétences dans les activités de contrôle	Retard dans la réception	Produit non conforme au CDC
Phase de déploiement	<i>Insuffisance des ressources disponibles</i>		<i>Projet inadapté à la vie série</i>
Service après-vente Démantèlement	Perte de la trace des compétences	Organisation insuffisante ou inadaptée Disparition des sous-traitants	<i>Obsolescence des matériels et logiciels (pièces de rechange)</i>

Légende du tableau : les termes en **gras** se rapportent plutôt aux **projets d'œuvre**, ceux en *italique* plutôt aux *projets de produits*.

un référentiel « prêt à porter » comme en proposent les organismes professionnels et les conseils de tous poils.

Un projet n'est pas répétable, on a vu plus haut que le nommer « processus » est quelque peu abusif. Mais si les projets se succèdent, la boucle vertueuse de l'amélioration continue devient alors essentielle et le processus de pilotage des projets devient alors un processus clé de l'entreprise.

Identifier les acteurs et les missions

D'abord, il faut définir les différents éléments se rapportant à la conduite de projet :

- Définir le projet :
 - les objectifs du projet (cahier des charges) ;
 - le périmètre du projet et les paramètres à prendre en compte.
- Les différentes tâches de la conduite de projet :
 - identifier toutes les activités du projet ;
 - construire le planning ;
 - définir les ressources nécessaires ;
 - préciser les phases critiques ;
 - définir les spécifications ;
 - contrôler l'avancement ;
 - construire un tableau de bord et assurer le suivi du projet.
- Construire l'équipe projet :
 - valider les critères de choix (expertise, motivation, disponibilité...) ;
 - déterminer les rôles et fonctions de chacun.
- Piloter l'équipe projet :
 - établir et respecter le plan de travail ;
 - se conformer tout au long du projet au tableau de bord de suivi ;
 - accompagner et mobiliser en permanence les acteurs : passer du mode collectif au mode individuel.

De plus, pour être performant au sein d'un projet, nous avons vu précédemment qu'il faut agir sur les coûts, les délais et la qualité. Pour ce faire, plusieurs outils sont à la disposition du groupe de travail :

- l'arborescence du produit ;
- l'organigramme des tâches ;

- les outils de contrôle des coûts prévisionnels ;
- les outils de gestion de la configuration.

Enfin, afin de maîtriser les risques pouvant se produire au cours des différentes phases du projet, le groupe procède à une analyse de risques en s'appuyant sur le tableau ci-dessus. Chacun des risques est ensuite répertorié selon son niveau de gravité, l'objectif est de rendre acceptables des risques jugés inacceptables. Pour cela, trois modes d'actions sont possibles :

- **Réduction** : pour réduire le risque on peut agir sur trois facteurs :
 - diminuer la probabilité d'apparition du risque (mise en place d'actions préventives) ;
 - diminuer la gravité du risque (mise en place de solution alternative en cas d'apparition) ;
 - améliorer la détection (mettre des verrous à certaines étapes du projet).
- **Transfert** : il s'agit des transferts de risques à un tiers, type assurance. Ce type de traitement permet d'atténuer les impacts sur les coûts.
- **Provisionnement** : c'est en quelque sorte une « auto-assurance ». En effet, il peut parfois revenir moins cher à l'organisme de provisionner les coûts éventuels que de « lutter » contre l'apparition du danger. C'est évidemment une opération... à risque, qu'on ne peut se permettre que quand on a les reins solides.

Organiser le projet

La séparation des pouvoirs et responsabilités entre les acteurs est un facteur clé de succès ; inversement le mélange des genres (l'un des pilotes faisant le travail de – ou des ! – autres) est une cause quasi inéluctable d'échec du projet, ou au moins de dépassements importants des coûts ou des délais. C'est souvent le manque de compétence ou de disponibilité du commanditaire qui en est la cause. On se souvient des projets informatiques des années 80, où on comptait, aussi bien en termes de coûts que de délais, un facteur « pi » entre les réalisations et les prévisions...

Quant à la qualité...

Les revues de projet

Un acte, ou plutôt une série d'actes, est essentiel à la sécurité du projet : les revues de projet.

Une revue de projet rassemble tous les acteurs ; elle se tient de façon la plus formelle possible au moins à la fin de chaque phase. C'est le moment où les pilotes stratégiques et opérationnels font le point devant le commanditaire ; c'est là que le commanditaire procède au seul geste que, en fin de compte, il ne peut déléguer : autoriser le passage à la phase suivante.

On n'insistera jamais assez sur l'importance des revues de projet ; on résistera aussi à la critique – facile – selon laquelle quand on arrive au moment de la revue tous les boutons de guêtre brillent de mille feux. Car une revue de projet, c'est fait pour cela !

Si elle est bien menée, si le *reporting* est bien fait, si le suivi entre les revues est garanti (par exemple par une fonction appelée « assistance à maîtrise d'ouvrage »), le projet n'est certes pas assuré d'arriver à son terme, mais au moins de ne pas connaître de gros aléas.

La communication

Afin de coordonner toutes les phases du projet, une bonne communication est essentielle. Mettre en place un plan de communication est donc indispensable.

Un plan de communication présente en général les points suivants :

- les moyens de collecte des informations ;
- les destinataires de l'information : suivant le type d'information, les destinataires peuvent être différents ;
- une description de l'information ;
- le calendrier d'émission de chaque type d'information.

6.2.5 Le domaine incidentel

• Comment le définir : savoir qu'on y est

La frontière entre chacun des domaines peut parfois être difficile à délimiter.

En début de projet, le groupe peut définir l'échelle de risques à partir des indicateurs de coût, qualité et délais. Ainsi lorsqu'une anomalie sera détectée, le chef du projet sera en mesure de réagir.

Il est, sous une forme ou sous une autre, deux outils indispensables au projet : le tableau de bord, qui rassemble les indicateurs de type « qualité » et « coûts » et le planning qui se rapporte plutôt aux indicateurs de type « délais ».

On entre dans le domaine incidentel quand les indicateurs de l'un ou de l'autre de ces outils dépassent des seuils que le commanditaire aura définis par avance,

et qui s'imposeront aux autres acteurs, à savoir le pilote stratégique et le pilote opérationnel. Ce qui n'interdit pas la coopération et la concertation... C'est donc de ce travail préalable au lancement même du projet que dépend la suite.

Le tableau ci-dessous (Tableau 6.2) permet de donner une idée de l'échelle que l'on peut adopter (l'exemple est pris pour le critère « délai », il pourra être fait de même pour les critères « qualité » et « coût »).

Tableau 6.2 échelle de risques pour le critère « délai »

Impact délai	Critère
4 : catastrophique	> 3 mois
3 : majeur	1 à 3 mois
2 : moyen	0,5 à 1 mois
1 : mineur	< 0,5 mois
0 : pas d'impact	

S'il s'agit d'un impact mineur, on peut considérer le projet comme étant en fonctionnement normal.

S'il s'agit d'un impact moyen, le projet est alors en fonctionnement incidentel

S'il s'agit d'un impact majeur et catastrophique le projet est en situation d'accident (ou crise).

• **Comment agir : méthodes et bonnes pratiques**

Si le projet entre en situation d'incident, il revient au chef de projet de remettre le projet sur les « rails ». Il doit être capable (sinon, l'incident, c'est lui...) de mettre en œuvre de façon autonome les moyens qui permettront de résoudre le problème : groupe de résolution de problème, audit, conseil, modifications de l'équipe, changement de fournisseur, etc.

Mais LA bonne pratique essentielle doit le conduire à alerter de façon formelle le commanditaire et le pilote stratégique. Ces derniers pourront décider que le problème est suffisamment important pour qu'ils investissent des ressources supplémentaires dans le projet, en premier lieu, leur propre temps et leurs propres compétences, sous la forme de revues de projet supplémentaires.

Que de passages en situation de crise auraient été évités si le chef de projet avait sorti sa tête de son guidon, mis son amour-propre dans sa poche, le temps de faire le point et d'en informer ses partenaires...

6.2.6 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

Un projet entre en situation d'accident si sa bonne fin est remise en cause, au moins sous la forme prévue dans les premières phases, ou telle que l'avait prévu le commanditaire.

Les outils cités plus haut, le planning et le tableau de bord, peuvent contenir des indicateurs qui permettront de décider de l'état de crise. Mais plus vraisemblablement ce sera un événement grave qui provoquera son déclenchement :

- perte brutale de compétences clés ;
- campagne de presse ;
- disparition d'un fournisseur clé ;
- émergence d'une concurrence inattendue...

- **Comment agir : méthodes et bonnes pratiques**

La décision de proclamer l'état de crise est prise par l'ensemble des acteurs. Il se peut que le chef de projet en soit l'origine, si celui-ci a une conscience de la situation et un recul suffisants. Plus souvent ce sera le commanditaire ou le pilote stratégique qui seront les mieux placés pour jouer ce rôle éminemment désagréable.

Comme toujours dans ce cas, l'organisation normale n'est plus adaptée, et il convient de constituer une équipe de crise dans les meilleurs délais. Tous les acteurs participent à l'action directe, et pendant un certain temps la séparation des pouvoirs et des responsabilités a tendance à s'atténuer : il ne faut donc pas que cela dure trop longtemps.

Les solutions pour revenir à l'état normal dépendent évidemment de la situation. Mais une chose est sûre : on ne réagit jamais trop vite ou trop fort. Un projet, même modeste, est un transatlantique lancé à pleine vitesse, et qui souvent cherche à battre un record de traversée au milieu des icebergs. Il faut du temps pour l'arrêter ou même infléchir sa route. Autre élément souvent déterminant : un projet véhicule beaucoup de passions, nées de l'idée, du fonctionnement en équipe, du goût du challenge. C'est donc à des obstacles psychologiques qu'on risque d'être confronté quand il faudra prendre des mesures comme le changement de l'équipe, l'appel à l'externalisation, la réduction de l'ambition du projet... Personne n'aime « tuer les petits chats ». Le courage et la coopération seront plus que jamais nécessaires s'il faut arrêter complètement le projet. Les qualités du commanditaire devront alors s'exercer à plein.

6.3 Risques humains

6.3.1 Que sont les risques humains ?

Dans cet ouvrage, on entendra par « risques humains » ceux dont la personne est la cible. Pas de confusion, donc, avec les risques causés par l'homme.

C'est un des domaines, et c'est bien normal, où les références documentaires et réglementaires sont les plus nombreuses et les plus complètes. Nous noterons simplement que depuis quelques années, on assiste à la généralisation de la recherche du risque zéro. Une évidence ?... Et pourtant, il y a seulement quelques dizaines d'années (et sans doute encore dans de nombreux pays où la vie ne semble pas avoir le même prix), il était « normal » que des mineurs meurent au fond de la mine, que des morts soient déplorés sur les chantiers de construction, et même plus simplement qu'on se tape sur les doigts avec un marteau : « c'est le métier qui rentre »...

Il faut tirer son chapeau à quelques grandes industries (pétrole, nucléaire – et ceci avec des motivations d'ailleurs différentes) qui ont montré que même si le risque zéro n'existe pas, une entreprise se doit de n'avoir qu'un seul objectif : que chaque collaborateur revienne de son lieu de travail et rentre chez lui en entier et en bonne santé.

6.3.2 Les types de risques dont la personne humaine est la cible

L'éventail des risques ayant trait à la sécurité des personnes dans un organisme est particulièrement vaste.

On peut néanmoins les classer selon quelques grandes familles :

- les risques liés aux circulations et déplacements ;
- les risques liés aux effondrements et chutes d'objets ;
- les risques liés aux bruits ;
- les risques thermiques ;
- les risques chimiques ;
- les risques de radiation ;
- les risques liés à l'utilisation des moyens de production (machines coupantes...) ;
- les risques liés à la manutention ;
- les risques liés au contact des personnes avec des produits ou matières nocives (amiante, plomb...).

6.3.3 Le domaine normal

- **Comment le définir : savoir qu'on y est**

Les acteurs de la maîtrise des risques humains ont de la chance : ils disposent de deux indicateurs bien définis et qui sont reconnus par tous : le taux de fréquence et le taux de gravité. Certes des réserves sont toujours possibles, et des précautions indispensables lors des analyses, mais ces deux outils sont essentiels pour mesurer les progrès et faire du *benchmarking*.

Ces deux indicateurs gagnent à être complétés par d'autres, plus fins, et plus « anticipateurs » : presque accidents, taux de formation, etc.

Le domaine normal est donc défini par rapport à ces indicateurs et à l'absence d'événements exceptionnels. Comme il s'agit de valeurs évoluant lentement, et sujettes, comme tous les indicateurs de ce genre, à des biais dus au mode de collecte, les tendances sont au moins aussi importantes que les valeurs absolues.

- **Comment y rester : méthodes et bonnes pratiques**

Les acteurs de la maîtrise des risques humains ont une chance supplémentaire : ils disposent aussi d'un texte normatif, l'OSHAS 18001. Il présente les exigences relatives aux systèmes de management de la santé et de la sécurité, afin de permettre à un organisme de maîtriser les risques pour la santé et la sécurité et d'améliorer ses performances. Comme tout texte normatif spécifique à une famille de risques, il présente l'avantage d'être assez facile à déployer, et l'inconvénient de ne pas simplifier l'intégration des autres démarches de progrès transverses.

Ces acteurs sont également encadrés par de nombreux autres textes réglementaires, et en particulier la loi du 31 décembre 1991 qui impose une évaluation des risques de chaque entreprise.

Afin d'aider les organismes dans leur démarche d'analyse des risques, les pouvoirs publics ont édité la circulaire DRT N° 6 (18 avril 2002). Cette directive a pour vocation d'informer les employeurs sur la création d'un document relatif à l'analyse des risques dans les domaines de la santé et la sécurité des travailleurs.

Les résultats de l'évaluation des risques devront être transcrits sur un document unique, et ceci dans l'optique de répondre à trois exigences :

- De cohérence, en regroupant, sur un seul support, les données issues de l'analyse des risques professionnels auxquels sont exposés les travailleurs.

- De commodité, afin de réunir sur un même document les résultats des différentes analyses des risques réalisées sous la responsabilité de l'employeur, facilitant ainsi le suivi de la démarche de prévention des risques en entreprise.
- De traçabilité, la notion de « transcription » signifiant qu'un report systématique des résultats de l'évaluation des risques doit être effectué, afin que l'ensemble des éléments analysés figure sur un support. Celui-ci pourra être écrit ou numérique, laissant à l'employeur le soin de choisir le moyen le plus pratique de matérialiser les résultats de l'évaluation des risques. Dans tous les cas, l'existence de ce support traduit un souci de transparence et de fiabilité, de nature à garantir l'authenticité de l'évaluation. Pour tout support comportant des informations nominatives, l'employeur devra, conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, procéder à une déclaration auprès de la Commission nationale de l'informatique et des libertés.

Mais dans le domaine de la sécurité comme nulle part ailleurs, la prévention et la formation sont essentielles.

L'attitude de la Direction ne l'est pas moins. Les Comités d'Hygiène et de Sécurité sont des endroits *ad hoc* pour faire avancer l'analyse des problèmes et leur solution. Bien plus, et ceci pour peu que toutes les parties prenantes en aient la volonté, ils sont des lieux privilégiés de dialogue social : ceci dépasse largement le management de la sécurité au travail. Autre bonne pratique, l'intervention systématique et individuelle du plus haut dirigeant lors d'un accident du travail est un levier efficace : la visibilité, dans ce domaine, ne se délègue pas.

Si on a l'opportunité de s'appuyer sur des démarches de progrès préexistantes, ou bien encore si on recherche cohérence et économie de moyens, on s'intéressera aux démarches QSE, qui intègrent le management de la Qualité, de l'Environnement et de la Sécurité.

6.3.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

On entre dans le domaine incidentel quand les indicateurs évoqués plus haut passent à l'orange, voire au rouge. Un accident de personne est **toujours** une cause de réaction immédiate.

Cela ne suffit pas, si on ne veut pas rester sur le mode de la réaction : il faut anticiper, et anticiper le plus possible.

Tous les signaux faibles montrant une augmentation des risques sont à prendre en compte. Ce qu'on appelle les « presque accidents » (« On a eu chaud », « C'était moins une »...) sont une source essentielle d'information... Pourvu qu'on sache les capter !

Mais il faut remonter encore plus haut, vers tous les signes qui font penser que la situation se dégrade : l'ambiance au travail (en particulier les conflits, la fatigue après un « coup de bourre »...), la propreté et l'ordre, les dysfonctionnements de processus... C'est la conjonction de plusieurs de ces signaux faibles qui déclenchera la réaction nécessaire des dirigeants.

• **Comment agir : méthodes et bonnes pratiques**

Après un événement, la réaction va des premiers soins à l'analyse des causes de l'événement. Elle ne doit pas omettre les cibles secondaires : les collègues, la famille, voire l'extérieur de l'entreprise. L'analyse des causes entraîne presque obligatoirement un plan d'action, qui devra être public, suivi, réalisé et faire l'objet d'un bilan.

Dans le domaine de la prévention, toutes les actions visant à amoindrir les effets potentiels des signaux faibles évoqués plus haut sont bonnes à prendre et à mettre en œuvre. La communication et la formation jouent un rôle essentiel ; mais il ne faut pas négliger les types d'actions toutes simples et très visibles, comme par exemple commencer par (faire) mettre de l'ordre dans les ateliers (méthode des « 5 S² »).

Le déclenchement d'une réaction suite à la détection de convergence de signaux faibles n'est possible que s'il existe un niveau de synthèse suffisant à la tête de l'organisme, et la volonté qui va avec : c'est le rôle des plus hauts dirigeants mais aussi des experts comme les ingénieurs sécurité. Rôle difficile s'il en est : jouer les Cassandre n'est pas agréable, et la sanction pour avoir joué ce rôle se solde par un non-événement !

-
2. La méthode des « 5 S » est un outil de management japonais, qui vient de la première lettre de chacune des cinq opérations :
- Seiri (ordonner, supprimer tout ce qui est inutile) ;
 - Seiton (ranger, pour retrouver facilement) ;
 - Seiso (dépoussiérer, découvrir des anomalies, inspecter régulièrement) ;
 - Seiketsu (standardiser, établir des règles) ;
 - Shitsuke (être rigoureux, respecter, faire respecter et améliorer continuellement).

6.3.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

C'est un truisme de dire qu'on entre en situation accidentelle... quand il se produit un accident. C'est pourtant à peu près cela, à cette réserve près que l'accident « de référence » en question peut être paramétré, selon ses effets et le nombre de ses cibles.

Il est également bon de décréter une situation de crise lorsqu'un incident moins grave se reproduit une nouvelle fois : il ne s'agit pas là forcément d'une atteinte directe à la personne humaine, mais d'un signal signifiant que les barrières qui doivent la protéger sont défaillantes, ce qui à terme revient au même. Cette attitude est d'autant plus justifiée que l'opinion, interne comme externe, accepte à la rigueur un événement grave quand il survient la première fois ; mais elle ne pardonne absolument pas s'il se reproduit.

- **Comment agir : méthodes et bonnes pratiques**

Les méthodes et bonnes pratiques évoquées plus haut sont bien entendu également valables dans ce cas-là : constitution d'une équipe de crise, maîtrise de la communication, etc. La visibilité des plus hauts dirigeants est particulièrement indispensable : plus encore que dans les autres cas, les fonctions de crise ne pourront pas être déléguées.

Un point singulier, en particulier après un accident grave de personne, est que les réparations, même sans limitation de leurs conséquences financières, ne sont pas capables de restituer l'état antérieur. C'est évident en cas de décès d'un collaborateur. C'est aussi vrai à la suite d'événements moins dramatiques, et les esprits restent marqués de façon durable. Pour les collaborateurs, l'idée que l'organisation qui les nourrit peut aussi être un danger pour eux, mais qu'elle est impuissante à tout réparer, leur est insupportable. Pour résumer, on ne peut jamais vraiment « revenir au fonctionnement normal ». Les conséquences peuvent donc largement dépasser le strict domaine des effets de l'événement, la confiance de tous est durablement ébranlée, et à cause de cela des « répliques » sont à attendre partout et très longtemps.

6.4 Risques financiers

6.4.1 Les finances

Il n'est guère besoin d'une définition. Cette partie du patrimoine présente un avantage considérable : il se mesure à l'aide d'une unité qui est parfaitement

partagée au sein d'une communauté économique, et même mondialement quand on use des monnaies de référence.

Quand on regarde les finances sous l'éclairage des risques, deux idées apparaissent qui tempèrent cependant ce point de vue :

- les problèmes financiers sont souvent, dans l'entreprise, le domaine des dirigeants – quand ce n'est pas des experts qui gardent jalousement leur pré carré à l'aide de méthodes et ou de vocabulaire abscons et le plus souvent empruntés au « *business English* » ;
- les ordres de grandeur sont difficiles à maîtriser pour le plus grand nombre : il y a plusieurs zéros entre un budget industriel et le budget familial... quand il ne se trouve pas encore quelques confusions entre les francs et les euros.

Ces deux constats font que les politiques en matière de risques financiers sont difficiles à déployer.

6.4.2 Les types de risques financiers

Les ouvrages très complets sur les risques financiers abondent ; c'est un des domaines où les réflexions ont été les plus riches (si on ose dire...). Ce n'est pas un hasard, car le sujet est motivant !

Il y a trois genres de risques financiers, selon qu'on se place du point de vue :

- de l'actionnaire ;
- des créanciers ;
- de l'entreprise.

À l'exception notable de l'actionnariat salarié, la gestion financière est en général l'apanage des dirigeants. Les attitudes de ces derniers dépendent largement de leur implication personnelle (capital personnel ou familial, stock-options...).

Il va de soi que les trois sont intimement liés, mais que les différences dans les enjeux conduisent à des politiques ou à des actes différents, voire antagonistes.

En ce qui concerne l'actionnaire, « il s'agit du risque de perdre tout ou partie de son capital, c'est-à-dire de ne pas récupérer sa mise de départ ».

Pour les créanciers, le risque est de ne pas recouvrer ce qu'ils ont injecté dans l'entreprise (banques), ou attendent d'elles (fournisseurs, État). Pour les premiers, c'est rarement une question de survie. Pour les seconds, c'est plus souvent le cas. En ce qui concerne l'État et les organismes sociaux, le risque est d'autant moins vital qu'en cas de difficulté, ils sont prioritaires.

En ce qui concerne l'entreprise, les risques sont plus nombreux et variés, puisqu'ils concernent aussi l'ensemble de la gestion financière, depuis le très court terme (trésorerie), jusqu'au long terme (investissements), en passant par le non-paiement des salaires. Pour les dirigeants en particulier, les situations sont également diverses, selon qu'ils risquent leur patrimoine personnel, leurs stock-options ou « simplement » leur poste.

« Qui ne tente rien n'a rien »... Ce dicton s'applique particulièrement aux risques financiers. Placer une action en bourse peut rapporter des sommes d'argent importantes. Mais on peut aussi en perdre. On est cependant là, toujours, dans le risque positif avant tout. Risque encore plus positif que pour le loto ou le casino : les « joueurs » de jeux de hasard savent plus ou moins inconsciemment que le gagnant le plus probable est l'organisateur du jeu. Quand on investit dans une entreprise, cotée en Bourse ou non, on ne part pas « potentiellement perdant ». Et pourtant...

Globalement, on peut dénombrer plusieurs familles de risques financiers :

- les risques de taux, ou « d'intérêt » ;
- les risques de « change » (ou plus généralement « risques pays ») ;
- les risques « clients » ;
- les risques « matières premières » ;
- les risques « actions et indices » ou « de marché ».

Comme toujours, une telle liste n'est pas parfaite, tout en montrant des redondances. On cite aussi les risques « de liquidité » (impossibilité à un moment donné de faire face à ses échéances), les risques « produits » (perte d'argent dû à un taux de non-conformité produit très élevé), etc.

On ne mentionnera pas ici non plus les risques issus des malversations et autres corruptions. D'une part ce genre de comportement n'a évidemment jamais existé nulle part, d'autre nous les classerons dans les risques éthiques, bien que les conséquences financières concrètes et sur l'image puissent en être particulièrement douloureuses.

6.4.3 Le domaine normal

• Comment le définir : savoir qu'on y est

On est dans le fonctionnement normal lorsque l'on se trouve dans l'une des situations suivantes :

- le placement qu'on a réalisé en bourse rapporte ;

- le prêt que l'on a consenti est honoré ;
- on a les moyens financiers de rembourser l'emprunt qu'on a effectué ;
- on est capable de faire face aux échéances de l'entreprise (salaires, fournisseurs, charges sociales, etc.) ;
- les clients paient leurs dûs en temps et en heure.

Tout ceci se transpose sur des tableaux de bord, munis des indicateurs qui conviennent. Sur ce point pas de souci, toutes les entreprises – sauf sans doute les toutes petites – disposent d'indicateurs financiers. Ils ont au moins à leur disposition ceux qui leur sont imposés par la loi et les services des impôts, ce qui n'est pas sans inconvénients, comme on le verra dans le paragraphe suivant.

C'est donc à partir de ces indicateurs que les dirigeants définiront dans quel domaine la veille financière seule est requise.

• **Comment y rester : méthodes et bonnes pratiques**

En matière de tableau de bord, les dirigeants veilleront à ce que ces indicateurs évoqués au paragraphe précédent aient un caractère suffisamment anticipatif des tendances qui peuvent se faire jour. Ils ne seront pas toujours aidés dans ce travail par leurs comptables, qui sont formatés pour penser plutôt « bilan »... Ce qui revient à piloter l'entreprise en regardant dans le rétroviseur. Un autre souci sera d'obtenir les indicateurs les plus pertinents, à la fois par leur poids sur les résultats et les risques, et aussi par leur dimension managériale : plus souvent les pertes matière que les fournitures de bureau...

Les risques financiers « se couvrent », c'est-à-dire qu'ils peuvent se transférer, sous de multiples formes, et en premier lieu sous forme d'assurances. Tous ces produits financiers, de plus en plus nombreux et sophistiqués, portent des noms à consonance anglaise. Sans prétendre proférer une vérité absolue, nous avancerons que tous les risques financiers s'assurent. Le seul problème est de savoir à quel prix. Et comme l'assurance est toujours trop chère avant l'accident, les entreprises sont en général sous-assurées pour ce genre de risques.

Les décisions de se couvrir s'appuient sur des méthodes classiques (VAR : *value at risk*) et sur des dispositions réglementaires ou pararéglementaires (FAS133/IAS39), etc.

Les audits financiers sont essentiels à la veille financière. Il s'agit en général d'activités convenablement organisées, et plutôt mieux acceptées par les collaborateurs impliqués que les autres types d'audits. Le choix d'un cabinet

d'audit est déterminant : il devra être à la fois à l'écoute et avoir le recul et l'indépendance nécessaires à l'efficacité de son action. Il n'est pas besoin de rappeler les scandales – on en parlera dans le paragraphe « domaine accidentel » – des dernières années : Enron, Crédit Lyonnais, etc.

De tels événements ne sont pas l'apanage des grandes entreprises : dans les petites, le mauvais fonctionnement du couple dirigeant-expert comptable est souvent une cause de non-détection des signaux qui conduisent à une crise.

Plus globalement – et plus pompeusement – les discours actuels tournent autour de ce qu'on appelle la gouvernance d'entreprise. Il s'agirait de LA parade à tous les risques financiers. Au-delà du mot, les concepts qui lui sont associés, et qui ne sont pas tous nouveaux, loin s'en faut, peuvent faire partie de la boîte à outils, ou au moins du vocabulaire des dirigeants.

En se plaçant d'un autre point de vue, la qualité de la relation avec les parties prenantes joue un rôle essentiel dans la solidarité avec laquelle elles vont aider l'entreprise à maîtriser ses risques. On cite évidemment le rôle des banques. Mais la confiance des clients et des fournisseurs est tout aussi déterminante quand l'entreprise connaît des difficultés. C'est alors – et aussi après, si elle survit ! – que l'entreprise se félicitera d'avoir pratiqué une politique d'amélioration de la satisfaction de toutes ses parties prenantes, autrement dit une politique TQM.

6.4.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

Un retard d'un paiement de la part d'un gros client, une action qui décote en bourse, un taux de non-qualité conduisant à des pertes importantes... L'équilibre financier peut dans ce cas se retrouver en danger. À ce stade l'organisme fonctionne encore normalement, la direction est en mesure de payer son personnel et ses fournisseurs.

Ce sont les indicateurs comptables qui vont déclencher les premières réactions. Encore faudra-t-il que les dirigeants aient préalablement fixé les seuils d'alerte, avec les bons indicateurs et les bonnes cadences de scrutation. Ceci semble d'un tel bon sens. Mais il ne faut pas oublier qu'un dirigeant d'entreprise en difficulté rapproche encore le nez de son guidon, et que sa volonté de s'en sortir se traduit par un optimisme excessif. Quand il n'enfoncé pas, de façon consciente ou pas, sa tête dans le sable des expédients : le surendettement n'est pas un fléau qui frappe seulement les familles modestes.

Avec ces gestes élémentaires, combien de dépôts de bilans seraient évités, et combien de liquidations se feraient sans dégâts majeurs sur les dirigeants et les actionnaires ! Cela peut même, ce qui à rechercher absolument, contribuer à adoucir le sort des personnels.

- **Comment agir : méthodes et bonnes pratiques**

La réaction doit être adaptée au problème, et n'est évidemment pas de même nature selon qu'on traite un défaut passager de trésorerie ou une chute du cours de l'action.

En matière financière plus que pour toute autre, une réaction immédiate est indispensable. Tout est y particulièrement volatil, et les effets se cumulent et s'enchaînent à une vitesse sans pareille. Au-delà du capital financier, le capital de confiance est toujours atteint, et le but final est de le reconstituer, voire de l'augmenter.

Le retour d'expérience et le plan d'actions qui doit suivre sont indispensables. L'incident peut présager d'autres événements plus graves, il convient donc de se prémunir contre une telle éventualité.

Parmi les mesures à prendre à moyen terme, le renforcement des fonds propres est en tout état de cause une saine précaution. Si on parle actionnariat, sa restructuration peut s'avérer pertinente. Si les ennuis viennent des clients, des mesures visant à mieux connaître leurs attentes et leur perception seront des apports précieux.

6.4.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

Dans ce domaine, le terme de « crise financière » est largement usité et correspond assez bien à ce que nous appelons le domaine accidentel.

La crise peut être circonscrite à l'entreprise ou bien venir de l'extérieur.

Lorsque les retards de paiements des clients s'accumulent, que les taux de non-conformités s'alourdissent au point que la direction n'est plus en mesure de payer ses dettes, ses fournisseurs et ses employés, on entre dans le domaine accidentel si la survie de l'entreprise est en jeu. On tombe alors dans une spirale plus ou moins violente dont le fond est le redressement judiciaire, voire la liquidation.

La crise peut être beaucoup plus globale, et même mondiale. Les indicateurs qui vont franchir les seuils qui déclencheront le passage en situation de gestion de crise sont difficiles à définir à l'avance. Les dirigeants ne seront pas aidés par les médias, dont le mot crise est un des ingrédients de base. On sait en général bien définir l'événement qui déclenche la crise... *a posteriori*, quand les historiens se sont emparés de l'affaire !

Tout autant que les indicateurs internes, qui joueront leur rôle s'ils sont bien faits, c'est l'observation de l'environnement qui fournira les signaux pertinents, mais plus ou moins faibles : attitude des concurrents, comportement des politiques... Si on est embarqué sur un bateau, il suffit d'observer les rats.

• **Comment agir : méthodes et bonnes pratiques**

En cas de crise financière, bien rares sont les cas où l'entreprise peut s'en sortir toute seule.

L'équipe de crise sera constituée selon la structure de l'entreprise. On aura soin de vérifier que le poste opérationnel soit tenu par un collaborateur qui ait les qualités adéquates, même si, comme cela risque d'être le cas, il occupe dans la vie normale un poste d'expert.

Bien entendu ses partenaires ont un rôle à jouer : les banques, c'est évident, mais aussi les fournisseurs qui pourront consentir des facilités, et même les clients qui apporteront leur soutien à l'entreprise d'une façon ou d'une autre, en premier lieu en ne la quittant pas.

C'est donc dans la « gestion » de ces partenariats que réside la capacité, ou non, de l'entreprise à éviter sa disparition.

Si on aborde le redressement judiciaire, les leviers d'action commencent à échapper aux dirigeants, même si on ne peut réussir cette opération sans eux. Le plan de redressement judiciaire est établi par le tribunal, il comporte un volet économique visant à la pérennité de l'entreprise, un volet financier visant au règlement du passif de l'entreprise, et un volet social, ayant pour but la réduction des charges salariales pour permettre le redressement de l'entreprise. Le juge dispose d'un panel « d'outils » : il peut imposer la cession d'actifs, imposer aux créanciers un échelonnement du remboursement de la dette, etc. Le but est de limiter au possible la casse sociale et de circonscrire au possible l'endettement. Il est parfois proposé la vente de l'entreprise ou l'arrivée de nouveaux partenaires financiers. Les offres des intéressés sont évaluées et mises en concurrence selon plusieurs critères, dont la qualité de l'éventuel repreneur, de son projet industriel, etc. Le créancier peut également proposer de transformer sa créance en une part de l'entreprise.

En cas de crise globale, nationale ou mondiale, les leviers d'actions ne sont évidemment guère à portée de mains. Ceci ne signifie pas qu'il faut subir ! Il est moins facile de nager dans un tsunami que dans une eau calme, mais ceux qui s'en sortent sont ceux qui, en tout état de cause, savent le mieux nager – ou surfer sur les vagues.

À propos de vagues, il faut savoir que dans la pire des tempêtes l'eau est calme dès qu'on s'enfonce de quelques mètres : le bon comportement peut donc être la veille, ou encore le retrait. C'est douloureux de renoncer à la jolie filiale étrangère qu'on a peiné à créer il y a peu, mais il faut parfois le faire si le pays entre en ébullition. Et on ne prend jamais ce genre de décision assez tôt.

6.5 Risques clients

6.5.1 Le client...

Sans client, l'entreprise n'a pas de raison d'être : toutes les organisations, plus ou moins explicitement, ont donc mis le client au centre de leurs préoccupations. Toutes essaient de déployer cette idée vers l'ensemble de leurs collaborateurs et partenaires. Ceci avec un succès plus nuancé cependant, selon la nature et la culture de l'organisation. Il y a des « clients rois », mais encore aussi des abonnés, voire des « assujettis » !

6.5.2 Les risques clients

On peut distinguer deux familles de risques clients, dont l'entreprise est la cible :

- le client a un défaut de solvabilité et ne peut pas payer l'entreprise : le risque vient de lui et peut impacter l'entreprise ;
- l'entreprise provoque l'insatisfaction de son client, qui va donc réagir négativement vis-à-vis de son fournisseur.

Nous ne mentionnons que pour mémoire les risques que l'entreprise – qui devient alors un danger – fait courir à ses clients : ils sont traités avec les risques fournisseurs, évoqués par ailleurs. On se reportera donc au chapitre correspondant, *mutatis mutandis*.

Nous ne traiterons pas non plus dans ce chapitre des risques que les clients font courir à l'entreprise via l'usage qu'ils font de leurs produits : on commence à mettre en cause des cafetiers qui ont laissé leurs clients partir ivres, mais on n'a pas – encore – poursuivi un marchand d'armes parce que ses produits ont

permis une guerre plus « efficace » donc plus meurtrière. On peut espérer des évolutions sur ce point...

Dans la littérature spécialisée – il suffit de taper « risques clients » sur un moteur de recherche pour s'en convaincre – les risques qui sont abordés sont quasiment toujours les risques de solvabilité. Comme si le client commençait à faire courir un risque à l'entreprise soit quand il est défaillant lui-même, soit quand il est insatisfait au point de ne pas vouloir payer ! Ce n'est pas le point de vue que nous adoptons. D'ailleurs les risques de solvabilité sont de type financiers, et traités dans le chapitre correspondant.

Nous proposons, conformément à l'esprit de cet ouvrage, une représentation plus dynamique et plus anticipatrice, où les risques que font courir les clients à l'entreprise s'identifient et se maîtrisent via l'évolution de leur taux de satisfaction. Il y a de multiples façons d'exprimer les taux de satisfaction, et autant d'échelles possibles.

Nous proposons la figure ci-après (Figure 6.4), tout à fait classique et qui suffit en général pour présager des risques que font courir les clients en fonction de leur position. Il n'échappera pas au lecteur que cet histogramme sommaire fait penser à une courbe de Gauss. Ce n'est pas faux en général quand on traite de panels et de segments importants en nombre. En revanche, nous insisterons sur le fait que la « barre » la plus longue n'est pas forcément celle du milieu. Et insisterons encore moins sur l'évidence que la politique de l'entreprise consiste à faire grandir les barres du haut !

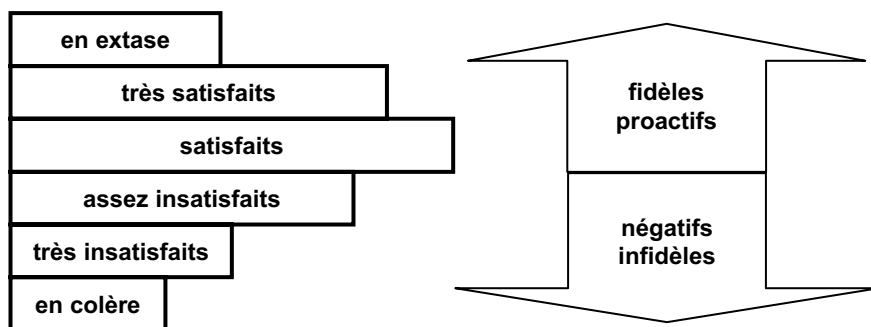


Figure 6.4 La satisfaction des clients

Le client en colère risque de faire très mal, puisqu'il va chercher à nuire à son fournisseur pour se venger du préjudice qu'il a subi. Ceci peut revêtir de nombreuses formes : recours à une association de consommateurs, procès, et autres moyens plus pernecieux (rumeurs...). Dans la famille « clients en

colère », une sous-famille intéressante : celui qui prend la peine d'adresser une réclamation. Une telle lettre est une lettre d'amour, disent certains. En tout cas il peut être intéressant de le voir sous cet angle, on n'a pas tellement l'occasion d'en recevoir...

Le client insatisfait ou très insatisfait n'est pas moins générateur de risques : il est susceptible de quitter le fichier des clients et surtout d'en parler : un client satisfait en parle à 3 personnes, un client insatisfait à 10, dit-on. À tout le moins il va émettre une réclamation, et on sait que le traitement *a posteriori* d'une non-conformité produit est beaucoup plus coûteux que son traitement *a priori* : environ dix fois, estime-t-on. Par le biais de son insatisfaction il va donc générer un risque financier, et d'image.

Le client satisfait estime, tout juste, qu'il en a pour son argent : il perçoit la transaction produit/rémunération comme étant équilibrée. Il ne va pas faire de publicité pour son fournisseur, mais ne va pas lui nuire non plus. Il va juste faire croître, de façon explicite ou pas, son niveau d'exigence vis-à-vis de lui. Le risque qu'il fait courir est donc un risque à terme d'insatisfaction ou d'exigence induite.

Le client très satisfait va en parler. Il aura tendance à être fidèle, mais ne le sera pas forcément. La fidélité se paie, à un prix qui n'est pas très important – en tout état de cause bien moins cher que la récupération d'un client insatisfait. Il générera donc peu de risques, sauf à travers ses exigences implicites qui demanderont à l'entreprise d'y faire face sans défaillir.

Le client « en extase » (traduction imparfaite du terme « *customer delight* », délicat à transposer en français), vit une relation particulière avec son fournisseur. Le produit, à la limite, n'a pas d'importance : qui s'est préoccupé de connaître les caractéristiques d'isolation thermique des foulards d'une certaine marque installée rue du Faubourg Saint-Honoré ? Les risques sont ceux des relations passionnelles : il ne faut pas décevoir, sinon ça fait mal, et le client « en extase » devient instantanément un « client en colère ». Voir donc plus haut.

6.5.3 Le domaine normal

- **Comment le définir : savoir qu'on y est**

Toute entreprise doit connaître le niveau de satisfaction de ses clients ; au minimum via une perception de cette satisfaction – idéalement via la connaissance de son panel de clients sur tout le spectre. La gestion du capital clients n'est pas chose facile, mais comment gérer un capital sans en savoir sa valeur ?

Les entreprises capables de donner une valeur cohérente et exhaustive à leur capital sont rares, voire inexistantes : en général la satisfaction n'est pas mesurée avec la même échelle que les réclamations. Et la fidélité est un paramètre souvent ignoré. Combien d'entreprises ne s'expriment qu'en nombre de clients : c'est comme évaluer un patrimoine en comptant indifféremment les immeubles en pierre de taille et les cabanes de jardin.

Mais ce n'est pas le sujet de cet ouvrage : on se reportera donc à la littérature existante pour aller plus loin et plus profond. Pour définir le domaine normal, nous dirons donc, en supposant le problème précédent connu sinon résolu, que l'entreprise est dans le domaine normal quand la valeur de son capital clients correspond à sa stratégie : en principe au moins constant, mais plutôt en progression en fonction des ambitions qui découlent de sa vision.

• **Comment y rester : méthodes et bonnes pratiques**

Toutes les méthodes d'amélioration du capital client sont bonnes, sinon à prendre, au moins à examiner. Cela va de la conception à l'écoute du marché (CEM) aux enquêtes satisfaction, en passant par la gestion des réclamations, etc.

La mise en forme, via un référentiel de type ISO, de la boîte à outils qu'on se sera constituée aidera à formaliser et à pérenniser les démarches. La certification peut être une étape très utile, en ne perdant pas de vue que pour faire évoluer l'ensemble du spectre des taux de satisfaction/insatisfaction, elle risque d'être insuffisante. En effet, si on veut agir sur le haut de spectre, on devra passer par des méthodes beaucoup plus efficaces, pour favoriser l'innovation, l'écoute des besoins implicites, etc. Tout ceci est disponible sur le marché.

Si on est sensible au mot « excellence » – ou à ce qu'il implique – les méthodes et outils de l'EFQM seront un appui précieux.

6.5.4 Le domaine incidentel

• **Comment le définir : savoir qu'on y est**

On entre dans le domaine incidentel quand le capital client se dégrade de façon nette. Pour cela les indicateurs auront été munis de seuils si possibles chiffrés :

- variation négative du taux de satisfaction ;
- afflux de réclamations ;
- départ de clients ;
- etc.

Si on ne dispose pas d'indicateurs, ce genre d'événement ne tardera pas à se faire sentir autrement : réaction des commerciaux, diminution des prospects, et en fin de compte baisse des commandes. Mais une baisse des commandes qui n'est pas expliquée par un élément conjoncturel externe indique une situation dégradée : on est déjà en chemin vers le domaine accidentel.

- **Comment agir : méthodes et bonnes pratiques**

À court terme, une réaction rapide ciblée est indispensable : donner un coup de fil sans délai à un client mécontent, même sans proposition précise de compensation, est bien plus efficace pour calmer sa colère qu'un rapport de 50 pages parvenu 3 mois après.

Ensuite, vient le moment des plans d'actions, établi selon les règles de l'art, c'est-à-dire en utilisant des outils de résolution de problèmes comme le « 8 D³ ». Comme déjà dit, le prix de la « récupération » d'un client infidèle est 10 fois le prix qu'il aurait fallu payer pour le satisfaire, et 100 fois celui qui l'aurait gardé « en extase ».

On portera un soin particulier aux effets de « contamination » des clients satisfaits par les clients mécontents : un client satisfait peut être un client inquiet, qui prêtera une oreille attentive aux bruits et rumeurs. Un mauvais produit peut dégrader la qualité perçue des autres, même s'ils sont parfaits. L'automobile fourmille de tels exemples. On est là dans le domaine de l'écoute des signaux faibles, de l'anticipation et de la prospective.

6.5.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

Les seuils incidentels sont franchis dans les grandes largeurs, ou bien plusieurs seuils le sont simultanément et de façon durable. Les taux de satisfaction

-
3. La méthode de résolution des problèmes 8 D (de l'anglais 8 « Do ») est une démarche qualité et de progrès continu, qui vise à faire participer les équipes de manière transversale. Les 8 D correspondent à des actions à mettre en oeuvre pour systématiser les résolutions des problèmes et pérenniser les solutions. Les huit actions sont :
 1. initiation de la résolution de problèmes, constitution de l'équipe ;
 2. décrire le problème ;
 3. identifier et mettre en place des actions immédiates ;
 4. déterminer les vraies causes du problème ;
 5. valider les actions correctives définitives et permanentes ;
 6. implémenter les solutions ;
 7. prévenir la réapparition du problème - standardiser ;
 8. féliciter l'équipe.

s'effondrent, les produits sont rebutés par les clients, les réclamations affluent. Une campagne médiatique, orchestrée, pourquoi pas, par des associations de consommateurs, se développe.

La survie de l'entreprise est, à plus ou moins long terme, en cause :

- via son équilibre financier ;
- via la dégradation de l'image et de la confiance ;
- via la démotivation – voire le départ massif – des collaborateurs.

• **Comment agir : méthodes et bonnes pratiques**

Il est particulièrement opportun de passer en organisation de crise, car c'est l'ensemble de l'entreprise qui est en question. Le poste opérationnel revient aux responsables les mieux placés pour l'interface avec les clients. La production est mise à contribution et doit réagir de façon pertinente et rapide.

Si la crise prend un caractère médiatique, la cohérence des actions entre poste de direction et communication est essentielle.

L'après crise devra être l'objet de tous les soins, c'est-à-dire qu'une structure de crise devra rester en place longtemps après le moment où on aura estimé qu'elle est terminée. On peut même espérer une crise rebond positive : il existe quelques exemples, dans le secteur de l'énergie ou de l'agroalimentaire, ou un retour positif a pu être organisé sur l'image. Mais qu'on ne se fasse pas d'illusion : en général, le capital clients sort écorné d'une telle crise, et le retour à la situation antérieure risque d'être long.

6.6 Risques ressources internes et externes

En cohérence avec le modèle EFQM, qui nous sert à structurer ce chapitre, nous avons pris le parti de traiter ici « ressources internes » et « ressources externes », bien que les risques correspondants ne se maîtrisent pas toujours de la même façon. On ne perdra pas de vue le fait que la frontière entre « interne » et « externe » peut être assez mouvante, au gré des tendances à l'externalisation, au retour au cœur de métier, ou bien au contraire à la diversification.

En tout cas une chose est certaine : il faut traiter tous les risques de ce genre. On tirera peut-être de ce qui suit une impression « d'inventaire à la Prévert » : c'est assez exact, car les ressources sont diverses et variées, et ce chapitre traite donc peu ou prou de tout ce qui ne « loge » pas dans les autres. Chaque fois que ce sera nécessaire, nous distinguerons les différents types de ressources ; le

reste du temps, il conviendra de considérer que les méthodes et outils présentés sont communs.

6.6.1 Les ressources d'une entreprise

Les ressources d'une entreprise constituent le support même de son activité. Ce sont en général les données d'entrée des processus support, dont certains peuvent être des processus clés.

La liste des ressources varie bien évidemment en fonction de la taille et de l'activité de l'entreprise considérée. Un inventaire de l'indispensable peut tout de même être dressé. On retrouve donc dans la plupart des entreprises les ressources internes suivantes :

- A, les ressources humaines : elles sont traitées par ailleurs sous le point de vue « santé-sécurité ». Mais sont concernés ici les autres aspects, et en particulier le capital de compétences et de savoir-faire qui est – plus ou moins – caché dans les cerveaux et les mains des collaborateurs.
- B, les technologies : elles sont souvent à l'origine de l'entreprise (brevets...) et lui garantissent une situation d'avantage concurrentiel plus ou moins durable. Leur évolution ou leur renouvellement est alors une condition à la survie.
- C, les infrastructures : ateliers, entrepôts de stockage, bureaux... Elles constituent la partie visible de l'iceberg du patrimoine de l'entreprise. À ce titre elles présentent une vulnérabilité particulière, en particulier vis-à-vis de la malveillance.
- D, le système d'information, ou « informatique » : plus ou moins développé selon la taille et l'activité de l'entreprise, il permet de gérer la documentation, de supporter les réseaux d'information et de communication interne, les logiciels de gestion des clients, de la production, la comptabilité, etc.
- E, les prestataires et fournisseurs : plus ou moins proches, plus ou moins soumis ou dominants, ils sont les partenaires des bons et aussi, il ne faut pas l'oublier, des mauvais jours. Toujours indispensables, parfois mal traités, mais de plus en plus souvent considérés comme de vrais partenaires avec lesquels le chemin parcouru peut – doit – être long.

Cette liste n'est pas exhaustive, et les ressources peuvent être organisées de bien d'autres façons. Par exemple, le système d'information peut être « fourni » par un partenaire externe, les bureaux peuvent être loués, etc.

Dans ce qui suit, les lettres A, B, etc. rappelleront à quel type de ressource on fait allusion ; en l'absence de cette mention, les idées présentées pourront être considérées comme valables pour tous les types... Enfin, c'est que nous espérons...

6.6.2 Les risques qui peuvent affecter les ressources

Les méthodes évoquées dans les autres chapitres pour identifier les risques sont, bien entendu, aussi pertinentes ici. La particularité est que les risques externes ne pourront être valablement identifiés et maîtrisés qu'en collaboration étroite avec les partenaires. Cela suppose donc une grande habitude du travail en commun, et un souci de transparence qui ne va pas toujours de soi.

Pour donner quelques idées générales, les risques liés aux ressources peuvent prendre une des formes suivantes :

- A, défection des compétences des collaborateurs, sous une forme ou une autre :
 - grèves ;
 - départs nombreux et simultanés ;
 - mauvaise anticipation des besoins ;
 - non-transmission des savoirs entre les générations ;
 - évolution technologique majeure entraînant une obsolescence brutale des connaissances existantes...
- B, arrivée d'un brevet dans le domaine public, arrivée d'un brevet extérieur affectant la performance de la technologie en cours, contrefaçon, espionnage industriel...
- C, catastrophe naturelle, incendie, vol, dégradations, endommageant :
 - les structures ;
 - le matériel de production ;
 - les équipements clés...
- D, atteinte à la performance ou à la sécurité du système d'information :
 - informatique : panne de réseau, virus informatique, *hacking*, défaillance de mode commun entre serveurs ;
 - obsolescence des informations et des bases de données ;
 - incendie touchant le matériel de communication, le stockage des documents...

- E, mise en cause de la performance des processus support :
 - disparition d'un prestataire clé ;
 - crise réplique d'une crise survenue chez un prestataire ;
 - non-respects graves et répétitifs du triptyque qualité/coûts/délais...

6.6.3 Le domaine normal

- **Comment le définir : savoir qu'on y est**

Les conditions de production sont optimales et garantissent la conformité du produit. Les technologies de l'entreprise se développent sensiblement de façon à lui donner une longueur d'avance par rapport à ses concurrents. Les moyens de communication et les systèmes d'information sont déployés de façon idéale au sein de l'entreprise. Les biens d'équipement sont en bon état, conformes aux normes de sécurité et de réglementation. Les informations parviennent en temps et en heure aux collaborateurs concernés, tous et rien qu'à eux. Les fournisseurs livrent à l'entreprise, en temps et en heure, des produits conformes au cahier des charges. Ils sont prospères et heureux de la collaboration avec l'entreprise.

Bref, aucun nuage, réel ou fictif, à l'horizon. Si on a eu la sagesse de mettre en place un tableau de bord qui prend en compte les ressources, ces indicateurs sont au vert.

- **Comment y rester : méthodes et bonnes pratiques**

Les ressources ne sont pas, en général, le souci immédiat des dirigeants : « l'intendance suivra » disait un (grand) général célèbre.

La bonne pratique de base en matière de ressources est la redondance (*cf.* chapitre 3.3). On double les équipements, on veille à ce que les compétences disponibles excèdent les besoins du moment, on sauvegarde les données, on dispose d'un fournisseur alternatif, etc.

Tout ceci a évidemment un coût. D'où la nécessité pour la direction d'élaborer et de déployer une politique en matière de redondance : il est essentiel que les décideurs de tous niveaux sachent clairement quel niveau de redondance est requis (et donc son coût accepté) et quel niveau n'est pas recherché (avec les risques induits).

Il est donc de bon augure de mettre en place un dispositif de suivi des ressources. Le minimum, comme on vient de le dire, est de les prendre en

compte dans les moyens de pilotage à disposition du management. Ces moyens de suivi pourront être assez décentralisés, afin de ne pas noyer les dirigeants sous des informations qui n'évoluent pas rapidement, et qui comme on l'a dit, ne les passionnent pas. Mais il faudra s'assurer que les dispositifs de remontée d'information et d'alerte fonctionnent.

L'inventaire des processus support, et leur description, est naturellement une saine initiative. D'autant plus que le déploiement d'une telle opération peut être progressif, en se limitant, pour commencer, aux processus clés de l'entreprise.

Il est aussi possible de franchir le pas et de mettre en place un système global de management qualité, pouvant déboucher sur une certification de type ISO 9000 – ou tout autre référentiel du genre.

Le pas suivant – un grand pas ! – consiste à lancer une démarche qualité totale (TQM) qui garantira que les ressources sont l'objet de tous les soins, au même titre que les autres parties prenantes.

Plus spécifiquement, on peut citer quelques bonnes pratiques :

- A, gestion anticipée des emplois et des compétences (entretiens annuels d'évaluation, plans de formation, fiches de fonction...) et plus avancé : mise en place d'une véritable politique de management des connaissances (« *knowledge management* »).
- B, veille technologique, audits de sécurité sur les informations, données et méthodes stratégiques, promotion de la recherche et de l'innovation... Une autre orientation peut être la promotion de labels, afin de créer un avantage concurrentiel durable... mais long à mettre en œuvre et coûteux à maintenir.
- C, programmes de maintenance préventive, voire prédictive (audits externes, visites de pompiers, visites de sécurité, opérations « 5 S »...).
- D, mise en place de sites de « *back-up* » (mise en place de mots de passe, d'antivirus et de pare-feu), expertises externes, exercices de repli... et plus globalement, deux méthodes classiques : EBIOS (Expression des besoins et Identification des Objectifs de Sécurité) et MEHARI (MEthode Harmonisée d'Analyse de Sécurité). À travers l'analyse de risques trois paramètres sont à prendre en compte : la confidentialité, l'intégrité et la disponibilité de l'information.
- E, partenariats et contrats à long terme, analyses communes des non-conformités, formations communes ou croisées, audits externes, internes, mixtes, croisés, démarches de suivi et d'accompagnement des fournisseurs de type AQF (Assurance Qualité Fournisseur).

6.6.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

On entre dans le domaine incidentel lorsque certaines ressources ne sont plus totalement opérationnelles, ce qui entraîne la défaillance des processus support, et que cette défaillance peut avoir, immédiatement ou à terme, des effets sur la performance des processus clé opérationnels et/ou de pilotage.

C'est donc la détection des signaux faibles qui est essentielle, d'autant plus que, on l'a vu, la surveillance des ressources est généralement assez largement déléguée. On veillera donc à ce que les indicateurs soient assez précis pour générer des informations sur leurs tendances.

A priori, sauf exception (comme par exemple pour les approvisionnements quand on pratique le flux tendu) la défaillance locale et temporaire d'une ressource n'est pas susceptible à elle seule d'entraîner l'entreprise vers une situation accidentelle. En revanche, deux ou plus défaillances mineures peuvent justifier le passage en situation de veille. Pour donner un exemple, une panne du système informatique peut ne pas être dramatique, mais si l'un des deux techniciens compétents est en vacances et que l'autre tombe malade... C'est donc un monitoring global qui doit être rendu possible, et ceci nécessite un niveau de synthèse suffisant.

- **Comment agir : méthodes et bonnes pratiques**

Les actions correctives nécessaires doivent être mises en œuvre rapidement et adaptées à la situation.

Si on a eu la sagesse de suivre le conseil du paragraphe précédent, on dispose de moyens permettant la redondance : l'appel à ces moyens est évidemment le premier acte à envisager.

Si ce n'est pas le cas, l'appel à d'autres ressources externes (moyens de secours, personnel intérimaire) est une solution qui génère des risques supplémentaires, peut-être d'une autre nature. La veille active sur leur performance est indispensable tout le temps qu'elles sont mises en œuvre. Cette menace peut être une opportunité si on arrive à valoriser ces moyens externes différents (autres cultures, autres techniques) mais il s'agit là d'un cas sans doute assez rare.

À court terme également, un dispositif plus ou moins temporaire doit être mis en place pour surveiller de plus près les processus qui ont été défaillants. Les interactions qui auront fait dégénérer la situation par superposition de

défaillances ponctuelles feront également l'objet d'un retour d'expérience et de plans d'actions.

En temps différé, une défaillance imputable à une mauvaise conception majeure du processus support lui-même doit logiquement entraîner la révision du processus... ou le remplacement de son responsable. Mais il vaut mieux prévenir que guérir : l'utilisation de cartes de contrôle permet de suivre l'évolution d'un processus donné. La recherche de la ou des causes profondes (grâce à une méthode de résolution de problème de type 8 D ou QRQC, *Quick Response Quality Control*) sera à l'origine d'un plan d'action permettant de revenir au mode de fonctionnement normal.

6.6.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

On est dans le domaine accidentel lorsque l'organisme n'est plus en mesure de réaliser le produit selon le processus de réalisation défini, à cause de la défaillance d'une des ressources mises en jeu.

Un incendie, une avarie bloquante provoquant l'arrêt brutal d'une machine, la démission d'un acteur clé d'un projet, un virus bloquant le système informatique... Autant d'événements qui empêchent le déroulement normal de l'activité de l'entreprise.

Ce sont donc les indicateurs des processus opérationnels qui passent au rouge. Le domaine se définit donc via celui des risques processus : par le franchissement des seuils préalablement définis.

- **Comment agir : méthodes et bonnes pratiques**

En situation accidentelle, le recours aux ressources externes est quasi inéluctable, avec les risques évoqués dans le paragraphe précédent. L'existence d'un plan d'urgence pour faire face aux risques majeurs est évidemment un gage de survie. À défaut, les mesures salvatrices seront prises dans le cadre de l'équipe de crise, et surtout pas de façon désordonnée et non concertée.

En ce qui concerne la composition de cette équipe, on veillera à ce que le poste opérationnel soit tenu par un collaborateur ayant des qualités relationnelles et commerciales (vente et achat) confirmées. Des compétences juridiques très larges devront sans doute être mobilisées.

L'appel à des ressources d'urgence a un coût très important, souvent immédiat (voire préalable à l'intervention !), quelquefois différé. Cela induit donc des

risques financiers dont il convient de tenir compte dès l'appel aux dites ressources.

Dans l'organisation type de crise, c'est le poste « moyens » qui est le plus important, puisqu'il se confond avec le poste opérationnel, qu'il n'est d'ailleurs pas forcément nécessaire de créer.

Comme toujours, en sortie de crise, un retour d'expérience musclé sera nécessaire, et son suivi une affaire de longue haleine. Un retour vers les parties prenantes (clients, fournisseurs) avec une mise en valeur des coopérations qui ont permis de sauver la mise, sera générateur de confiance. En revanche, ces partenaires n'accepteront plus le renouvellement d'une telle situation, surtout s'ils en ont pâti eux-mêmes : en fin de compte, comme le signifiait le Général, il n'est pas imaginable que l'intendance ne suive pas...

6.7 Risques juridiques

6.7.1 La loi et l'entreprise

« Nul n'est censé ignorer la loi »... Cette phrase clé du droit s'applique à l'entreprise, comme au citoyen, mais pourrait être rédigée sous une forme un tantinet plus sévère : « Non seulement l'entreprise n'est pas censée ignorer la loi, mais en tout état de cause elle a le devoir de l'appliquer ».

Les risques juridiques se définissent donc par une cible, l'entreprise, et une menace : les conséquences que peut avoir le non-respect de la loi. Nous engloberons dans le terme « la loi » tout le *corpus* réglementaire existant, ce qui simplifie l'exposé mais complique de façon exponentielle la tâche des dirigeants !

6.7.2 Les risques juridiques

L'entreprise est soumise à des risques juridiques dès lors que sa responsabilité civile ou pénale est engagée. Rappelons les définitions, prises sur un site Internet référencé en bibliographie :

« La responsabilité civile est « l'ensemble des règles juridiques qui permettent à la victime d'un fait dommageable d'obtenir réparation du préjudice qu'elle a subi ». Le dommage peut être matériel, corporel ou d'ordre moral (diffamation, harcèlement...). Si on ne peut arriver à la situation antérieure, la réparation du dommage est pécuniaire. Que le dommage soit issu d'une inexécution d'un contrat (responsabilité contractuelle) ou non (responsabilité délictuelle), la responsabilité civile est engagée sensiblement de la même manière.

Les assurances couvrent la responsabilité civile, c'est-à-dire qu'elles prennent en charge la réparation du préjudice.

La responsabilité pénale suppose une faute pénale, c'est-à-dire une infraction à une règle prescrite par une réglementation : Code pénal, loi informatique et liberté, Code du travail, Code de la Sécurité sociale... L'infraction est sanctionnée par une amende, par un travail d'intérêt général ou par l'emprisonnement, proportionnés à la faute.

Les assurances ne couvrent pas la responsabilité pénale puisque la loi interdit d'assurer les conséquences pécuniaires (les amendes) de la responsabilité pénale. »

Une façon, qui en vaut bien une autre, de dresser la liste des risques juridiques consiste à les classer selon les parties prenantes de l'entreprise :

- Le personnel : non-respect du Code du travail, discrimination à l'embauche, licenciements, exploitation des données personnelles sans accord des personnes concernées...
- Les clients : non-respect des réglementations vis-à-vis du produit fabriqué, des contrats de vente, des clauses de confidentialité, contrefaçon...
- Les fournisseurs : ruptures de contrats, mauvaise gestion et utilisation de logiciels, de bases de données, de marques, de brevets...
- Les actionnaires : litiges juridiques opposant les dirigeants de l'entreprise aux actionnaires...
- La collectivité : pollutions, atteinte à la sécurité publique, corruption, lobbying un peu trop « poussé »...

6.7.3 Le domaine normal

• Comment le définir

La définition du domaine normal est simplissime : c'est lorsque l'entreprise respecte les lois et règlements qui s'appliquent à elle. Nous dirons même : l'entreprise est au centre du domaine normal quand elle respecte toutes les lois et règlements, en toutes circonstances.

• Comment y rester : méthodes et bonnes pratiques

Il ne faut pas se faire d'illusion : on n'est jamais au centre du domaine normal. La politique de certaines organisations serait même plutôt d'être toujours au bord, afin de disposer d'une marge de manœuvre la plus large possible.

La meilleure façon d'y rester consiste donc à s'interdire une telle politique : il est plus facile d'éviter de mordre la ligne blanche si on est bien au centre de sa voie de circulation. C'est une politique qui peut s'écrire (*cf.* le chapitre sur les risques éthiques) mais qui se déploie surtout par l'attitude des dirigeants.

Les différences entre les deux types de responsabilité ne sont pas minces et ont des conséquences immédiates sur la façon dont on va maîtriser les risques correspondants. Dans un cas, on peut recourir à l'assurance – toujours trop chère avant l'événement – dans l'autre cas c'est exclu.

Cela ne suffit évidemment pas : l'évolution constante des textes, leur complexité grandissante, l'empilement croissant des niveaux qui produisent les référentiels (pas seulement Bruxelles !) rend la veille législative et réglementaire indispensable. Dans les grandes entreprises, on s'appuiera donc sur des collaborateurs payés pour cela. Pour les plus petites ce sera une des tâches du dirigeant (une de plus !), plus ou moins appuyé par des soutiens externes (comptable, conseiller juridique, organismes professionnels ou consulaires).

Tout ceci sera complété par une boucle de contrôle, destinée à identifier et corriger les petits écarts par rapport au point central. On peut les considérer comme des non-conformités des processus de management de l'entreprise, et donc les traiter comme on traite les non-conformités des processus de production, à l'aide d'un système de contrôle qualité, pouvant aller jusqu'à la certification. On ne cachera pas que ce n'est pas un domaine, tant s'en faut, où une telle démarche est facile à déployer, compte tenu de la culture des collaborateurs impliqués. En revanche, la motivation sera au rendez-vous, pour des raisons évidentes.

6.7.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

On entre dans le domaine incidentel dès lors que la responsabilité civile ou pénale de l'entreprise, telles qu'elles ont été définies plus haut, se trouvent engagées de façon concrète, sous forme de procès, plainte, recours devant telle ou telle instance d'arbitrage, etc. Ce sont donc des signaux binaires, simples à percevoir, qui provoquent la réaction des dirigeants.

Dans les très grandes entreprises, un autre type de risques ne doit pas être oublié : une « inflammation » en provenance d'une partie éloignée de l'entreprise, et non perçue à temps par le niveau de synthèse adéquat.

- **Comment agir : méthodes et bonnes pratiques**

Évidemment, il n'est pas imaginable de préconiser ici une autre conduite que la réaction immédiate, la réparation des préjudices provoqués et le paiement des dettes (amendes, indemnités) correspondantes. « Qui paie ses dettes s'enrichit » : à défaut d'améliorer la trésorerie, c'est au moins le capital de confiance des clients et des autres parties prenantes qui sera conservé, ou au pire dégradé dans une mesure demeurant acceptable.

En réalité, c'est un peu plus compliqué, car il faut faire la distinction entre responsabilité collective – et donc assumée dans notre cas par l'entreprise – et responsabilité individuelle. La limite est assez floue et évolue tout le temps sous l'influence des événements, et par l'évolution de la jurisprudence. Sans entrer dans des détails qui ne sont pas de notre compétence, il semble clair qu'on cherche désormais plutôt à faire payer le chef de gare que le lampiste – métier ayant d'ailleurs tendance à disparaître – voire le Président de la société de chemins de fer. Mais il semble bien aussi que le lampiste, quand il sera effectivement responsable, paiera de sa poche et que l'entreprise limitera son soutien plus ou moins moral – aux deux sens de l'expression...

Il y a même des cas où l'infraction génère des profits ! Voir le (mauvais ?) exemple des centres commerciaux qui paient régulièrement des amendes conséquentes parce qu'ils ouvrent leurs portes le dimanche.

Un retour d'expérience est de rigueur, avec le plan d'action adapté. Un plan de communication peut s'avérer opportun, une fois les dettes réglées, et à condition – qui pourrait en douter – que les messages proposés soient sincères.

Un élément dont l'influence est déterminante est l'image que l'entreprise a auprès de ses clients et autres parties prenantes. Si la confiance est là, certes elle ne sortira pas grandie d'une affaire judiciaire, mais elle sortira vivante. Ceci ne se décide pas, et ne s'organise pas sur le moment : c'est un facteur de succès – presque un facteur clé – qui est ou qui n'est pas au moment de l'affaire.

6.7.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

On entre dans le domaine accidentel lorsque la survie de l'entreprise est en jeu. Elle peut l'être soit par les conséquences financières de l'affaire, soit plus vraisemblablement par ses retombées sur la confiance des clients et des autres parties prenantes. Ce qui à terme revient d'ailleurs au même.

- **Comment agir : méthodes et bonnes pratiques**

La mise en place d'une organisation de crise s'impose, et rapidement. Le poste opérationnel sera plutôt confié aux spécialistes du droit, mais ce n'est pas forcément la meilleure solution : ils seront peut-être mieux au poste des contrôles. La cohérence de l'action judiciaire, médiatique et vis-à-vis des clients pourra y gagner.

Contrairement à certains cas de situation incidentelle, où on peut justifier de se contenter de plaider la forme, il ne nous semble pas judicieux d'imaginer, en situation accidentelle, qu'on puisse en faire autant. Certes, on peut gagner à court terme, mais on induit des risques différés de crise rebond qui peuvent faire beaucoup plus mal.

La sortie de crise est bien entendu importante à gérer ; c'est comme cela qu'on commencera à restaurer la confiance. Le retour d'expérience, comme toujours, permettra d'éviter le renouvellement d'une nouvelle crise (plus ou moins) semblable.

6.8 Risques environnementaux

6.8.1 Qu'est-ce qu'un risque environnemental ?

D'après la norme NF EN ISO 14001:2004 portant sur « le système de management environnemental », un impact environnemental est caractérisé par toute « modification de l'environnement négative ou bénéfique, résultant totalement ou partiellement des aspects environnementaux d'un organisme. »

Pour rester cohérents avec notre définition des risques, on parlera donc de risque environnemental s'il y a un impact **négatif** sur l'environnement.

6.8.2 Les risques environnementaux

La sauvegarde de l'espèce est, de notre égoïste point de vue d'humains, l'enjeu majeur de la sauvegarde de l'environnement. Mais « laisser la planète dans l'état où nous l'avons trouvée » n'est un objectif mesurable que si quelqu'un est (encore) là pour le mesurer... C'est pourtant l'ensemble des menaces et toutes les cibles qui doivent être prises en compte, ne serait-ce que qu'au titre de principe de précaution !

Le premier risque environnemental auquel on pense est le risque de pollution. Les causes peuvent en être diverses :

- rejets gazeux toxiques ;
- déversements de produits liquides dangereux dans les rivières ;

- déchetteries sauvages ;
- émissions radioactives ;
- métaux lourds...

On peut prendre pour exemple l'intoxication au plomb. Le saturnisme affecte notamment les systèmes hématologique, neurologique et rénal. Ce type d'intoxication peut provenir de plusieurs sources :

- la pollution de l'eau (dégradation du plomb présent dans les canalisations, rejets industriels plus ou moins contrôlés...) ;
- la pollution de l'air (émission de plomb dans l'atmosphère émanant de l'essence des voitures) ;
- la pollution des aliments due aux retombées de la pollution atmosphérique et à la contamination des sols, mais aussi (autrefois) l'utilisation de vaisselle en plomb ;
- et finalement – curiosité – le plomb est le métal qui reste en fin d'évolution d'une chaîne de désintégration radioactive.

Mais il existe bien d'autres sortes de pollutions, plus ou moins pernicieuses, et dont les effets ne sont pas forcément perceptibles à court terme :

- agressions sonores ;
- pollutions visuelles ;
- pesticides et (?) OGM ;
- émissions de télé-réalité...

Au-delà des risques de pollution, on ne doit pas non plus omettre toutes les autres agressions à l'environnement : prélèvement de matières premières, déforestations, destruction des récifs coralliens, etc., et ceci même si on n'a pas le sentiment qu'un impact négatif, direct ou indirect, soit à escompter sur le bien-être de notre espèce... et de celles qui vont nous survivre et nous succéder. Les scorpions résistent à une explosion nucléaire : leur a-t-on demandé ce qui est le plus important pour eux ?

6.8.3 Le domaine normal

• Comment le définir : savoir qu'on y est

Vis-à-vis de son impact sur l'environnement, l'entreprise doit se maintenir dans une des deux situations suivantes, à l'exclusion de toute autre :

- ou bien un impact est prévu et accepté, et ceci est assorti de seuils ;

— ou bien il n'est rien prévu, et en ce cas l'impact doit être strictement nul.

Le domaine normal est donc défini ainsi. Dans le cas où un impact est accepté, il peut même faire l'objet d'autorisations. C'est le cas des installations nucléaires par exemple, qui font l'objet d'autorisations de rejets officielles. En l'absence de telles contraintes « administratives », il est du devoir de l'entreprise d'exprimer les seuils qui lui semblent acceptables, et d'en tenir informées toutes les parties prenantes.

En l'absence de seuils formalisés, la difficulté est bien entendu de garantir qu'un éventuel impact sera détecté ; c'est bien souvent l'extérieur qui émettra le premier signal. Mais si l'entreprise sait le faire, cela sera porté à son crédit. Or dans ce domaine plus que tout autre, la confiance que la collectivité accorde à l'entreprise sera déterminante pour sa tolérance à la pollution qu'elle subit. Les exemples sont nombreux, on n'évoquera que l'Erika et le comportement de TOTAL dans les jours qui ont suivi le naufrage.

• **Comment y rester : méthodes et bonnes pratiques**

Même en présence de seuils voire d'autorisations, c'est avant tout une attitude de type « zéro rejet » qui doit être promue au sein de l'entreprise.

Cette attitude sera d'abord perceptible par des gestes simples : tri sélectif, récupération et recyclage des déchets. Cela commencera par la chasse aux gaspillages : éteindre les lumières, ne pas abuser du chauffage et de la climatisation, adopter une conduite souple (gage par ailleurs de bien d'autres bénéfices), réduire les consommations de toutes sortes. Il sera difficile de résister aux critiques faciles sur les économies de bout de chandelle, d'autant plus que pour beaucoup de collaborateurs la consommation de matières et d'énergie est le signe même de leur activité. Mais il s'agit là de promouvoir une attitude, et la communication est donc délicate.

Des méthodes simples comme les 5 S pourront être utilisées.

Il va de soi qu'une exigence absolue est de se conformer aux règles et à la législation en vigueur. Cela suppose une veille réglementaire minimale, qui dans les cas les plus simples peut être assurée par des organismes consulaires ou publics (DRIRE en particulier). Il s'agit d'une tâche complexe, car les textes sont nombreux, redondants, et ne font pas souvent l'objet d'une communication prioritaire vers les chefs d'entreprise : « tu ne pollueras point » ne fait pas partie des commandements qui sont cités au premier abord. Ceci rend donc quasi indispensable la désignation au sein de l'entreprise d'un responsable de cette veille, avec le positionnement hiérarchique et les moyens qui conviennent.

Bien entendu, on ne peut que préconiser d'aller plus loin, en mettant en place un véritable système de contrôle et d'amélioration continue. L'outil existe, c'est la norme ISO 14001:2004, portant sur les systèmes de management environnementaux. La mise en place d'un tel système conduit à se conformer naturellement aux indications qui précèdent, et la certification viendra attester de cette conformité.

Si l'entreprise est déjà engagée dans une démarche qualité, il conviendra de se poser la question de « passer » directement à un système plus intégré, comme la démarche QSE.

6.8.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

On sort du domaine normal pour entrer dans le domaine incidentel, quand un de ces deux événements se produit :

- détection du franchissement d'un (au moins) des seuils prédéfinis ;
- rejet dans l'environnement non prévu.

A priori (et au risque de choquer les esprits les plus exigeants), nous dirons que l'entrée dans le domaine incidentel ne se traduit pas par des conséquences mesurables sur l'environnement. Sinon, dans le cas de dépassement de seuil, cela signifierait que ce seuil est fixé vraiment trop haut ! Dans le cas où l'événement ne correspond pas au franchissement d'un seuil, un impact effectif et perceptible sur l'environnement implique qu'il faut alors considérer qu'on est directement entré dans le domaine accidentel.

- **Comment agir : méthodes et bonnes pratiques**

La première chose à faire est de mettre fin à la pollution, pour prendre l'exemple d'une pollution. Les notions de coût passent lors au second plan. Il se peut que les moyens normaux de l'entreprise, en hommes, en matériel et en argent soient insuffisants, mais dans tous les cas la collectivité ne pardonnera pas d'avoir ergoté sur les moyens.

Elle pardonnera encore moins à l'entreprise d'avoir gardé le silence ou, pire, d'avoir menti. La deuxième série de gestes est donc du domaine de la communication : vers l'extérieur, les organismes d'État, les parties prenantes (y compris les clients, qui pourront être selon la situation les meilleurs des alliés ou les pires des adversaires) et bien entendu les médias. Il n'est pas si

difficile que cela de communiquer dans ce genre de contexte. Si l'entreprise a su générer un capital de confiance suffisant, on recevra sans malveillance excessive les informations qu'elle va communiquer : faute avouée est à demi pardonnée... En tout état de cause, faute non avouée est sanctionnée au carré !

Ensuite, si une dérive du processus de gestion des impacts environnementaux s'est produite, le responsable environnement devra mettre en place les actions curatives puis correctives permettant de revenir au fonctionnement normal, et surtout éviter le renouvellement de l'événement. Le plan d'action correctif s'accompagnera souvent d'un renforcement de la formation du personnel sur la gestion des déchets et des autres impacts environnementaux.

6.8.5 Le domaine accidentel

- **Comment le définir : savoir qu'on y est**

On entre dans le domaine accidentel dès que :

- plusieurs seuils ont été franchis simultanément ;
- un seuil a été franchi au point qu'il devient dérisoire ;
- l'impact sur l'environnement est clairement perceptible.

En résumé, on est en phase accidentelle dès que le système – ou son absence – de contrôle des impacts de l'entreprise sur l'environnement s'avère gravement défaillant.

- **Comment agir : méthodes et bonnes pratiques**

Si on faisait un sondage sur le trottoir, il est probable que les deux accidents les plus souvent cités seraient le naufrage de l'Erika et l'explosion de Tchernobyl. Sans entrer dans une analyse comparée et exhaustive des deux événements, ils sont assez différents. Dans le premier cas, l'impact a été immédiat, constatable et probablement intégralement réparable à plus ou moins long terme. Dans l'autre cas, les retombées ont été différées, la mesure de l'impact ne fait pas l'objet d'un consensus, tant s'en faut, et la crise s'est doublée d'une polémique médiatique franco-française sur « le nuage qui s'est arrêté aux frontières ». Elle met en cause beaucoup plus qu'une entreprise, ou même une industrie, aussi importante que soit celle du pétrole ou du nucléaire. Sans parler de l'effet sur l'effondrement du bloc soviétique.

Si un tel événement se produit, l'équipe de crise s'appuiera naturellement sur l'existence d'un plan d'urgence, qui sera évidemment de la plus grande utilité.

Ce plan peut être spécifique et obligatoire, en particulier pour les entreprises soumises à une réglementation comme celle dite « de Seveso ». Il peut aussi émaner des pouvoirs publics (ORSEC, etc.).

L'organisation à adopter est, typiquement, l'organisation de crise telle qu'elle a été décrite. Les deux postes de commandement les plus importants sont celui de direction et celui des contrôles : en effet, pas de communication de qualité sans fiabilité des informations transmises.

Comme toujours, la mise en place du plan de crise, puis la sortie de crise, feront l'objet de retour d'expérience. Afin d'éviter une éventuelle « crise rebond » les mesures de l'impact sur l'environnement seront prolongées bien longtemps après la sortie de crise, et feront l'objet d'une communication légère mais positive et bien ciblée. Ceci contribuera à restaurer le crédit de confiance de l'entreprise, qui aura forcément été peu ou prou entamé.

Dans certains cas il peut même en sortir augmenté : on observera en particulier comment certaines grandes entreprises (Hydro Québec lors du « grand gel », EDF lors de la tempête de 1999, la RATP après certaines grèves...) savent « positiver » une sortie de crise... Pas d'optimisme irraisonné cependant : on ne prête qu'aux riches !

6.9 Risques éthiques

6.9.1 Qu'est-ce que l'éthique ?

« L'éthique est la théorie de l'action que l'homme doit mener pour bien conduire sa vie et parvenir au bonheur ».

On associe souvent l'éthique à la morale. Rappelons que la morale, d'après le Robert, est une « science du bien et du mal qui soumet la conduite de l'homme à des règles en vue du bien ».

Il est hors de propos ici de partir dans des considérations sur le Bien et le Mal... À supposer, ce qui est bien sûr totalement faux, que nous soyons (moralement...) autorisés à le faire, cela découlerait d'une ambition que nous nous refusons même de qualifier.

Nous nous contenterons donc d'une approche s'appuyant sur la pyramide dite « de Maslow », qui hiérarchise les besoins de l'être humain, depuis ceux qui sont les plus fondamentaux (liés à sa survie même) jusqu'à ceux qui lui sont nécessaires pour se réaliser complètement (Figure 6.5).

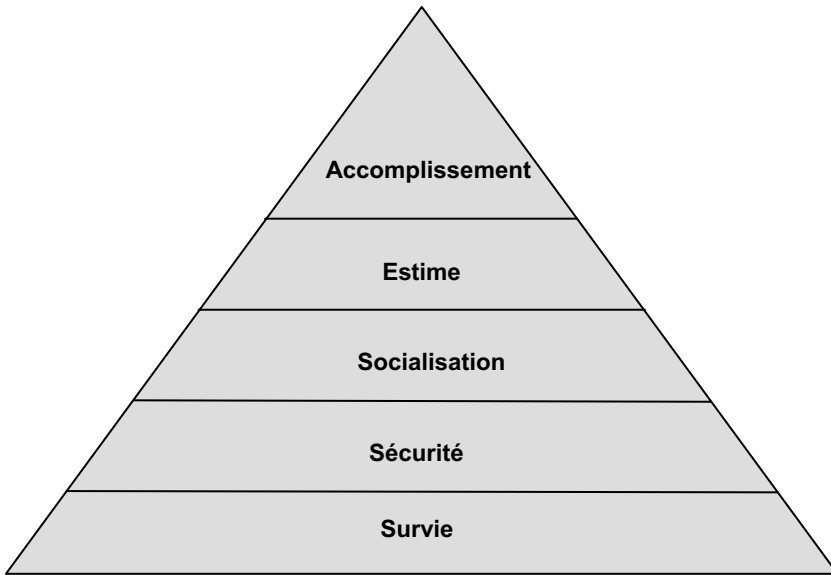


Figure 6.5 La pyramide de Maslow

Ce modèle est largement utilisé dans bien des domaines, et fonctionne correctement avec des populations de tous types. Il en existe plusieurs représentations, nous choisissons la plus simple, décrivant cinq niveaux.

Les cinq niveaux de la pyramide permettent de classer d'une façon assez agréable les différentes de risques perçus par l'homme, et facilitent la mise au clair des actions de maîtrise qui en découlent.

L'idée – certainement discutable – qui nous guide dans ce qui suit est la suivante : « être éthique » consiste à ne pas nuire à la satisfaction de ces besoins, et « avoir une démarche éthique » conduit à favoriser la recherche de la satisfaction des besoins vers les niveaux supérieurs.

6.9.2 Les risques éthiques et les besoins humains

- **Risques sur la survie : se nourrir, se reproduire**

Avant de vivre, il faut survivre, c'est le lot de la majeure partie de l'humanité et de la totalité du règne animal, à l'exception des toutous de compagnie (quoique...). Les êtres humains ont huit besoins physiologiques fondamentaux : les besoins d'oxygène, de liquides, de nourriture, de maintien de la

température corporelle, d'élimination, de logement, de repos et de rapports sexuels. À ce niveau de la pyramide, la conscience de l'Homme n'entre pas compte, il est guidé par ses besoins primitifs. Le besoin de survie pousse à agir d'instinct et pour parvenir à ses fins l'individu ou le groupe est capable de descendre très bas dans l'estime de soi. À ce niveau, il est encore difficile de parler d'éthique, mais le minimum qu'on doit contribuer à assurer est le respect.

• **Risques sur la sécurité : garantir l'intégrité de la personne**

La sécurité comporte une partie visible, la sécurité physique, et une autre qui ne l'est pas, la sécurité psychologique :

- Sécurité physique : elle implique la réduction ou l'élimination des dangers qui menacent le corps ou la vie de la personne. Le danger peut être une maladie, un accident un risque ou l'exposition à un environnement dangereux.
- Sécurité psychologique : une personne doit savoir ce qu'elle peut attendre des autres, y compris des membres de sa famille et des professionnels, ainsi que des interventions, des expériences nouvelles et des conditions de son environnement.

La sécurité est assurée quand aucun de ces dangers n'est à redouter, et que par conséquent on peut avoir l'esprit libre. La sécurité est également un droit (Déclaration universelle des droits de l'homme).

On retrouve ainsi la notion de sécurité dans beaucoup de domaines tels que :

- sécurité économique : revenu minimum garanti ;
- sécurité sanitaire : protection contre la maladie et les infections ;
- sécurité politique : protection des droits de l'homme ;
- sécurité environnementale : eau potable, pureté de l'air...

On se rend compte que sécurité et éthique sont deux termes dépendant l'un de l'autre. Si on ne se fixe pas de règles à respecter d'un point de vue éthique ou moral, cela rend difficile la mise en place de codes de sécurité. Prenons l'exemple du Code de la route ; il repose sur des notions de sécurité. Les voitures doivent s'arrêter au feu rouge et laisser passer les piétons. Pour garantir sa sécurité un piéton ne doit pas traverser en dehors de passages cloutés (qui d'ailleurs ne le sont plus depuis longtemps)... Autant de règles dont l'utilité est évidente mais qui sont régulièrement enfreintes. Qui n'a jamais traversé la route en dehors des passages cloutés, que cela soit sous prétexte de gagner du temps ou simplement par désinvolture ? Or, déroger à

ces règles reflète un manque d'éthique, qui peut se révéler très dangereux pour autrui, pour son entourage et finalement pour soi.

Inversement, il est difficile d'instaurer des règles éthiques lorsque la sécurité n'est pas assurée. Au sein d'un organisme en difficulté économique, quand la sécurité de l'emploi est menacée, l'éthique risque d'être mise au second plan.

- **Risques sur la socialisation : garantir l'appartenance de la personne**

Après les besoins physiologiques et les besoins de sécurité viennent les besoins d'amour et d'appartenance.

Un individu ressent le besoin d'être aimé par les membres de sa famille et d'être acceptée par ses pairs et par les membres de sa communauté. Habituellement, le désir de combler ces besoins survient lorsque les besoins physiologiques et les besoins de sécurité sont satisfaits, car ce n'est que lorsqu'une personne se sent en sécurité qu'elle a le temps et la force de rechercher l'amour et l'appartenance, et de partager cet amour avec d'autres.

La vie collective est une condition à la survie, mais est aussi liée à la sécurité. Au delà, l'appartenance à un groupe améliore l'efficacité : le nombre d'idées d'un groupe peut être sensiblement supérieur à la somme des idées des individus. Enfin, le sentiment d'appartenance à un ensemble dont l'image est positive est positif pour l'individu.

Les modes et les tendances évoluent : on ne fait guère plus marcher une équipe sur des braises, et on la fait encore moins souvent sauter d'un pont au bout d'un élastique. Il n'en demeure pas moins que le bien-être qu'un individu éprouve à appartenir à un groupe est une notion qu'on ne doit pas sous-estimer, non plus que les dangers qu'une telle appartenance peut générer si elle est exacerbée par des manipulateurs ou des marchands : les pages de l'Histoire (et des matches de football) en sont pleines.

Dans le premier cas, on concourt à l'éthique, dans l'autre on y est évidemment contraire.

- **Risques sur l'estime : préserver l'opinion perçue par l'individu sur son environnement et sur lui-même**

C'est le besoin d'être respecté, de se respecter soi-même et de respecter les autres. Besoin de s'occuper pour être reconnu, avoir une activité valorisante qu'elle soit dans le domaine du travail ou dans celui des loisirs. Il s'agit en particulier du besoin de se réaliser, de se valoriser (à ses propres yeux et aux yeux des autres) à travers une occupation.

Le besoin d'estime de soi est rattaché au désir de force, de réussite, de mérite, de maîtrise et de compétence, de confiance en soi face aux autres, d'indépendance et de liberté. Une personne a aussi besoin d'être reconnue et appréciée des autres.

Lorsque ces deux besoins sont satisfaits, la personne a confiance en elle et se sent utile ; s'ils ne sont pas satisfaits, la personne peut se sentir faible et inférieure. On a aussi besoin de faire des projets, d'avoir des objectifs, des opinions, des convictions, de pouvoir exprimer ses idées. Attention : certains auteurs avancent que le snobisme entre dans cette catégorie...

En tout cas, maîtriser les risques de non-respect, de soi ou des autres, est une valeur qui à l'évidence est tout à fait cohérente avec la recherche d'un comportement éthique.

• **Risques sur l'accomplissement : favoriser la quête du bien-être**

On dit aussi parfois : besoins d'actualisation de soi. Ils se trouvent au sommet de la hiérarchie des besoins humains de Maslow. Lorsqu'une personne a satisfait tous les besoins des niveaux précédents, c'est dans l'actualisation de soi qu'elle parvient à réaliser pleinement son potentiel.

L'actualisation de soi se définit par de multiples caractéristiques :

- résout ses propres problèmes ;
- aide les autres à résoudre les problèmes ;
- accepte les conseils des autres ;
- témoigne un grand intérêt pour le travail et les questions sociales ;
- possède de bonnes aptitudes à la communication, tant pour écouter que pour communiquer ;
- contrôle son stress et aide les autres à contrôler leur stress ;
- apprécie son intimité ;
- recherche de nouvelles expériences et de nouvelles connaissances ;
- prévoit les problèmes et les réussites ;
- s'accepte.

La personne qui s'est actualisée a l'esprit mûr et sa personnalité est multidimensionnelle ; elle est souvent capable d'assumer, de mener à terme des tâches multiples et elle tire satisfaction du travail bien fait.

La façon dont une personne réussit à satisfaire le besoin d'actualisation de soi dépend de ses besoins actuels, de son environnement et des agents stressants.

En analysant chacun des paliers de la pyramide, on constate que la notion d'éthique est partout présente. Le respect de l'éthique se développe de plus en plus, notamment dans les pays riches, au fur et à mesure que les besoins les plus basiques sont assurés – même s'il est bien clair qu'ils ne le sont pas, loin s'en faut, pour tout le monde. Pour revenir à l'entreprise, on commence à voir des cas où le non-respect des codes éthiques peut conduire un employeur à se justifier devant les tribunaux... Les risques liés au non-respect de l'être humain, de ses droits et de son intégrité ne sont donc pas à observer par le petit bout de la lorgnette.

- **Risques éthiques et partie prenantes**

L'organisme est en perpétuelle situation d'échange avec ses différentes parties prenantes. Les risques éthiques peuvent également concerner les autres des parties prenantes de l'organisme :

- le personnel : c'est peu ou prou l'objet du paragraphe précédent ;
- les clients ;
- les fournisseurs ;
- les actionnaires ;
- la collectivité.

Face à chacune des parties prenantes, l'organisme peut être amené à se retrouver, bon gré ou mal gré, face à des problèmes d'ordre éthique. Ces risques sont différents selon chacune des parties prenantes. On trouvera ci-dessous quelques pistes pour identifier les couples partie prenante/risque :

- Personnel :
 - harcèlement physique et moral ;
 - non-respect de la parité ;
 - défaut de management ;
 - mauvaises conditions de travail.
- Fournisseurs :
 - discrimination ;
 - pots de vin ;
 - abus de position dominante, marges arrière... ;
 - détournement de compétences ;
 - espionnage.

- Actionnaires :
 - non-transparence financière ;
 - délit d’initiés ;
 - manipulations boursières douteuses.
- Collectivité :
 - non-respect de l’environnement ;
 - corruption ;
 - abus de position dominante.

- **Éthique, générations futures, développement durable**

Il est une partie prenante qui n’est pas citée dans ce qui précède, car elle ne peut guère faire entendre sa voix : les générations futures. Il devient de plus en plus évident que nos activités ne seront pas influencées sur l’état dans lequel nous allons laisser la planète. Problème éthique s’il en est, et qui concerne des êtres que nous aimons déjà.

Ce sont les concepts du développement durable qui représentent le mieux, actuellement, cette problématique. Considérer les générations futures comme une cinquième partie prenante, et observer l’impact que nous avons sur notre environnement avec cet éclairage, peut être la source de réflexions intéressantes pour les entreprises dont les valeurs sont assez fortes pour supporter le déploiement d’une telle politique.

6.9.3 Le domaine normal

- **Comment le définir : savoir qu’on y est**

Ce n’est pas simple de poser les bornes du domaine normal quand on parle d’un sujet aussi vaste et subjectif que l’éthique. En effet comment définir les limites du bien et du mal ?

On dispose de textes réglementaires ou assimilés :

- le Code du travail (en particulier pour le harcèlement) ;
- la norme « Social Accountability 8000 », qui peut être utilisée comme référentiel pour des risques éthiques se rapportant aux conditions de travail.

Les principes du Développement durable et de la Responsabilité sociale et environnementale sont également sources de références.

Mais tout ceci reste peu quantifié, et surtout soumis à des appréciations (et à des appréciateurs...) pas toujours qualifiés, pas toujours reconnus... et encore moins, parfois, désirés.

C'est donc en fin de compte aux dirigeants de l'organisme de définir les limites entre les trois domaines. Ils peuvent utilement s'appuyer sur les valeurs, bases de l'organisme, telles que nous les avons positionnées dans le paragraphe 4.1.1.

- **Comment y rester : méthodes et bonnes pratiques**

Cette idée a donné naissance, il y a quelques années, à la rédaction de chartes d'éthique, qui ont parfois fait l'objet de publicité plutôt que de déploiements réels. Il semble que la mode en soit un peu passée, et comme pour toute mode les beaux esprits ont tendance à exprimer du mépris pour ce genre d'initiatives. C'est à notre avis un peu dommage, car le fait même de mettre le sujet sur la table, d'en exprimer les problématiques, dans des mondes où l'omerta était plutôt la règle, a constitué et constitue encore souvent un progrès. Tout dépend de la culture de l'organisme dans lequel une telle charte doit être élaborée et déployée.

Une charte bien faite a en effet l'avantage de pointer les domaines où le comportement de l'ensemble de l'entreprise doit être conforme aux valeurs qu'elle a elle-même adoptées. Pour peu qu'on l'ait assortie de chiffres (soit dans le texte lui-même, soit dans des « décrets d'application ») elle est même un élément essentiel pour promouvoir les progrès et les évaluer.

Il n'est pas interdit, loin de là, d'insérer des indicateurs ayant trait à l'éthique dans ceux qui instrumentent les processus de l'entreprise : si on le veut vraiment, on peut mesurer des éléments même réputés occultes, comme ceux ayant trait à la corruption. Il en est de même des indicateurs relatifs à la discrimination, par exemple. Le fait de refuser ce genre d'indicateurs, en général sous le prétexte que « ce n'est pas nécessaire chez nous », est souvent le signe d'un refus sur le fond, quand ce n'est pas un signe de mauvaise conscience, voire de culpabilité...

On trouvera également dans les référentiels évoqués plus haut, ainsi que dans ceux issus des méthodologies de la qualité totale (par exemple l'EFQM) des éléments permettant une telle évaluation.

6.9.4 Le domaine incidentel

- **Comment le définir : savoir qu'on y est**

Il est des événements qui justifient une réaction immédiate : découverte de cas de corruption, plainte pour harcèlement, discriminations évidentes, violation du Code du travail, etc.

Si on a développé une charte, et surtout si elle est munie d'indicateurs, la tâche est facilitée. Il en est de même si les processus sont instrumentés.

Comme ce n'est pas toujours le cas, et pas dans tous les domaines, c'est l'appréciation des dirigeants qui va déclencher les réactions. Les signaux qui vont être à l'origine sont souvent des signaux faibles, au moins pris individuellement.

On citera : les enquêtes de satisfaction (du personnel, mais aussi des clients et autres parties prenantes), les conflits sociaux locaux, les articles de presse... mais aussi, et c'est plus gênant (sur le plan... de l'éthique !) : les rumeurs, les « corbeaux », voire des méthodes moins avouables (enquêtes...) mais qui peuvent être nécessaires. La condition que ce genre d'initiatives doit absolument respecter est que la morale fasse à peu près bon ménage avec l'intérêt global de l'entreprise, sans trop contrevenir à la morale individuelle...

• **Comment agir : méthodes et bonnes pratiques**

Dans le cas simple où un événement tel qu'évoqué plus haut se produit, il n'y a pas deux types de réaction, mais un seul : il faut traiter, tout de suite, et si possible publiquement. C'est à la rapidité et à la transparence de la réaction que les collaborateurs et l'environnement jugeront de la crédibilité des dirigeants.

Dans le cas où la réaction est initiée par des signaux faibles, les dirigeants devront « instruire l'affaire » et seront souvent confrontés à un dilemme : le maintien de la morale peut exiger des actes qui ne la respectent pas, comme la violence peut être nécessaire pour prévenir une violence plus grande.

6.9.5 Le domaine accidentel

• **Comment le définir : savoir qu'on y est**

On ne meurt pas d'une « crise éthique », mais de ses conséquences. On entre donc dans le domaine accidentel quand une crise affecte l'entreprise dans ses aspects plus « matériels ». Pour reprendre les concepts développés au paragraphe 5.3.3, c'est souvent la « crise réplique » qui va mettre l'entreprise en danger.

Sans être exhaustif, on peut citer :

- une crise médiatique majeure ;
- la remise en cause radicale d'une équipe dirigeante ;
- des dysfonctionnements des processus assez importants pour compromettre la performance ;

- une crise juridique majeure ;
- et, ce qui en est souvent la conséquence, une crise financière.

Les actionnaires et surtout ceux qui les manipulent adorent « faire leur beurre » avec les crises éthiques des autres... Nous laisserons au lecteur le soin de se faire une opinion personnelle sur le caractère éthique d'un tel comportement...

• **Comment agir : méthodes et bonnes pratiques**

Comme nous venons de le voir, une crise éthique ne met en danger l'entreprise que par sa crise réplique. Il va donc falloir savoir traiter simultanément – ou plutôt successivement – deux crises.

En ce qui concerne la crise réplique, on se reportera aux chapitres correspondants de cet ouvrage. Comme on ne peut pas demander l'impossible à une équipe de dirigeants, la crise éthique passera donc au second plan tant que la première ne sera pas terminée.

Le traitement de la crise éthique sera donc le plus souvent long et parfois s'enfoncera dans une certaine discrétion. Le risque majeur pour les dirigeants de l'entreprise est d'oublier un peu... La tempête est passée, il faut remettre le bateau sur sa trajectoire, et aussi souffler un peu... et si on passait à autre chose ? D'autant plus que les médias qui se sont tant intéressés à nous font désormais leurs choux gras du tournoi sportif ou du mariage de la princesse !

L'équipe de crise devra donc se préparer à une très longue vie. Ce point n'est pas sans incidence sur la façon de la constituer, et de la maintenir pendant longtemps ; au-dessus de l'équipe, une autorité dûment mandatée par les plus hauts dirigeants devra garantir cette pérennité.

En tout état de cause, le corps social se souvient des agressions qu'il a subies, un peu comme le corps humain se souvient de tous les verres d'alcool qui l'ont traversé. Une absence de traitement radical des causes profondes de la crise éthique compromettra de façon absolue toute chance pour l'entreprise de résister au mieux à la suivante – et personne ne peut garantir qu'il n'y aura pas de suivante. À l'heure chaude de l'été 2006 où nous écrivons ces lignes, une grande entreprise européenne aéronautique est impliquée dans une carambouille politico-financière assez minable, et plonge dans une autre où ses plus hauts dirigeants sont soupçonnés de délits d'initiés. Loin de nous l'idée de prétendre savoir la vérité, et encore moins de dire la justice ou de prédire l'avenir. Mais une chose est certaine : même si les deux affaires n'ont pas grand-chose en commun, la fragilisation issue d'un traitement insuffisant de la

première crise risque de coûter très cher quand il faudra traiter la deuxième... et la suivante.

Quant au Café du commerce, dont il convient de mépriser les échos jusqu'au moment où ses clients se transforment en électeurs, le verdict est simple et définitif : « tous des pourris » !

Autant dire que la communication sur le traitement de la crise devra être particulièrement pertinente, soignée et durable. C'est en dizaines d'années qu'il faut évaluer le temps qui sera nécessaire pour restaurer la confiance : en gros, il faudra qu'une génération succède à la précédente. Même ceux qui n'étaient pas encore en âge de comprendre les événements au moment où ils se sont produits n'oublieront jamais le travail des enfants de Nike (même s'il y a eu bien pire ailleurs et depuis), les malversations d'ELF et du Crédit Lyonnais (même si elles étaient dans les mœurs du temps), le nuage de Tchernobyl (même si le vrai coupable n'est pas celui qu'on désigne), etc.

Conclusion

Ou le paradoxe d'Astérix

Notre conclusion sera un encouragement : manager les risques, c'est agir. La pire des choses serait que la lecture de cet ouvrage, ou plus globalement la réflexion sur une politique de management des risques, vous conduise à l'inaction. Nous aurions pu trouver dans la littérature des phrases admirables de grands auteurs pour appuyer cette idée. Ce serait pure pédanterie. Nous évoquerons donc simplement des personnages dont nous avons déjà parlé au début : les Gaulois de la tribu d'Astérix. Là au moins vous pouvez croire, cher lecteur, que nous avons lu les ouvrages, et vous aussi sans doute.

Pourquoi, en effet, alors que le seul danger qu'ils craignent est la chute du ciel sur leur tête, portent-ils un casque ?

Nous vous laissons là, sur cette question fondamentale, et terminerons par deux affirmations :

- **Le management des risques, c'est très compliqué** : ce n'est pas facile d'identifier, de caractériser, de hiérarchiser, de maîtriser... Il est même certain qu'on ne saurait le faire parfaitement.
- **Le management des risques, c'est très simple** : un peu d'énergie, un zeste de méthode, beaucoup de bon sens... On gagne à tous les coups.

Bon courage !

Annexe 1

Le concept de

« Management par Projet »

(Commentaire AFITEP)

Dans un nombre restreint de cas, le « décideur » estime qu'une activité à caractère non répétitif dont il a la charge comporte une part importante d'inconnu ou d'incertitude et ne peut être confiée sans risque à l'organisation habituelle de l'entité, laquelle, pour cette occasion précise, peut être jugée inadaptée à la nature du problème. Le décideur prend alors l'option forte de mettre en place, pour la seule conduite de cette activité, une organisation spécifique, dénommée « **Management par Projet** ». L'activité correspondante, qu'elle concerne la technologie, la gestion, le social, etc. est alors toujours désignée par le terme de projet.

Selon les appréciations portées par le « décideur » sur les compétences de l'entité dont il a la charge, cette organisation spécifique peut s'écarter plus ou moins de l'organisation permanente. Ainsi, dans la version la plus intégrée du « Management par Projet », tous les acteurs sont déchargés de leurs missions habituelles et retirés du système hiérarchique auquel ils appartiennent pour être totalement dédiés au projet et intégrés dans son système de management. Mais l'organisation peut aussi chercher à s'appuyer, pour une part plus ou

moins importante du projet, sur quelques groupes professionnels constitués que le décideur estime adaptés à la nature de la tâche qu'il désire leur confier et que le « Management par Projet » se contentera alors de coordonner.

Le « Management par Projet », qui remplace temporairement et sur un thème bien délimité, tout ou partie des organisations en place, a un caractère potentiellement déstabilisant car il peut remettre en cause les fondements et les comportements de l'entreprise, c'est-à-dire la structuration par service, la permanence de l'organisation et des règles, la standardisation des procédures, le fractionnement des responsabilités, le regroupement des tâches par nature, le travail séquentiel... Il importe donc de ne décider la mise en place d'un « Management par Projet » et son niveau d'intégration que si la nature de la performance attendue et l'existence de risques et d'enjeux forts justifient d'en accepter les exigences. Aussi, chaque fois que possible, le choix pourra s'orienter vers une simple « Coordination » intégrée dans l'organisation permanente, quitte à chercher à en accroître l'efficacité en reprenant certains des « fondamentaux » du « Management par Projet » (la responsabilisation individuelle, la formalisation des missions, la conception du *reporting* en particulier).

Ces considérations éclairent bien l'aspect subjectif de l'appréciation du facteur de nouveauté ou d'incertitude qui doit être évalué, non dans l'absolu mais par rapport à ce que l'entreprise et certaines entités savent faire. L'une des responsabilités majeures du « décideur » est d'estimer avec clairvoyance et sans *a priori* les capacités et les limites de l'organisation existante. L'échec d'un projet pour cause de non-adaptation des structures en place lui sera d'autant plus imputable qu'il est le seul ayant la mission et le pouvoir de décider le lancement d'un « Management par Projet » ou de lui préférer une simple « Coordination ».

Annexe 2

Définitions

- Acceptation du risque : décision de faire face aux conséquences d'un risque.
- Accident : événement non désiré portant atteinte aux ressources de l'organisme.
- Aléa : événement identifiable et dont la probabilité d'occurrence n'est pas quantifiable (AFNOR, FD X50-117).
- Analyse des risques : processus d'identification, d'estimation et d'évaluation des risques afin de décider du traitement des risques retenus (AFNOR, FD X50-117).
- Appréciation du risque : processus d'identification des risques et de détermination du type d'analyse à mener pour chacun d'eux (analyse qualitative ou analyse quantitative).
- Caractérisation des risques : processus visant à déterminer les caractéristiques essentielles (causes, nature, origine, conséquences...) des risques.
- Conséquence : résultat d'un événement (ISO, guide ISO 73).
- Couverture financière du risque : réserve de fonds pour couvrir les coûts de mise en œuvre du traitement du risque et les coûts associés (ISO, guide ISO 73).
- Criticité d'un risque : niveau d'importance d'un risque résultant de la combinaison de ses caractéristiques quantifiées : la gravité de ses conséquences, sa possibilité d'apparition et/ou sa possibilité de détection (AFNOR, FD X50-117).

- Danger : situation, condition ou pratique qui comporte en elle-même un potentiel à causer des dommages aux personnes, aux biens ou à l'environnement (OHSAS 18001). On peut aussi lui donner une notion de maîtrise *a contrario* du péril complètement non maîtrisable.
- Détectabilité : capacité à pouvoir identifier des indicateurs de survenance (ou symptômes) d'un risque.
- EFQM : *European Foundation for Quality Management* ; association européenne fondée dans les années 90 par de grandes entreprises, et gérées par des entreprises qui décerne tous les ans le Prix Européen de l'Excellence. Maintient le « modèle EFQM » et ses outils et méthodes attachés. Siège à Bruxelles.
- Évaluation des risques : processus de comparaison et de hiérarchisation des risques estimés avec des critères de risque donnés pour déterminer l'importance d'un risque (ISO, guide ISO 73).
- Exposition au risque : indicateur résultant du produit de la probabilité d'apparition du risque par les coûts associés.
- Fréquence d'apparition : correspond au nombre d'observations de la survenance d'événements plus ou moins similaires sur une période passée.
- Financement du risque : réserve de fonds pour couvrir les coûts de mise en œuvre du traitement du risque et les coûts associés.
- Gravité des conséquences : importance des conséquences de l'événement redouté sur les différents objectifs.
- Identification des risques : processus permettant de trouver et de lister les risques encourus.
- Incertitude : situation résultant d'une insuffisance d'informations.
- Incident : événement de faible gravité mais qui aurait pu entraîner un accident (parfois dénommé « presque accident »).
- Management des risques : processus d'application de la politique de l'organisme permettant la mise en œuvre itérative et continue de l'analyse et de la gestion des risques (AFNOR, FD X50-117).
- Opportunité : événement dont les conséquences potentielles sont favorables à l'atteinte des objectifs.
- Partie intéressée : individu ou groupe concerné ou affecté par les performances d'un organisme.

- Perception du risque : manière dont une partie prenante considère un risque à partir d'un ensemble de valeurs ou de préoccupations (ISO, guide ISO 73).
- Période active : période durant laquelle le risque est susceptible de se manifester (AFNOR, FD X50-117).
- Pilote de risque : personne chargée de recueillir les informations sur le risque, de définir et mettre en œuvre les stratégies de traitement de ce risque et d'en assurer le suivi (AFNOR, FD X50-117).
- Plan de management des risques : document définissant la mise en œuvre du management des risques.
- Prise de risque : acceptation de la possibilité de la charge d'une perte, ou du bénéfice d'un gain, d'un risque particulier (ISO, guide ISO 73).
- Probabilité d'apparition : degré de vraisemblance de l'occurrence d'un événement.
- Probabilité de détection : degré de vraisemblance pour que les signes précurseurs de l'apparition de l'événement redouté puissent être détectés (AFNOR, FD X50-117).
- QSE : Qualité-Sécurité-Environnement, démarche de management globale partant du principe que les systèmes de management de la qualité, de l'environnement et de la sécurité sont de nature analogue et gagnent à être déployés de façon cohérente. Peut faire l'objet d'une « tri-certification ».
- Risque : combinaison de la probabilité d'un événement et de ses conséquences (ISO/CEI 73).
- Refus du risque : décision visant à ne pas être impliqué dans une situation à risque, ou dans une action visant à se retirer d'une situation à risque (ISO, guide ISO 73).
- Risque secondaire : risque résultant directement de la mise en œuvre d'une stratégie de réponse.
- Risque résiduel : risque subsistant après le traitement du risque (ISO, guide ISO 73).
- Sécurité : absence de risque de dommages inacceptables.
- TQM : « *Total quality management* », traduit en français par « management total de la qualité », ou « management de la qualité totale », ou « par la qualité totale » ou enfin – encore mieux ! – simplement TQM.
- Traitement du risque : processus de sélection et de mise en œuvre des mesures visant à modifier le risque (ISO, guide ISO 73).

- Transfert du risque : partage avec une autre partie du bénéfice du gain, ou de la charge de la perte, d'un risque particulier (ISO, guide ISO 73).
- Vulnérabilité : une vulnérabilité se caractérise par les pertes financières induites par la réalisation d'un événement aléatoire frappant une ressource de l'entreprise. Autrement dit une vulnérabilité, pour une organisation donnée, est parfaitement identifiée par trois paramètres : l'objet du risque, le péril (ou événement) et l'impact potentiel sur les objectifs (J.-P. Louisot).

Bibliographie

Remerciements : cette base bibliographique a été constituée grâce à l'aide de Didier Groperrin, étudiant du mastère Qualité et Management des Performances de l'Université de Franche-Comté.

Bibliographie Internet

Nota : les liens de la liste ci-dessous étaient opérationnels au moment de la rédaction du texte... Dans le monde rapidement changeant d'Internet, les auteurs ne garantissent pas au lecteur que son surf sera toujours efficace...

Sites Web

ISO, organisation internationale de normalisation : www.iso.org

AFNOR : www.afnor.org

DRIRE : www.drire.gouv.fr

AIDA.INERIS : <http://aida.ineris.fr>

Institut Européen de Cindyniques : www.cindynics.org

Ministère de l'Écologie et du Développement durable, rubrique « risques et pollutions », sous-rubrique « risques industriels » :
www.ecologie.gouv.fr/rubrique.php3?id_rubrique=29

MICROSOFT, « Guide de gestion des risques de sécurité » :
www.microsoft.com/france/technet/securite/guidance/default.msp

P. Lagadec, site personnel : www.patricklagadec.net/fr

Réseau Allquality : www.allquality.org

Liens Internet utilisés dans le chapitre 6

risques projets : www.csp.fr

www.gestiondeprojet.net/plan_communication.html

risques éthiques : www.heraclitea.com/ethique1.htm

<http://membres.lycos.fr/papidoc/573besoinsmaslow.html>

risques ressources : www.sg.cnrs.fr/fsd/securite-systemes/organisation.htm

Méthodologies et démarches de gestion des risques

Ouvrages généraux

B. Barthélemy, P. Courrèges, *Gestion des risques, méthode d'optimisation globale*, Éditions d'Organisation, 2003.

Ifaci, PriceWaterhouseCoopers, Landwell, *Le management des risques de l'entreprise, Cadre de références, techniques d'application*, Éditions d'Organisation, 2005.

F. Moreau, *Comprendre et gérer les risques*, Éditions d'Organisation, 2002.

É. Degobert, J. Le Ray, *Maîtrise des risques professionnels, Mettre en œuvre une démarche d'amélioration*, AFNOR, 2004.

J. Le Ray, *Gérer les risques, pourquoi ? Comment ?*, AFNOR, 2006.

A. Desroches, A. Leroy, F. Vallée, *La gestion des risques*, Hermès-Lavoisier, 2003.

A. Desroches, A. Leroy, F. Vallée, *Dictionnaire d'analyse et de gestion des risques*, Hermès Science Publications, 2005.

S. Gaultier-Gaillard, J.-P. Louisot, *Diagnostic des risques, identifier, analyser et cartographier les vulnérabilités*, AFNOR, 2004.

X. Guilhou, P. Lagadec, *La fin du risque zéro*, Éditions d'Organisation, 2002.

P. Lagadec, *La gestion des crises*, Mac Graw Hill, 1991.

C. Roux-Dufort, *Comment en est-on arrivé là ? Du terrain de crise à la catastrophe*, Magazine de la communication de crise, sept. 2005.

S. Ramboatiana, *Les crises organisationnelles : fièvre ou choléra*, Magazine de la communication de crise, sept. 2005.

M.-C. Delaveaud, *Le risk management en 5 étapes*, AFNOR, 2003.

G. de Mareschal, *La cartographie des risques*, AFNOR, 2003.

G.-Y. Kervern, *Les éléments fondamentaux des cyndiniques*, Economica, 1995.

J.-L. Nicolet, A. Carnino, C. Wanner, *Catastrophes ? Non, merci !*, Masson, 1989.

G.-D. Carton, *Éloge du changement*, Village Mondial, 2004.

P. Peretti-Watel, *La sociologie du risque*, Armand Colin, 2003.

B. Froman, J.-M. Gey, F. Bonnifet, *Qualité / Sécurité / Environnement – Construire un système de management intégré*, AFNOR, 2002.

Guides pratiques et études

Maîtrise des risques, classeur à feuillets mobiles, AFNOR, 2004.

G. Landy, *AMDEC-Guide pratique*, AFNOR, 2006 (2^e éd.)

Baromètre du risk management, Étude TNS-SOFRES, TNS-SOFRES, 2005.

Maîtrise des risques, la sûreté de fonctionnement, livret ISDF, Octares Éditions, 1997.

Normes

ISO/IEC Guide 73:2002, « Management du risque-Vocabulaire-Principes directeurs pour l'utilisation dans les normes », AFNOR.

ISO/IEC 17799:2005, « Code de bonne pratique pour la gestion de la sécurité de l'information », page 5/65, AFNOR.

ISO 9001:2000, « Système de Management de la Qualité », AFNOR.

NF EN ISO 14001:2004, « Système de Management Environnemental », AFNOR.

OHSAS 18001:1999, « Le Management de la Santé et de la Sécurité au travail », AFNOR.

SA 8000 Social Accountability Standard 8000:2001.

