

Documents Numériques relatifs au Cours Gestion des Risques et Intelligence Economique :

- ✓ **Syllabus du Cours**
- ✓ **Documents supports du Cours**
- ✓ **Etudes de Cas avec Corrigées**
- ✓ **Examens 2023-2024-2025**

Syllabusⁱ

Titre UE: Management des Risques et Intelligence Economique Enseignant(e): Dr. karima Mnasser Département: Sciences de Gestion	Parcours: 3LSMGT Semestre : 1 Volume horaire : 42h Cours 21h TD
Objectifs du cours :	
<ul style="list-style-type: none">✓ Maîtriser les différents concepts fondamentaux liés au management des risques.✓ Comprendre le rôle fondamental de l'intelligence économique dans la gestion des risques.✓ Montrer l'importance de l'intelligence économique entant qu'outil d'aide à la prise de décision stratégique.✓ Comprendre la relation entre IE et SI✓ Mobiliser IE comme mode de management de l'information✓ Maîtriser les différents outils d'intelligence économique et leurs rôles dans la gestion des risques.	
Compétences attendues :	
<ul style="list-style-type: none">➤ Maîtriser l'étude et l'analyse des risques à travers une analyse qualitative : (Matrice/Cartographie des risques, hiérarchie et priorité des risques et c).➤ Savoir appliquer la méthodologie de la gestion intégrée des risques.➤ Proposez des recommandations managériales pour une gestion efficace des risques.➤ Maîtriser l'outil de l'intelligence économique au service de la gestion des risques et dans la prise des décisions stratégiques.➤ Savoir appliquer les outils de l'intelligence économique notamment : Lobbying, Benchmarking, La veille, communication des crises et c.	
Plan du cours :	
Semaines	Chapitres
1	<p>Chapitre1 : Gestion des Risques : Définitions, Typologies et Composantes</p> <ul style="list-style-type: none">➤ Définition générale du risque.➤ Les Attributs du risque : Incertitude ; Information et connaissance, coût du risque, le facteur temps, l'être humain et la perception.
2	<p>Chapitre1 : Gestion des Risques : Définitions, Typologies et Composantes</p> <ul style="list-style-type: none">➤ La mesure du risque : Analyse quantitative.

	<ul style="list-style-type: none"> ➤ La mesure du risque : Analyse qualitative (Matrice : probabilité d'occurrence du risque/Impact du risque) // (Zone d'inacceptabilité, Zone de tolérance, Zone d'acceptabilité). 	
3	<p style="text-align: center;">Chapitre1 : Gestion des Risques : Définitions, Typologies et Composantes</p> <ul style="list-style-type: none"> ➤ Profil du risque de l'organisation. (Type du risque, source du risque, objet du risque et degré du contrôle). 	
4	<p style="text-align: center;">Chapitre1 : Gestion des Risques : Définitions, Typologies et Composantes</p> <ul style="list-style-type: none"> ➤ Typologies des risques : <ul style="list-style-type: none"> • Grille d'analyse pour « Cartographier les risques ». ➤ La gestion intégrée des risques : Outil pour une bonne prévention : <ul style="list-style-type: none"> • Quatre phases requises : <i>Elaborer le profil des risques, créer une fonction de gestion intégrée des risques, pratiquer une gestion intégrée des risques et assurer l'apprentissage continu en matière de gestion des risques.</i> 	
5	<p style="text-align: center;">Chapitre1 : Gestion des Risques : Définitions, Typologies et Composantes</p> <ul style="list-style-type: none"> ➤ <i>Etude de Cas sur Gestion des Risques : Cartographie des risques, hiérarchisation des risques, recommandations managériales pour une gestion efficace des risques et c.</i> 	
6	<p style="text-align: center;">Chapitre2 : Intelligence économique et Gestion des Risques :</p> <ul style="list-style-type: none"> ➤ Définition de l'intelligence économique. (IE) ➤ Interaction entre gestion des risques et intelligence économique : <ul style="list-style-type: none"> • Trois niveaux d'étude (Macroéconomique, Mésoéconomique, Microéconomique). • Lien entre les finalités de l'IE et les risques encourus par les entreprises. 	
7	<p style="text-align: center;">Chapitre2 : Intelligence économique et Gestion des Risques :</p> <ul style="list-style-type: none"> ➤ Processus de l'intelligence économique (IE) : 4 étapes requises. 	

8	<p>Chapitre2 : Intelligence économique et Gestion des Risques :</p> <ul style="list-style-type: none"> ➤ Intelligence économique (IE) et Gestion des risques informationnels : <ul style="list-style-type: none"> • IE d'entreprise : Intelligence du management : (Nouvelle compétence des entreprises). • IE d'entreprise : Intelligence du management : (Système d'information SI adapté à la démarche d'IEE : Protection du patrimoine informationnel).
9	<p>Chapitre2 : Intelligence économique et Gestion des Risques :</p> <ul style="list-style-type: none"> ➤ Analyse de l'entretien avec Marc Chatelard (Sénior vice président Transport Asie-Pacifique, Groupe Alstom) : <i>IE, patrimoine informationnel de l'entreprise et stratégie internationale, Type de Risques, Priorités, stratégies de gestion de risques et c....</i>
9.....12	<p>Chapitre 3 : Les Outils en Intelligence économique</p> <ul style="list-style-type: none"> ➤ IE comme mode de management stratégique de l'asymétrie informationnelle : <ul style="list-style-type: none"> • Approche fonctionnelle de l'IE : Renseignement, Influence et protection. • Relation entre Gestion de Risques, IE et Outils de l'IE ➤ Outils de l'IE : <ul style="list-style-type: none"> • Outil 1 : Cycle de Renseignement • Outil 2 : Lobbying • Outil 3 : Veille • Outil 4 : Benchmarking • Outil 5 : Communication de Crise
13- 14	<ul style="list-style-type: none"> ✓ Etude de cas sur Outil Lobbying : Acteurs clés du Lobbying ✓ Etude de Cas sur les Facteurs Clés de Succès (FCS) du Lobbying

Mots clés : Profil du risque, Mesure du risque, cartographie des risques, Intelligence économique d'entreprise, IEet SI, Outils en IE, gestion intégrée des risques.

Documents Supports du Cours Management des risques et Intelligence Economique

de la chaîne, où il peut causer des dégâts importants. Ainsi il est nécessaire pour chaque entreprise de pouvoir contrôler le processus d'évaluation des risques et de pouvoir parer aux situations dangereuses mettant en péril sa survie.

La notion de risque comporte deux composantes importantes, soit :

- a) *le degré d'incertitude* : le risque se rapporte à l'incertitude qui entoure des événements et des résultats futurs. Le risque ne peut se dissocier de cette incertitude, car c'est par l'existence même de cette incertitude entourant le futur, qu'un risque existe. Ainsi pour l'entreprise il s'agira de diminuer l'incertitude concernant les événements susceptibles de nuire à la réalisation de ses objectifs.
- b) *l'ampleur des conséquences* : il s'agit ici des dommages causés à l'entreprise, à ses employés, à ses investisseurs, à ses partenaires, etc. Ainsi, on pourrait parler de dommages physiques ou de différentes pertes comme les pertes financières, la perte d'image et de notoriété, de part de marché, etc.

Le risque combine donc la probabilité d'un événement et l'ampleur de ses conséquences. L'objet de la gestion des risques n'est pas de supprimer la totalité des risques pour atteindre le *risque zéro*, mais de déterminer les risques que l'entreprise pourra assumer en fonction de sa stratégie globale, sans se mettre en péril, et de déterminer aussi les éventuelles conséquences.

La définition utilisée dans cette thèse pour la notion de risque sera : « *La nature d'un risque se rattache à l'incertitude des événements dont les probabilités d'incidence et de nuisance, ainsi que l'ampleur des conséquences peuvent avoir une répercussion préjudiciable sur les objectifs d'une entreprise.* » (Camélia Dumitriu, 2004). Ainsi la vigilance face aux risques est de rigueur dans les processus de gouvernance et de décision. La probabilité et l'incidence d'un événement laissent entendre qu'il faut procéder à une analyse quantitative ou qualitative avant de prendre une quelconque décision concernant les plus importants risques ou les menaces majeures qui nuiront à l'atteinte des objectifs de l'organisation.

3.2.2 Les attributs du risque

Afin de mieux comprendre ce qu'est réellement un risque il nous est apparu important dans cette étude de connaître les différents attributs qui constituent un risque. En premier lieu l'incertitude constitue une composante majeure du risque, ensuite viennent l'information, les coûts, le facteur temps, les facteurs humains, la notion d'utilité et la notion d'impact du risque.

a. L'incertitude : une composante majeure du risque

Si l'on se réfère à la définition du risque qui a été développée en premier lieu, tout risque peut se matérialiser avec une certaine probabilité. Le calcul ou l'estimation de cette probabilité comporte un degré d'incertitude qui dépend de la manière dont cette probabilité a été analysée et étudiée. L'étude de cette probabilité présente, malgré le caractère scientifique de certaines méthodes analytiques, une importante composante subjective.

Jean Charles Dubois écrit dans son ouvrage « L'analyse du risque » que « *la façon la plus répandue de mesurer quantitativement l'incertitude consiste à lui attribuer une probabilité subjective* ». L'organisation a de toute manière intérêt à planifier sa gestion des risques malgré l'incertitude du futur et l'auteur Beer (Beer S, 1972 « Brain of the firm : The managerial cybernetics of organisation », Allen Lane, The Penguin Press) nous rappelle que nous ne connaissons pas le futur. Nous avons seulement des suppositions sur ce que nous projetons dans le futur, mais nous ne maîtrisons pas totalement notre environnement pour manipuler les événements avec grande certitude. Et comme cette incertitude compose une situation donnée, chaque situation comporte ainsi un grand nombre de composantes variables qui sont difficiles à maîtriser. Ce sont ces variabilités qui composent la mesure de l'incertitude selon Beer.

b. L'information et la connaissance

L'information et la connaissance sont devenues une matière première très précieuse et représentent des actifs intangibles stratégiques; dans certains cas, l'utilisation stratégique de l'information peut très vite devenir une arme stratégique. L'information et la connaissance influencent de plus le processus de gestion des risques et des crises. En effet les études qui ont été effectuées par Lutz et Reilly (Lutz R et Reilly P, 1973, « An Exploration of the Effects of Perceived Social and Performance Risk on Consumer Information Acquisition », Edition Advances in Consumer Research, p393 – 405) démontrent que « plus le risque perçu est élevé, plus l'homme aura tendance à rechercher de l'information ». Ainsi, la recherche, l'analyse, et le traitement de l'information et de la connaissance sont proportionnels aux risques perçus. La valeur de l'information est mesurable selon sa capacité à influencer une décision et sa capacité à être transmise au bon moment, au bon endroit, et à la bonne personne. Selon Jean Charles Dubois, cette valeur de l'information dépend de plusieurs paramètres qui sont les suivants :

- ◆ *L'accessibilité : L'information pourra prendre de la valeur si celle-ci peut être accessible rapidement. Si elle est disponible au moment de l'analyse du risque ou au moment de la crise, alors elle aura une grande valeur pour les gestionnaires.*
- ◆ *La date : Toute information perd de la valeur avec le temps. En effet plus l'information prend de l'âge, plus elle tend à se périmer. Ainsi une information en temps réel peut prendre une valeur stratégique. Mais par contre elle perd de son utilité et peut devenir nuisible à une prise de décision si elle est rendue trop vieille ou obsolète avec le temps. Elle n'aura plus de valeur significative.*
- ◆ *La présentation : L'information prend de la valeur en fonction de la qualité qu'on lui apporte à partir d'une bonne présentation. Par exemple la valeur d'un graphique peut avoir plus d'influence et d'impact qu'une longue explication de texte qui noie l'essentiel. Sa valeur est alors proportionnelle à sa présentation.*

- ◆ *La pertinence : L'information dépend aussi de sa pertinence, c'est-à-dire du message qu'elle apportera entre sa nature et son emploi potentiel pour la prise de décision. Cette pertinence dépendra du contexte et des utilisateurs.*
- ◆ *L'ordre : La place des mots est très importante pour donner un sens à l'information ainsi que pour son pouvoir d'influence. En effet les premiers mots sont le plus souvent retenus en priorité et dans une situation particulière donnent plus de sens et ont plus d'impact. Dans une bonne gestion d'évaluation et de perception des risques et des crises, la personne en charge de cette mission doit savoir utiliser cette caractéristique pour communiquer à son organisation le renseignement concernant un risque futur.*
- ◆ *La précision : La valeur de l'information augmente avec le niveau de précision qui s'y rapporte. Cette valeur est inversement proportionnelle au niveau de son approximation, et l'information perd de sa valeur si celle-ci est trop approximative.*
- ◆ *La quantité : La valeur unitaire d'une information décroît exponentiellement en fonction du nombre d'informations traitées.*
- ◆ *La validité : La validité de l'information est primordiale, elle permet d'assurer la fiabilité de l'information, c'est-à-dire la crédibilité de la source, la vraisemblance de l'information. Cependant cette validité reste du domaine de la subjectivité car elle ne peut pas être vérifiée à 100 %. L'invalidité de la source d'information constitue un risque majeur dans le processus de prise de décision, et les individus qui manipulent une grosse quantité d'informations, réalisent bien souvent un filtrage automatique et souvent ils ne retiennent que les informations qui ont à leurs yeux une valeur significative.*

Source : Dubois, Jean Charles 1996, « Analyse du risque : une approche conceptuelle et systémique », édition Chenelière/McGraw-Hill

Depuis l'arrivée des technologies de l'information et de communication, le rôle de l'information a considérablement évolué. On parle de plus en plus de confidentialité de l'information, de piratage, de protection des données, et de manipulation, phénomènes générés par la prolifération des moyens de transférer d'une manière électronique cette

c. Le coût du risque

En se référant à la définition du risque donné par L'AEMAR, [la combinaison de la probabilité d'occurrence et de la gravité des conséquences], le risque peut être considéré comme l'ensemble des pertes qui sont multipliées par la probabilité d'apparition du risque. Les pertes subies par une organisation ont bien souvent des répercussions en coût monétaire. En effet qui dit perte dit coût. Selon Jean Charles Dubois ce coût n'est pas forcément un coût monétaire mais il peut être un coût psychologique, ou un coût intangible (en terme d'image et de notoriété par exemple), un coût stratégique, etc. En effet, comment pourrait-on mesurer les effets négatifs d'une perte d'image sur le chiffre d'affaire et sur la fidélisation de la clientèle à une marque, après une crise? Il existe beaucoup d'interactions dans le système lors d'une perte, compte tenu du fait que les actifs intangibles ont bien souvent des répercussions sur les actifs tangibles et vice versa, ce qui rend difficile toute tentative de quantifier les coûts du risque.

d. Le facteur temps

Mesurer et évaluer un risque c'est savoir prévenir des événements qui pourraient nuire à l'organisation. Deux auteurs, Ball et Brown (Ball R, Brown P, 1969 « Portfolio Theory and Accouting ») présentent le risque comme un concept *ex ante* que l'on peut mesurer *ex post*. En effet la mesure du risque est une prévision dans le présent de ce qui pourra se produire en mesurant les indicateurs en fonction des événements passés. Pour choisir une bonne échelle de mesure ou mesurer des variables, les études sont réalisées en fonction des faits passés pour ensuite déduire des probabilités d'occurrence qui puissent permettre au gestionnaire du risque d'établir des prévisions et donner des recommandations opérationnelles. Le temps est donc bien une notion indissociable du risque et le futur, autant que le passé, conditionne notre jugement et nos perceptions sur un événement qui pourrait se reproduire. La méthode des scénarios, qui sera décrite un peu plus tard dans l'étude, se base sur la notion de «temps».

Jean Charles Dubois précise en outre que les personnes ont tendance à oublier les faits éloignés dans le temps, malgré leurs conséquences, et que, par conséquent, les gestionnaires

évaluent la probabilité du fait en fonction de leur facilité à se rappeler de la catastrophe. En général lorsqu'il est nécessaire de quantifier la probabilité d'un risque, on utilise une base de connaissances qui est reliée au temps, car le risque est bien souvent calculé sur une période donnée.

e. L'être humain et la perception

L'être humain joue un rôle incontournable dans la gestion des risques et des crises car c'est bien lui qui, le plus souvent, réalisera les analyses et prendra la décision finale. Or l'être humain est un « animal complexe » qui cherche à répondre à certains besoins en priorité d'après la pyramide de Maslow, comme les besoins physiologiques (c'est-à-dire la survie), les besoin de sécurité, de protection, d'affection et d'appartenance, et ce, bien souvent dans un contexte plein de contraintes et de risques. Or l'individu ne se comporte pas en tout temps de façon rationnelle et logique en fonction d'une seule finalité, il est bien plus complexe et ses réactions dépendent souvent de plusieurs facteurs externes et internes. En présence d'un risque ou d'une catastrophe, on ne peut pas affirmer catégoriquement que tout homme va agir rationnellement et logiquement. De plus, il est souvent difficile de pouvoir imaginer tous les scénarios possibles. La finalité d'une gestion des risques et des crises est d'arriver à une prise de décision ; d'un autre côté, le processus de prise de décision est un processus intellectuel et complexe qui dépend d'une situation donnée dans laquelle l'être humain va établir sa propre réflexion en fonction de ses capacités intellectuelles, de sa mémoire, de ses différentes tensions et finalement de la perception globale qu'il a face à la prise de risque.

Nous avons vu dans la définition du risque proposée par Loup Francart que le risque est la combinaison de la vulnérabilité et de la perception de celle-ci. Ainsi, même si l'homme est un être raisonnable on lui trouve bien des limites cognitives qui se répercutent dans son analyse et sa perception du risque. Bien des fois il existe des individus qui se trouvent en désaccord **les uns des autres** à cause de leurs différences d'opinion qui résulte en réalité de leur différence de perception.

Myers et McCaulley (Myers I.B et McCaulley MH, 1985 « A guide to the development and use of the Myers-Briggs type indicator », Consulting psychologists Press) expliquent que la

Pour conclure, il faut souligner le niveau d'influence que la perception humaine a sur l'identification, l'évaluation et le traitement des risques, ce qui rend le processus de gestion des risques très délicat. Cette influence réagira automatiquement et d'une manière directe sur la prise de décision finale concernant les moyens à mettre en œuvre pour limiter, contrôler et réduire le risque. Dans la partie où nous traiterons de « l'Infosphère », nous reviendrons sur la notion de la perception et de son influence dans la gestion de l'information et de la connaissance, par l'analyse «*des trois mondes*».

Il nous reste maintenant à connaître la mesure des risques selon différentes approches théoriques et sociales.

3.2.3 La mesure du risque selon l'approche théorique et selon l'approche sociale du risque

a. Approche théorique

Selon l'AMRAE (Association pour le Management de Risque et des Assurances de l'Entreprise) le risque est classiquement mesuré en fonction de la combinaison des deux paramètres principaux qui sont la probabilité d'occurrence et la gravité des conséquences. On a ainsi la relation suivante :

$$\blacklozenge \quad \textbf{Risque} = \textbf{Conséquences} * \textbf{Probabilité}$$

Les facteurs de probabilité sont les possibilités que le risque se réalise. On parle aussi de « fréquence d'occurrence » c'est-à-dire la vraisemblance mathématique qu'un événement se réalise. La fréquence correspond au nombre d'observations d'un événement dans une période donnée. Il y a plusieurs manières traditionnelles de calculer la grandeur de ses facteurs en fonction de critères qualitatifs, comme par exemple, la quantification d'une fréquence moyenne, faible ou forte, ou encore en utilisant une échelle approximative de mesure (de 1 à 10 ou de 1 à 5, par exemple). Selon cette approche qualitative, on peut classer le risque suivant une table de probabilité qui va du probable à l'extrêmement improbable, suivant

quatre possibilités: probable, rare, extrêmement rare ou extrêmement improbable. La probabilité peut se mesurer aussi avec des critères quantitatifs comme une probabilité effective d'apparition pour une période donnée (dans une année, ou dans un siècle par exemple).

Le facteur de gravité du risque, quant à lui, détermine une quantification de la perte subite qui fut engendrée par la réalisation du risque. L'incident peut mettre en péril certains enjeux de l'entreprise. L'impact de l'incident dépendra surtout des enjeux touchés. En effet un risque d'explosion n'aura pas le même impact dans une zone urbaine que dans une zone rurale. Ces pertes peuvent être mesurées selon une méthode qualitative (évaluation de l'impact : fort, moyen, faible ou bien mineur, majeur, critique et catastrophique par exemple), en utilisant une échelle de mesure ou bien selon une méthode quantitative (en calculant les pertes financières). Nous pouvons ainsi obtenir le tableau suivant pour la mesure des risques.

Tableau 3.1 : Tableau de fréquence et de gravité

<i>Fréquence</i>	<i>Fréquent</i>	<i>Peu fréquent</i>	<i>Rare</i>	<i>Extrêmement Rare</i>
<i>Gravité</i>				
<i>Mineur</i>				
<i>Majeur</i>				
<i>Critique</i>				
<i>Catastrophique</i>				

Selon la théorie des dominos de Heinrich, ce n'est pas seulement un fait seul et isolé qui provoque l'incident mais une combinaison de plusieurs causes qui sont reliées en chaîne et qui dans un état stationnaire fonctionnent en interaction. Mais dès que surgit un déséquilibre c'est la chaîne toute entière qui provoque l'incident ou l'accident. Ainsi il existe plusieurs approches probabilistes qui permettent d'utiliser dans la gestion des risques les arbres des défaillances et les arbres des causes et qui prennent en

Le modèle mini-max qui est représenté ci-dessous est un modèle de hiérarchisation des risques en fonction de la conjugaison des deux composantes du risque : fréquence d'occurrence et gravité. Le carré A représente le classement des risques qui ont un impact très fort sur l'organisation et dont la gravité du dommage est la plus importante et dont la probabilité est forte. Le carré A schématisse les risques les plus dangereux pour l'organisation. Le carré B représente le classement des risques ayant un impact toujours fort, c'est-à-dire que le risque décrit une grosse gravité de préjudice mais dont la probabilité d'apparition est faible. Le carré C rassemble tous les risques dont l'impact est l'inverse de celui du carré B avec un faible impact, ce qui démontre une faible gravité du risque mais la probabilité d'occurrence reste toujours forte. Le carré D rassemble les risques ayant un faible impact et une probabilité faible, ce qui représentent les risques les moins dangereux pour l'organisation. Ainsi grâce à ce modèle le gestionnaire de risques est capable de définir les priorités en terme de risques.

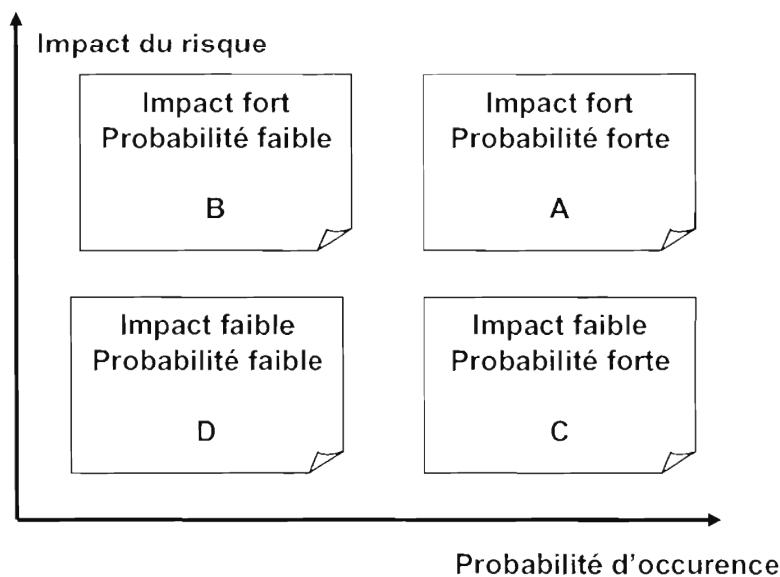


Figure 3.3 : Modèle de hiérarchisation des risques

b. Approche sociale du risque: les zones d'acceptabilité et de tolérance des risques

L'approche sociale module fortement l'approche théorique du risque à cause de la subjectivité et de la perception des décideurs face aux risques. La subjectivité du public conditionne l'appréhension des risques et elle est de plus en plus influente. Cette subjectivité est décrite par Adrien Bénard et Anne-Lise Fontan dans « La gestion des risques dans l'entreprise ; management de l'incertitude » 1994, selon trois facteurs qui sont : *l'inconnu, l'absence de maîtrise, et la gravité du risque ou de la crise.*

- ◆ La peur de l'inconnu dans des domaines ultrasophistiqués et encore peu compréhensibles pour l'être humain peut amener des comportements irrationnels ou idéologiques. A cette difficulté peuvent se greffer des lacunes de communication qui rendent le risque plus flou, tout en augmentant cette peur de l'inconnu.
- ◆ L'absence de maîtrise permet d'accepter plus facilement les risques inhérents à une activité.
- ◆ La gravité ou l'impact du risque comporte souvent un degré d'affectivité surtout si le risque peut toucher à l'intégrité de la personne humaine. Cette affectivité frappe aussi les médias qui se font la caisse de résonance amplifiant l'affectivité négative face à un risque, à une catastrophe ou à une crise majeure. Cette affectivité de l'opinion publique peut être une arme puissante pour faire adopter de nouvelles lois et de nouvelles contraintes réglementaires.

La littérature traditionnelle sur la gestion des risques fixe un cadre de réglementation des risques à trois niveaux, c'est-à-dire un niveau où le risque est jugé inacceptable, (on parlera de zone d'inacceptabilité sociale), un niveau où le risque est jugé largement acceptable, on parlera de zone d'acceptabilité sociale, et une zone intermédiaire qui sera

appelée zone de tolérance. Le niveau de risque jugé inacceptable d'après Romain Laufer est celui d'un « *risque majeur qui résulte de la crise du système de légitimité, c'est-à-dire une crise du droit et de la science* ». Selon cet auteur, il s'agirait d'un « *risque majeur qui résulte de l'effondrement du cadre d'anticipation qui permet de fournir une évaluation quantitative du risque* ».

Ainsi on peut regrouper les différentes acceptations des risques suivant le tableau ci-dessous inspiré du Séminaire Trustnet, une nouvelle perspective sur la gouvernance des activités à risques « Proposition & conclusion du séminaire européen Trustnet, 2000.»

Tableau 3.2 Acceptabilité du risque

Zone d'inacceptabilité	Le risque n'est pas justifié sauf dans des circonstances exceptionnelles
Zone de tolérance	Dans la zone de tolérance des mesures de contrôle doivent être mises en place afin de rapprocher le risque de la zone d'acceptabilité. Si le risque reste situé dans cette zone intermédiaire, l'activité ne sera entreprise qu'à la condition que des avantages soient attendus, qu'une réduction supplémentaire soit impossible ou qu'une forte disproportion subsiste entre les moyens engagés et la réduction du risque obtenue.
Zone d'acceptabilité	Le niveau de risque résiduel est insignifiant. Les ressources supplémentaires allouées à la réduction du risque seraient vraisemblablement disproportionnées par rapport à la réduction de risque obtenue.

Source : Proposition & conclusion du séminaire européen Trustnet, 2000, 36 p.

<http://www.mceapc.org/ateliers/7/doc1.html>

Camélia Dumitriu propose plusieurs situations distinctes qui déterminent le niveau de non acceptabilité sociale, qui sont présentées dans le tableau suivant :

Tableau 3.3 Crise et acceptabilité sociale

Toute catastrophe naturelle mal gérée	Un risque induit par l'activité humaine (par exemple, l'exposition à une pollution industrielle ou à une irradiation nucléaire) est généralement moins acceptable qu'un risque naturel (par exemple, l'exposition à un ouragan ou à une tornade). Par contre, dans ce dernier cas, une gestion «post-catastrophe» défectueuse entraîne un fort sentiment de non acceptabilité sociale.
Action imposée à une société ou à un groupe	Une action imposée involontairement (par exemple, l'expropriation imposée par le gouvernement du Québec pour construire l'aéroport de Mirabel); des mesures et des règles imposées par la force à une collectivité : la crise d'OKA; la décision de déménager ou de désactiver une usine, etc.
Action qui produit un effet ou conséquence atypique	Une conséquence atypique suite à l'utilisation ou à la consommation d'un produit/d'un service est jugée moins acceptable qu'une conséquence potentiellement désastreuse mais fortement connue: par exemple, pour les transporteurs aériens, le risque de thrombose veineuse des passagers contre le risque de crash d'avion; pour McDonald's, la crise de l'ESB contre le risque bactérien banal.
Action d'un « champion »	J&J et son produit-vedette, le tylenol; Mercedes et son nouveau modèle classe A; la crise de la marine royale britannique : Titanic, qu'on disait insubmersible, faisait partie de la classe « Olympique ».
Action qui produit un effet totalement opposé à la mission et aux valeurs déclarées par l'entreprise	J&J, le champion de la santé et son « médicament qui tue »; Nestlé, le symbole du « nourrisson » et son substitut repas qui « tue », etc.
Action injuste	Qui touche les enfants (la crise récente de l'Hôpital St. Justine), les personnes âgées (la crise des établissements de séjour-santé pour les personnes âgées à Montréal), etc.
Action qui menace directement un aspect qui représente « un souci » générique de la société civile	Les principaux soucis de la société civile: santé (71,2%); chômage (60,75%); environnement (68,71 %); crises économiques (39,7%); la violence, les guerres et la criminalité (67,8 %), etc. (Étude CFDD-FRDO, 2002).
Action immorale	L'exploitation des enfants (Mc'Donald's en Asie); viol (la crise de « Terres des hommes »); fraude (la crise d'Enron), imposture (la crise de BRE-X); tricherie (la crise des odomètres Chrysler).

Source : C. Dumitriu, 2004.

- *Les facteurs sociaux : les principales tendances démographiques et sociales, le degré de participation des citoyens.*
- *Les facteurs technologiques : les nouvelles technologies.*

Selon le même rapport, les aspects qui sont examinés lors de l'analyse en interne, sont la politique de gouvernance de l'entreprise, sa structure, ses valeurs et sa vision, le milieu de travail opérationnel, la culture relative à la gestion du risque et la tolérance des individus et de l'organisation à l'égard du risque, l'expertise en gestion du risque, et les procédures organisationnelles.

L'évaluation du contexte permet de déterminer les différentes caractéristiques des risques qui sont, d'après le rapport, les suivantes :

- ♦ *Le type de risque : technologique, financier, lié aux ressources humaines (capacité, propriété intellectuelle), santé, sécurité, etc.*
- *La source du risque : externe (politique, économique, catastrophes naturelles), interne (réputation, sécurité, gestion du savoir, information aux fins de la prise de décisions).*
- *L'objet du risque : zone d'impact ou type d'exposition (personnes, réputation, résultats des programmes, matériel, biens immobiliers).*
- *Le degré de contrôle du risque : élevé (opérationnel), moyen (réputation) ou faible (catastrophes naturelles).*

Ainsi on peut conclure que le profil de risque d'une organisation doit indiquer les principales activités à risque pouvant déstabiliser une organisation ainsi que les événements, les activités ou les projets particuliers susceptibles d'influer sensiblement et négativement sur les objectifs de l'entreprise et de l'amener dans un état de déséquilibre, soit dans une position de crise.

Figure 1

Intégration des méthodes de gestion des risques

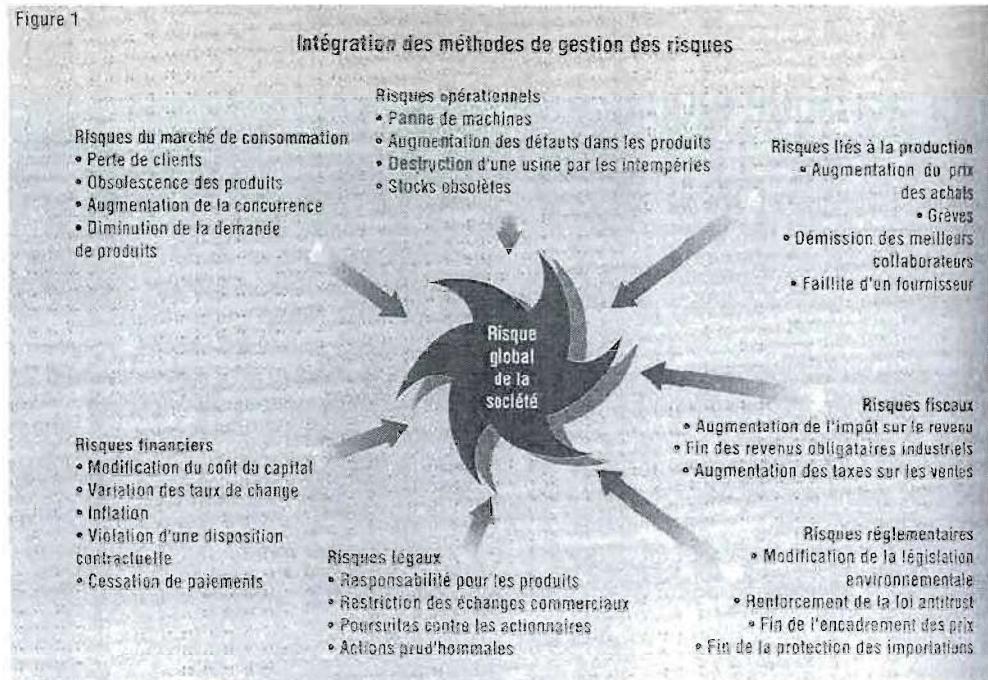


Figure 3.4 : types des risques et leurs sources

Source : Lisa Meulbroek, « Gérer le risque global », Les Échos, 2002

Il existe de multiples cartographies possibles pour réaliser le profil de risque de l'entreprise. Par exemple, Franck Moreau nous propose une autre cartographie basée sur six formes de risque. Cette cartographie définit six risques différents qui sont :

- Les risques liés à la création d'entreprise à forte croissance;
- Les risques pays;
- Les risques politiques;
- Les risques dans la gestion des ressources humaine;
- Les risques liés à la gouvernance, à l'éthique, et au développement durable;
- Les risques liés à la gestion de projet.

Michel Santi, dans un article paru dans Les Échos et intitulé « L'analyse des risques d'un business plan » 2002, présente une cartographie des risques dans laquelle il parle de *risques critiques* pour l'entreprise :

- Risques liés à l'activité : mauvaise estimation du marché, sous estimation de la compétition, etc.
- Risques stratégiques et commerciaux liés au business model : modèle d'affaire inadapté au marché et à la concurrence.
- Risques liés au personnel de l'entreprise : perte de personnel qualifié et stratégique pour l'entreprise
- Risques technologiques et techniques : erreur ou surestimations dans les choix technologiques, par exemple.
- Risques organisationnels : sous-estimations de l'importance et des coûts de l'organisation, etc.
- Risques financiers : exposition au risque de change par exemple
- Autres risques : d'ordre écologique, réglementaires etc.

Camélia Dumitriu propose une typologie des risques basée sur le système relationnel interne et externe de l'entreprise et sur l'envergure de ses opérations.

Tableau 3.4 : Grille d'analyse pour cartographier les risques .

<p>1. Risque opérationnel (d'exploitation) : le risque de perte directe ou indirecte résultant de procédures ou de processus inappropriés ou inadaptés, d'erreurs humaines ou d'anomalies liées aux systèmes, d'événements stratégiques ou d'événements externes (par exemple réglementaires, fiscaux ou comptables)- Philippe Deniau, Frank Morisano et Céline Roy-Laretry, 2001.</p>	<p>1.1 Risques reliés au fournisseur -délai d'approvisionnement; -mauvaise qualité; - le pouvoir du fournisseur.</p> <p>1.2 Risques reliés à la continuité et à la qualité des processus, des services, des opérations;</p> <p>1.3 Risque de produits défectueux (vice dans un produit dû à la conception, à l'utilisation de matières premières défectueuses, à l'absence d'un dispositif de sécurité, à un étiquetage impropre ou à une notice d'emploi mal rédigée).</p> <p>1.4 Risques reliés à l'activité logistique (entreposage, transport, distribution);</p> <p>1.5 Risque de mauvais clients (mauvaises créances);</p>
<p>2. Le risque stratégique de réseau : risque découlant du système relationnel de l'entreprise avec ses fournisseurs (y compris ses sous-traitants), ses clients, ses partenaires.</p>	<p>2.1 Les compétiteurs : risques de forte concurrence et d'érosion de l'avantage concurrentiel ; mauvaise estimation de la dynamique du marché ; erreurs sur les forces et drivers de la compétition ; sous-estimation de la compétition sur les prix (réactions des compétiteurs et arrivée de nouveaux entrants).</p> <p>2.2 La relation-client : le risque de perdre le contact avec la clientèle; perte de la capacité d'innovation; etc.</p> <p>2.3 La relation de confiance avec les investisseurs : les risques liés à la prise en compte des perceptions et des anticipations des investisseurs; le risque sur les marchés financiers, l'éventualité d'une mauvaise évaluation des investissements et des acquisitions.</p> <p>2.4 La relation avec les employés : le risque de voir partir du personnel qualifié ; le risque de « retraite massive » ; augmentation de l'absentéisme; le risque de grève; vandalisme; discrimination et harcèlement.</p> <p>2.5 La relation avec la communauté : le risque environnemental; le risque affectant la réputation de l'entreprise.</p> <p>2.6 Le risque juridique découlant des relations mentionnées.</p> <p>2.7 Le risque informationnel découlant des relations mentionnées</p>

	(divulgation des informations stratégiques, pertes de bases de données, malveillance, etc.)
3. Le risque de marché	Perte potentielle due aux variations des : - prix des matières premières ; - taux de change - taux d'intérêt
4. Le risque financier	Perte potentielle due à : - un manque de liquidité ; - un mauvais investissement ; - une utilisation défectueuse des produits dérivés (et des autres instruments financiers)
5. Le risque de crédit	Perte potentielle due à une défaillance d'une contrepartie sur une opération financière sur les termes et conditions du contrat.
6. Le risque technologique	6.1 Le risque d'accidents industriels majeurs (site fixe); 6.2 Le risque de perte de confinement relié au transport des matières dangereuses, y compris les déversements; 6.3 Les risques liés au transport des personnes (avions, trains, métro, autobus); 6.4 Le risque nucléaire; 6.5 Le risque de rupture de barrage; 6.6 Le risque des nouvelles technologies, tels que l'informatique, la biotechnologie, etc. 6.7 Le risque de surestimation dans les choix technologiques; 6.8 Le risque d'incapacité à livrer dans les temps (<i>time to develop, time to market</i>) ; 6.9 Le risque de surestimation des courbes d'apprentissage.
7. Le risque d'externalisation	7.1 Le risque lié à une dilution des responsabilités 7.2 Le risque de dépendance de partenaire 7.3 Le risque social (impliqué par le transfert de plusieurs employés) 7.4 Le risque lié à une mauvaise définition des indicateurs de qualité 7.5 Le risque d'emprisonnement face au partenaire
8. Le risque d'intégration	8.1 Risque de performance globale médiocre, même si bonne performance au niveau de chaque maillon de la chaîne 8.2 Risque de diminution « invisible » du cash-flow, car cycle de production plus long; 8.3 Risque d'inflexibilité face aux changements technologiques; 8.4 Risque d'inflexibilité face aux diverses fluctuations de la demande et face aux demandes cycliques (surtout quand les revenus dans les différents marchés ou secteurs situés en aval et en amont sont positivement corrélés); 8.5 Risque d'inflexibilité face aux changements survenus dans la

	structure du marché (augmentation du nombre de vendeurs et d'acheteurs, diminution des coûts de substitution, arrivée des fournisseurs compétitifs versus l'impossibilité de sous-traiter à moindres coûts avec tel fournisseur extérieur).
9. Le risque commercial (exportation, franchising, joint-ventures, etc.)	<p>9.1 Le risque de contrat : règlements et organismes différents de réglementation en droit commercial pour les partenaires (Europe et Amérique du Nord);</p> <p>9.2 Le risque de non-paiement;</p> <p>9.3 Le risque de transport;</p> <p>9.4 Le risque de douane;</p> <p>9.5 Le risque de défaillance de qualité.</p>
10. Le risque de changement des contextes	<p>10.1 Changement du contexte économique;</p> <p>10.2 Changement du contexte technologique (par exemple, la technologie de satellite versus la technologie de transmission par câble);</p> <p>10.3 Changement du contexte social : nouvelles valeurs sociales (comme, par exemple, l'alimentation bio, la reconsideration de la vie privée versus les objectifs de carrière, etc.); nouvelle pyramide d'âge d'une société, etc.</p> <p>10.4 Changement du contexte de marché (nouveaux drivers de la compétition);</p> <p>10.5 Changement du contexte juridique (nouvelle réglementation - par exemple, l'accord du Kyoto, nouvelle loi sur l'information, déréglementation des marchés, etc.)</p>
11. Le risque-pays Le risque-pays est composé de deux composants primaires : la capacité de payer et la volonté politique de payer. Le risque politique est associé à la volonté de payer et le risque financier et économique est associé à la capacité de payer (International Country Risk Guide)	<p>11.1 La composante politique</p> <p>11.1.1 Actes ou mesures prises par le gouvernement du pays d'origine :</p> <ul style="list-style-type: none"> - <i>la nationalisation de la propriété privée et l'expropriation des intérêts étrangers (Iran, 1979);</i> - l'imposition de restrictions légales; - le gel des actifs; - le désinvestissement; - les changements dans les politiques générales (Irak, 2003); - les changements fréquents de leadership (Roumanie); - attitude xénophobe envers les investisseurs internationaux; - les incidents liés à l'instabilité politique (coups d'Etat). <p>11.1.2 Événements internes</p> <ul style="list-style-type: none"> - la corruption et la bureaucratisation des institutions; - l'activité criminelle de l'extrémisme, le terrorisme (Algérie, 1995) et - la prise d'otages; - l'arrêt des activités dû aux grèves générales (Argentine,

	<p>1999), aux agitations populaires ou aux désordres civils (Roumanie, 1995, les actions contestataires des travailleurs dans les mines) , etc.</p> <ul style="list-style-type: none"> - l'absence de cadre institutionnel et l'inefficacité des systèmes légaux <p>11.1.3 Événements externes</p> <ul style="list-style-type: none"> - Guerre et conflits armés, (les guerres civiles africaines, la guerre au Kosovo, les conflits israélo-palestiniens) - Les influences régionales négatives <p>11.2 La composante économique et financière</p> <p>11.2.1 La mauvaise gestion économique et financière du gouvernement</p> <ul style="list-style-type: none"> - hyper-inflation et crises monétaires ; - dépréciation monétaire ; - l'absence de devises et l'inconvertibilité de la monnaie ; - défaut de paiement ; - endettement excessif fragilisant le système bancaire local ; l'impossibilité d'exécuter les contrats ; - l'impossibilité de rapatrier les profits ; - code commercial et douanier défavorisant les investisseurs étrangers. <p>11.2.2 Le risque de pays souverain</p> <ul style="list-style-type: none"> - L'État emprunteur fait défaut de paiement sur sa dette externe (le Brésil et Argentine)
--	--

(© C. Dumitriu, 2003)

Source : C. Dumitriu, «Gestion des risques et des crises : méthodes et outils», codex UQAM, 2003,2004.

La présente étude n'a pas pour vocation de démontrer la pertinence de chacune des cartographies mais de démontrer qu'il existe de multiples grilles de risque en fonction des auteurs dans la littérature.

La typologie qui sera proposée dans cette étude sera une typologie synthétique des typologies qui ont été présentées, dont celles de Lisa Meulbroek, celle de Franck Moreau et celle de Camelia Dumitriu. Meulbroek (2001) propose sept types de risques. Moreau (2002) propose comme typologie aussi sept familles de risques comme les risques liés à la création d'entreprise à forte croissance, les risques pays, les risques politiques, les risques dans la gestion des ressources humaines, les risques liés à la gouvernance, à l'éthique et au développement durable, et les risques liés à la gestion de projet. Dumitriu (2004) propose

Tableau 3.5: Cartographie des risques

Familles de risque	Description
Risques opérationnels	Liés aux activités d'une entreprise comme la panne des machines, les défauts d'un produit, les processus défectueux... Selon Dumitriu (2004) ce sont des risques reliés aux fournisseurs (dépendance vis à vis d'un fournisseur, faillite du fournisseur, mauvaise qualité des composantes, etc.), à la qualité des processus, aux activités logistiques, aux produits défectueux, ainsi que les risques liés aux mauvais clients
Risques stratégiques et économiques	Risques liés au modèle d'affaires de l'entreprise dans le marché et face à la concurrence; risques de réseaux reliés aux compétiteurs, à la relation client, à la confiance des investisseurs, à la relation avec les employés, avec les partenaires.. On incorpore dans ces risques, selon la typologie de Dumitriu, les risques d'externalisation, les risques d'intégration, les risques commerciaux et les risques liés au changement des contextes.
Risques financiers	Tous les risques d'ordre financier que ce soient les risques dus à la structure du capital, à la cessation de paiement, au manque de liquidité, aux mauvais investissements mais aussi les risques de crédit et les risques de marché liés aux taux de change,etc..
Risques fiscaux	Risques liés à la politique fiscale du pays en vigueur, que ce soit l'augmentation des taxes, la législation sur l'impôt sur le revenu, mais aussi les risques liés à une mauvaise compréhension ou application des politiques fiscales : ex. versement de dividendes excessifs à la société mère, mauvaise politique d'amortissement fiscal, etc.
Risques pays	Liés, selon la typologie de Dumitriu (2004), à la composante politique des différentes gouvernances des pays dans lesquels est implanté l'entreprise avec le lot des événements internes

	comme les formes de corruption existantes dans certains pays et comme les évènements externes concernant la stabilité politique d'un pays ou d'une région (conflit, guerre).
Risques technologiques	Liés aux technologies et aux risques d'accident industriel liés aux technologies comme les risques reliés aux transports (avions, trains, etc..), aux risques nucléaires, aux risques des technologies de l'information, les risques de surestimation de choix technologiques, aux risques liés aux défaillances du matériel technologique etc.
Risques informationnels	Liés à l'information, comme les risques reliés aux rumeurs, à la guerre de l'information, à la perte d'information stratégique, à la perte de données, à la corruption de l'information, à la propagande, à la désinformation, etc..
Risques politiques et/ou juridiques	Liés à une nouvelle législation politique, aux risques réglementaires – comme le renforcement de la loi antitrust ou la fin du protectionnisme économique – aux risques liés aux poursuites judiciaires.
Risques environnementaux	Risques environnementaux concernant l'écologie, la protection de l'environnement, les attaques d'ONG de défense de l'environnement et des animaux sur l'entreprise en fonction de son secteur d'activité (exemple pour le nucléaire, les mesures de protection de la nature et des populations suite à la catastrophe de Tchernobyl)
Risques de gouvernance	Liés à la responsabilité sociale de l'entreprise et à l'éthique des affaires (par exemple, le cas de Enron et les délits d'initiés) et aussi les risques liés à la gestion des ressources humaines.

Sources : tableau 3.4 (© C. Dumitriu, 2003) et figure 3.5 (© E. De Sablet, 2005)

3.2.6 La gestion intégrée des risques : outil pour une bonne prévention des crises

La prévention des crises et la gestion intégrée des risques mobilisent à tous les échelons le processus décisionnel d'une organisation où sont définies des lois et des réglementations, au travers d'une gestion opérationnelle. La capacité globale d'une entreprise à gérer les risques sera déterminée par des mesures de protection spécifiques mais aussi par une « culture du risque », qui est son attitude vis-à-vis du risque et de la sécurité à chaque niveau du processus. **La culture du risque se doit d'être le résultat d'un ensemble collectif de pratiques, de normes** et de lois qui incluent notamment: la manière dont est défini le risque « *acceptable* » ou « *tolérable* », le risque « *inacceptable* » ou « *intolérable* » ; les modalités de mise en oeuvre et d'application des réglementations en matière de sécurité ; les régimes d'assurance liés au risque, le droit de la responsabilité face au risque et surtout en dernier lieu la disponibilité de l'information sur les risques. L'efficacité de la gestion du risque à l'intérieur d'une gestion préventive des crises tient essentiellement à la création d'une culture de gestion de crise et d'une culture de gestion de risques qui soutiennent la stratégie, la mission et les objectifs de l'organisation. La gestion intégrée du risque doit faire partie intégrante de la stratégie globale de l'organisation. L'identification, l'évaluation et la prévention des crises à l'échelle de l'organisation permettent de saisir l'importance des risques et l'interdépendance des composantes.

Les risques peuvent survenir sur de nombreux fronts, être de haut niveau et avoir des conséquences graves; une réponse coordonnée et systématique de l'organisation doit alors être élaborée. Un grand nombre des forces actuellement perçues comme des facteurs qui accroissent les risques et les obstacles à la prévention (progrès technologique, interdépendances croissantes, extension continue des réseaux, mobilité croissante des personnes, des biens et de l'information en deçà et au-delà des frontières, approfondissement de l'intégration des marchés, etc.) offrent parallèlement des solutions utiles pour réduire les risques et prévenir les aléas. Par exemple, les technologies de sécurité avancées et de cryptologie qui permettent la correction des faiblesses des systèmes d'information et de communication ; une pollution peut être cartographiée par satellite, etc.

Dans leur ouvrage « La gestion des risques dans l'Entreprise; management de l'incertitude» 1994, Adrien Bénard et Anne-Lise Fontan proposent une méthodologie de gestion intégrée des risques selon quatre phases :

- ♦ « **L'identification et la pré-analyse** » : Cette étape vise à connaître, à analyser et évaluer toute une panoplie d'évènements qui seraient susceptibles d'entraîner un préjudice, une perturbation pouvant être à l'origine d'un état de crise.
- ♦ « **L'analyse détaillée et la quantification** » : Cette étape vise à répertorier les évènements perturbateurs potentiellement dangereux pour l'organisation. L'outil de base pour bien débuter son analyse de gestion préventive d'une crise est la connaissance de son profil de risque par une cartographie de risque spécifique à l'organisation. Puis la deuxième phase de cette étape est de pouvoir déterminer la gravité des facteurs de crise potentielle en imaginant différents scénarios, ainsi que leur probabilité d'occurrence. Ensuite le gestionnaire regroupera les risques pour les hiérarchiser en fonction de leur impact et pour déterminer si ces facteurs potentiels de crise sont tolérables ou intolérables pour élaborer une échelle des risques.
- ♦ « **Le choix des solutions de traitement** » : Cette étape définit les différentes mesures et solutions qui seront mises en l'œuvre pour contrôler le potentiel déstabilisateur d'un risque. Les mesures mises en l'œuvre détermineront le niveau de sécurité de l'organisation face à l'aléa en question. Cette phase sera déterminante car elle s'attache à trouver toutes les pistes de solutions et déterminera le meilleur équilibre possible entre toutes les possibilités.
- ♦ « **Le suivi** » : Le suivi permettra de contrôler que les mesures prises fonctionnent et réduisent le potentiel de crise et son incertitude. Les gestionnaires devront être en mesure de pouvoir réévaluer dans le temps et en fonction des avancées technologiques que les mesures soient toujours opérationnelles, et de suivre l'évolution des risques internes et externes à l'organisation.

Toutes les étapes décrites par les auteurs Adrien Bénard et Anne-Lise Fontan montrent un ensemble de tâches complexes qui déterminera le potentiel de l'organisation à contrôler et maîtriser ses risques et leurs incertitudes, pour éviter la crise comme le représente la figure suivante.

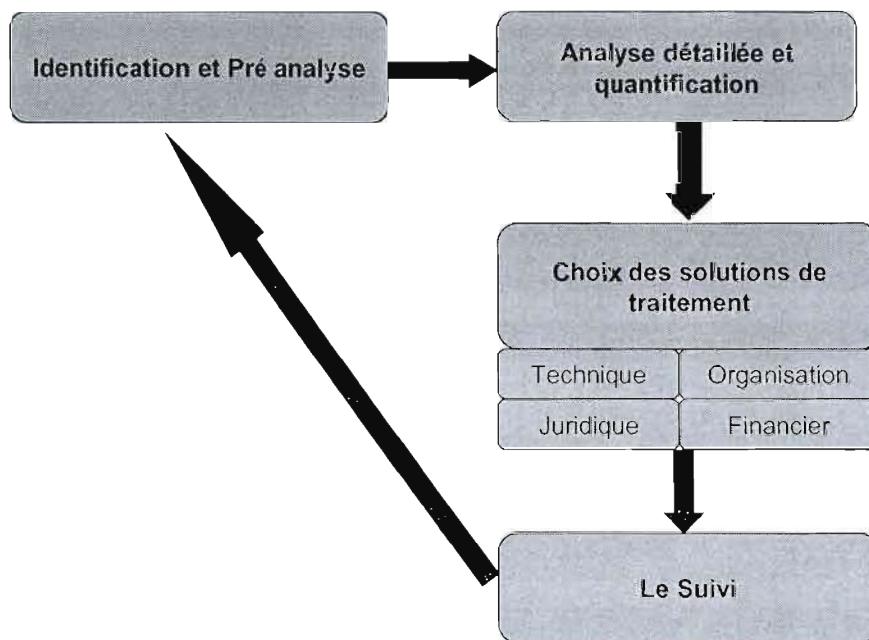


Figure 3.6: Étapes de la gestion intégrée des risques

Source : Bénard Adrien, Fontan Anne-Lise, « La gestion des risques dans l'entreprise management de l'incertitude », Eyrolles, Paris, 1994.

Depuis les années 90 de nouvelles études ont peu fini la gestion des risques pour une meilleure prévention des crises. Ainsi le rapport du Secrétariat du conseil du trésor du Canada définit quatre phases dans la gestion intégrée des risques. Ces phases sont présentées ci-après.

4.2.2 Le cycle de renseignement

Le cycle de renseignement est une méthode de gestion de l'information proposée par l'École de Guerre Économique. Il est également un instrument d'audit, parce qu'il permet de repérer les besoins critiques en informations, les pistes d'opportunités, les risques futurs potentiellement dangereux pour la survie de l'entreprise et permet de réduire l'incertitude à la prise de décision de la part des gestionnaires. Sa mise en œuvre repose avant tout sur le potentiel et le savoir humain au sein de l'entreprise car l'enjeu incontestable est le déploiement d'une culture commune et collective de l'information. L'information se définit comme tout signe ou signal qui peut être acquis, communiqué ou entreposé et qui participe de la représentation de l'environnement réel. Le cycle de renseignement est un modèle structuré autours de quatre phases importantes qui sont premièrement l'expression des besoins, deuxièmement la recherche d'information, troisièmement le traitement et l'analyse des données et quatrièmement la diffusion des informations et du savoir aux bonnes personnes au bon moment. Le cycle du renseignement est un outil d'aide à la décision et permet d'éclairer la stratégie des dirigeants. Il est un processus de transformation, d'intégration des données dans une volonté de donner du sens, et qui ambitionne d'entretenir une action ou toute décision orientée par un but et par des résultats. Le schéma suivant illustre les quatre phases ainsi que le tableau suivant.

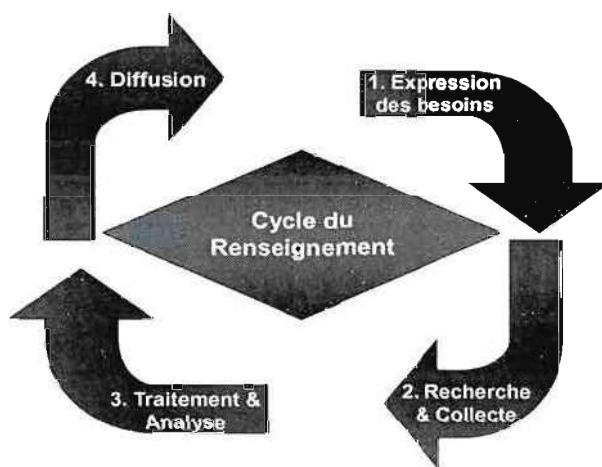


Figure 4.10 : Le Cycle du Renseignement

Source : École de Guerre Économique, Paris

1. Expression des besoins Analyse des besoins en information Déclinaison des axes de recherche Planification du processus Réexamen et réajustement possible en fin de cycle	2. Recherche & collecte Exploration des sources légales Choix des moyens de collecte Opération de recherche et de collecte
4. Diffusion de l'information Protection et Dissémination de l'information Identification des personnes cibles Organisation de la mémoire collective	3. Traitement et analyse Identification des experts internes et externes Circuit de validation Processus d'estimation, d'interprétation et de synthèse

Tableau 4.4 : Le Cycle du Renseignement

Source : École de Guerre Économique, Paris

- La première étape du cycle permet d'identifier les enjeux, et les nécessités en informations et en renseignements. Elle traduit les orientations stratégiques en axes de développement et elles sont ensuite traduites en zones de recherche et en questions opérationnelles. Elle amène donc à une planification de la recherche et de la collecte d'informations récentes, et oriente la productivité des organes de recherche. Les besoins s'expriment ponctuellement ou sont décrits comme une liste de questions adressées aux organes de collecte par les décideurs.
- La recherche et la collecte définissent la période d'action de recensement ou de recueil des informations, des sources formelles et informelles disponibles en fonction des besoins exprimés précédemment. Les unités de collecte identifient les sources d'informations.
- Le traitement et l'analyse composent la phase pendant laquelle les informations passent par un état de réflexion destiné à élaborer des conclusions stratégiques en vue

d'une prise de décision, afin de donner du sens et des connaissances nouvelles par un processus d'évaluation, d'interprétation et de synthèse. Les informations sont traitées et jugées en fonction de leur pertinence par des experts internes ou externes.

- La diffusion est la dissémination des renseignements aux organes cibles dans un format adapté à la confidentialité des données. Cette étape participe à l'organisation de la mémoire collective de l'organisation et permet une réorientation en fonction des conclusions de la première analyse ou bien à l'élaboration de nouvelles orientations stratégiques en fonction de l'évolution de l'environnement de l'organisation. Ainsi cette étape permet de recommencer un nouveau cycle pour approfondir sa connaissance de l'environnement ou définir de nouvelles pistes de recherche.

4.2.3 La veille

Tout comme le lobbying, la veille dans son ensemble est une des composantes de l'Intelligence Économique. Trop souvent on réduit la notion d'Intelligence Économique juste à celle de la veille. La veille ne fait que participer à la dynamique de l'Intelligence Économique dans la recherche d'information, de savoir et de connaissance. Seulement, elle doit s'inscrire dans un processus dynamique pour utiliser pleinement les capacités de la veille à déceler des signaux faibles et à permettre de saisir l'information qui serait susceptible de gérer les risques, de comprendre la crise et gérer une sortie de cette crise.

La veille est avant tout une démarche prospective qui vise la surveillance d'un environnement et devient un facteur clef de l'adaptation de l'entreprise face aux changements. La notion de veille est une notion qui permet d'anticiper les risques, de les prévoir et de préparer ainsi une planification de gestion des risques. Elle est donc un processus dynamique en amont des crises, puisqu'elle est avant tout destinée à repérer les risques qui seraient nuisibles pour une entreprise. Mais dès que la crise survient, la veille peut s'avérer bien utile pour aller rechercher l'information utile à la compréhension des facteurs ayant amené la crise.

4.2.3.1 Les différents types de veille dans la littérature

Dans la littérature, plusieurs auteurs qualifient plusieurs sortes de veille. Dans le cadre de cette étude, nous avons choisi la typologie proposée par E.A Pateyron présente dans «La veille stratégique» 1998, que nous avons complétée avec quelques éléments tirés de la typologie de Francart.

Dans son ouvrage, Pateyron considère cinq types de veille; la veille concurrentielle, la veille technologique et la recherche de développement, la veille sociétale, la veille environnementale, et la veille commerciale. L'information est une ressource accessible et facile d'accès par tout bon veilleur sur la toile Internet grâce aux techniques et logiciels qui permettent de chercher l'information sur le Web visible et le Web invisible ainsi que sur les autres supports. Ce qui est rare en revanche est la capacité d'analyse de cette masse d'information qui nécessite de bien formuler ses besoins afin de ne rechercher que l'information pertinente nécessaire à toute prise de décision. Toute entreprise doit savoir ce qu'elle doit observer et quels sont ses priorités et ses intérêts afin de déterminer quel genre d'information elle a besoin.

Ainsi une entreprise qui désire rester compétitive, limiter ses risques et prévenir une crise éventuelle, organisera une veille stratégique lui permettant de faire face aux différents changements de son environnement pouvant lui porter préjudice. Ainsi les besoins en information seront donc bien ciblés et les entreprises évalueront leur objectif de veille.

En ce qui concerne la **veille concurrentielle**, M. Porter énumère les différentes informations susceptibles d'être recherchées par un veilleur en cinq points :

- ◆ *Les performances actuelles du concurrent*
- ◆ *La stratégie du concurrent*
- ◆ *Les nouveaux objectifs du concurrent*
- ◆ *Les capacités du concurrent*
- ◆ *Les hypothèses qui sous-tendent l'action et les décisions du concurrent*

Pateyron énumère entre autres d'autres informations intangibles pour la veille concurrentielle, comme :

- ◆ *Les efforts fournis en recherche et développement*
- ◆ *Les relations avec de nouveaux fournisseurs*
- ◆ *Le lancement de nouveaux produits*
- ◆ *L'approche de nouveaux marchés*
- ◆ *L'attrait d'une nouvelle technologie*
- ◆ *Une nouvelle campagne de publicité*
- ◆ *L'évolution des parts de marché*
- ◆ *L'évolution des effectifs*

Cependant ce qu'il faut bien retenir dans toute veille est la nécessité de suivre dans le temps la concurrence. Cela est aussi vrai pour les autres types de veille que nous allons énumérer ultérieurement. Ainsi, selon Pateyron (1998), pour apporter une valeur à l'entreprise et l'aider à s'ajuster dans son environnement, le travail de veille « *doit être fait de manière continue dans le temps et non de façon parcellaire.* »

La veille technologique et la recherche en développement font référence à une veille qui cible toutes les questions et les problématiques liées à l'innovation d'un secteur économique. Quelles sont les nouvelles technologies susceptibles de permettre à l'entreprise de prendre l'avantage ou de perdre l'avantage face au marché ? Quelles sont les technologies que l'entreprise n'a pas décelées et dont l'absence pourrait lui coûter sa survie dans le futur ? Quelles sont les technologies qui peuvent devenir vitales ?

Cette veille technologique désigne selon Pateyron « *les efforts que l'entreprise consent à faire, les moyens dont elle se dote et les dispositions qu'elle prend dans le but d'être à l'affût et de déceler toutes les évolutions et toutes les nouveautés qui se font jour dans les domaines des technologies qui la concernent actuellement ou sont susceptibles de la concerner dans le futur* »

Toute veille technologie représente pour une entreprise un intérêt capital pour sa survie et sa croissance; ainsi, certaines entreprises ont raté des « virages technologiques » soit parce qu'elles ne connaissaient pas ou mal les nouvelles tendances du marché ou soit parce qu'elles étaient trop confiantes dans leurs technologies. En ce que concerne la première raison, on pourra prendre comme exemple le non moins célèbre virage technologique des PC que IBM avait sous-estimé. En effet IBM, trop confiant dans son produit et sa technologie d'ordinateur 360, n'a pas remarqué la nouvelle tendance qui s'ouvrait sur le marché par l'arrivée des PC, erreur stratégique qui l'a conduit à subir l'une de ses premières crises. Le second exemple que nous pourrons prendre est celui de la marque d'automobile Citroën que nous présente Pateyron dans son ouvrage. En effet cette entreprise était tellement confiante dans sa technologie et devançait tellement ses concurrents qu'elle n'a pas compris que la technologie n'était plus une priorité de vente et que cela ne répondait pas aux attentes des consommateurs. De plus après la première crise pétrolière la crise l'a conduit à la fusion avec Peugeot. Ces deux exemples qui ont été présentés brièvement nous montrent l'importance de considérer l'outil de la veille comme un moyen efficace d'anticiper les tendances du marché et d'éviter une crise qui pourrait s'avérer fatale pour la survie d'une entreprise.

La veille commerciale fait référence à la recherche, au traitement et à la diffusion de renseignements relatifs à l'évolution du marché et des clients (en vue de leur exploitation). Elle recherche les informations vitales pour comprendre les besoins des clients à long terme afin de proposer de nouvelles façons de faire innovantes et de nouveaux produits qui apporteront un avantage compétitif face au marché. La veille commerciale ou marketing consiste à surveiller, l'évolution de son marché, l'image d'une entreprise, le comportement des consommateurs, les axes de communication des concurrents les plus agressifs et les plus dangereux pour la survie d'une entreprise, les retombées d'une campagne de communication. Cette veille permet donc de pouvoir identifier de nouveaux marchés, proposer des produits nouveaux adaptés aux besoins des clients.

Dans cette approche il est nécessaire de connaître les points d'infexion stratégique du marché qui détermineront l'instant où une situation connue laisse place à un changement radical des différentes tendances. Nous pouvons prendre l'exemple de l'impact de l'Internet

sur les canaux de vente des billets d'avion. En effet il n'était plus aussi primordial pour les transporteurs de vendre des billets de vol via des agences de voyages, car ils pouvaient le faire par Internet directement, ce qui leur permettait de limiter du même coup leurs coûts et d'améliorer la relation avec la clientèle; ceci a influé sur leur décision de réduire les commissions faites aux agences. Pour les agences de voyages cette situation est des plus catastrophique si celles-ci n'arrivent pas à gérer ce virage technologique de l'Internet et à composer avec le changement dans les habitudes d'achat des consommateurs.

La veille commerciale permet aussi de suivre l'évolution en amont du marché (c'est-à-dire en direction des fournisseurs) et d'améliorer la relation avec les fournisseurs. Cette veille pourra prendre en compte les informations concernant la capacité des fournisseurs à offrir au moindre coût des produits dont l'entreprise aura besoin. Il est donc vital pour une entreprise d'analyser son marché en aval et en amont afin de saisir toutes les meilleures opportunités qui s'offriraient à elle. L'entreprise pourra ainsi satisfaire les besoins changeants de sa clientèle et prospecter vers de nouveaux fournisseurs.

La veille sociétale d'après la définition donnée par Pateyron consiste à « *discerner parmi un certain nombre de changements les grandes fractures qui s'opèrent dans la société et qui risquent de transformer ou de perturber l'entreprise et son environnement* ». Par exemple la mode est un besoin de changement constant chez les individus et toute entreprise de ces secteurs doit pouvoir gérer avec anticipation toutes les nouvelles tendances de la société sous peine de disparaître. Cette définition nous explique bien le rôle stratégique d'une veille dans certains secteurs d'activités qui sont sensibles aux aléas de la société environnante. Cette veille permet donc de limiter les risques et de prévoir une crise éventuelle si l'entreprise n'a pas ou mal répondu aux demandes du marché en fonction des nouvelles tendances de mode.

La veille environnementale dans sa définition donnée par Pateyron comprend les moyens mis en œuvre pour surveiller l'environnement d'une entreprise. Souvent les stratégies misent en place sont confrontées à de nouveaux types de risque face aux changement de l'environnement qu'il soit politique, sociétal, ou environnemental. Les

entreprises qui seront les plus performantes et qui limiteront les risques d'incertitude sont celles qui réussiront à se distinguer par leur observation du monde extérieur et par leur capacité à gérer les informations par « *zones clefs à surveiller* » (Pateyron, 1998)

Dans la littérature scientifique la notion de **veille juridique** est définie comme étant la recherche, le traitement et la diffusion (en vue de leur exploitation) de renseignements relatifs à la législation et la réglementation. Cette veille consiste à surveiller les lois et décrets, la jurisprudence, les débats parlementaires, les propositions de lois, les propositions patronales, la fiscalité. La veille juridique permet donc d'anticiper tout changement lié à l'adoption d'un texte de loi, et de pouvoir pénétrer des marchés étrangers soumis à des règles nationales spécifiques, en toute légalité.

A part ces grandes catégories de veille, on trouve dans la littérature scientifique la notion de **veille brevet** qui fait référence à la recherche, le traitement et la diffusion de renseignement relatifs aux brevets, marques, modèles déposés afin d'éviter toute copie et tout piratage. Elle consiste à surveiller les brevets déjà déposés, les entreprises dépositaires de brevets, la capacité de l'entreprise à protéger son patrimoine contre la concurrence, contre la contrefaçon et aussi les stratégies de protection de la part des concurrents concernant la propriété intellectuelle.

Toujours comme complément à cette typologie, Loup Francart nous propose, dans son ouvrage « Infosphère et intelligence stratégique », une typologie de veilles qui s'inspire de la veille politico militaire, que nous présentons dans le schéma suivant.

ci se manifeste à un moment précis et nécessite une recherche d'information pour sa compréhension globale au moment de son irruption. Mais par contre en fonction des thèmes ciblés par les veilleurs selon la crise, la phase de la veille de crises sera aussi celle d'une veille occasionnelle.

Notre démarche d'étude aide à formuler les questions suivantes afin d'aider à l'expression des besoins en information dans une situation d'urgence :

- ◆ Quelles sont les causes de la crise ?
- ◆ Quels sont les événements déclencheurs de la crise ?
- ◆ Quel est le type de crise ?
- ◆ Quelles sont la phase et la portée de la crise pour l'entreprise ?
- ◆ Quelles sont les parties prenantes de la crise ? Concurrents, opposants, alliés...
- ◆ Quels sont les acteurs de la crise ?
- ◆ Quels sont leurs intérêts ?
- ◆ Quel est l'état de l'opinion publique ?
- ◆ Quelle peut être la position de l'Entreprise face à la crise ?
- ◆ Existe-t-il des scénarios de crise prévus dans l'entreprise ?
- ◆ Y a-t-il eu d'autres crises du même genre dans le passé et comment ont-elles été gérées ?
- ◆ Y a-t-il des signaux faibles avant coureurs de crise qui n'ont pas été décelés?
- ◆ Quelles sont les valeurs remises en cause ?
- ◆ Quelles sont les conséquences possibles des dégâts de la crise ?

4.2.3 Le Benchmarking

Le *benchmarking* est une méthode qui a été développée au début des années 80 par la société Xerox pour une prise de décision concernant un investissement lourd destiné à moderniser la gestion des stocks. Xerox s'est intéressé alors aux "meilleures pratiques de la concurrence" mais également aux pratiques dans d'autres secteurs sur le sujet étudié. La comparaison s'est finalement faite avec une firme de vente d'articles de sport par correspondance qui excellait pour la gestion des commandes. David Kearn, l'ex-directeur de Xerox, a défini le

benchmarking comme « un processus continu et systématique d'évaluation des produits, des services et des méthodes, par rapport à ceux des concurrents ou des partenaires des plus sérieux ou des organisations reconnues comme leaders ou chef de file.»

L'idée de base dans la démarche de *benchmarking* est de faire des comparaisons entre le processus utilisé dans une organisation et le processus utilisé dans une autre organisation plus performante. Le but de cet comparaison est de pouvoir fixer de nouveaux objectifs et de modifier le processus afin de le rendre optimum. L'étalonnage repose sur un échange d'information avec les entreprises réputées excellentes de leur domaine. Il se définit comme l'effort à accomplir pour trouver et mettre en œuvre la meilleure pratique au sein d'une organisation.

Selon une étude « Benchmarking : the missing link between evaluation and management », 1998 de Emilio Patarelli et Eric Monnier il existe trois types les plus importants de Benchmarking ; le *benchmarking concurrentiel*, le *benchmarking interne*, le *benchmarking générique*.

Le *benchmarking interne* se pratique à l'intérieur d'une organisation. Dans de grandes entreprises des processus similaires se retrouvent dans différents départements et il est ainsi aisés de faire des comparaisons afin de déterminer le meilleur des processus. Les partenaires sont normalement faciles à identifier mais seulement il est difficile de trouver des sources d'amélioration significative pour toute l'organisation de l'entreprise et d'universaliser la meilleure pratique.

Le *benchmarking concurrentiel* se réfère à une entreprise externe, généralement un compétiteur qui excelle dans son domaine. La comparaison et l'évaluation s'effectuent souvent dans des domaines d'activités similaires. Les bénéfices de ce *benchmarking* sont souvent très importants mais il faut faire attention au partage et aux données confidentielles.

Le *benchmarking générique* est la démarche qui consiste à se comparer aux entreprises les plus excellentes ayant des processus similaires et ce, quelque soit leur domaine d'activité. Il

est important de souligner que certains processus sont similaires quelque soit l'industrie et qu'il peut être fort judicieux de pouvoir comparer ces processus, dits génériques, d'un secteur à l'autre.

François Jakobiak propose une typologie plus large, comprenant quatre types de *benchmarking*. Les termes utilisés sont assez similaires. Cependant François Jakobiak définit dans son modèle ci-dessous non pas un *benchmarking* générique mais il différencie dans tout ce qui est générique ce qui est de l'ordre des fonctions génériques et ce qui de l'ordre des processus identiques et ce, quelque soit le secteur d'activité.

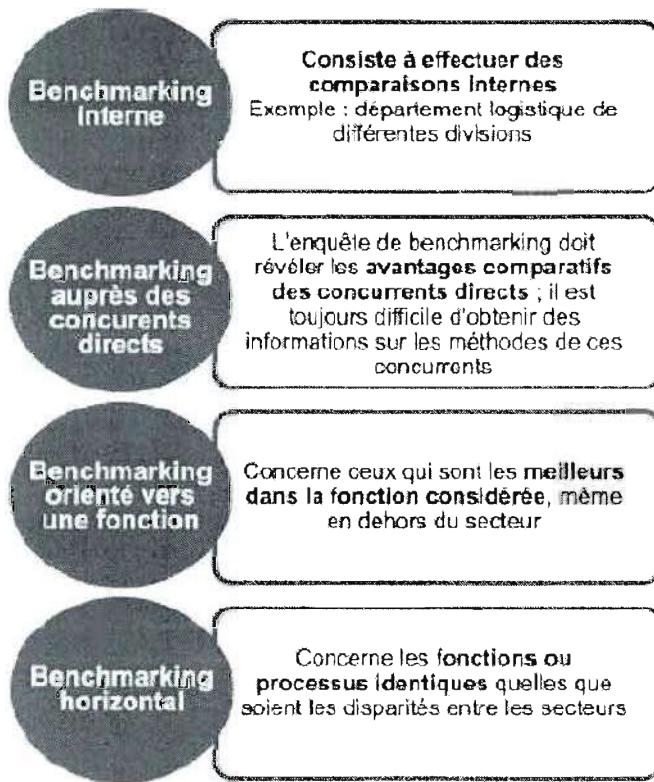


Figure 4.12 Les 4 Types de Benchmarking

Source: Jakobiak François, «L'Intelligence Économique en pratique», Éditions Organisation, 1998

La démarche de *benchmarking* peut se dérouler selon le rapport « benchmarking : the missing link between evaluation and management » de Emilio Patarelli et Eric Monnier par étapes tel que :

- ◆ Sélectionner ce qui doit faire l'objet du *benchmarking* (ce qui doit être amélioré)
- ◆ Identifier les partenaires du *benchmarking* (points de référence)
- ◆ Collecter et organiser les données
- ◆ Déterminer l'écart concurrentiel en comparant avec les données internes
- ◆ Fixer les futurs niveaux de performance (objectifs)
- ◆ Communiquer les résultats du *benchmarking*
- ◆ Elaborer des plans d'action
- ◆ Mettre en place des actions concrètes (gestion de projet)
- ◆ Contrôler la progression

Cependant afin de simplifier la démarche, le *Benchmarking* peut se dérouler en quatre grandes phases : **l'auto-diagnostic et l'identification** des cibles et des objectifs; **la collecte des informations; l'adaptation et le déploiement**, ce qu'on peut appeler le *post-Benchmarking*; et enfin **l'observation des résultats et les ajustements possibles**.

En réalité la première phase, c'est-à-dire l'auto-diagnostic et l'identification des cibles, vise à analyser les processus internes de l'entreprise et permet de saisir les indicateurs essentiels à la mesure de ses performances. Ensuite l'identification vise à repérer le ou les concurrents qui pratiquent au mieux le processus analysé. Il s'agira d'analyser les objectifs à atteindre, de connaître les partenaires et de pratiquer un partage des informations. La seconde phase, qui est la collecte des informations, vise à la recherche des informations réalisée grâce à la comparaison chez les partenaires du *Benchmarking*, et ensuite d'analyser les actions susceptibles d'être mises en œuvre dans l'entreprise. La troisième étape vise à adapter à l'organisation, les concepts, les processus, les fonctions permettant d'améliorer la performance de l'organisation. Enfin la dernière étape est destinée à estimer les améliorations, les progrès réalisés et les résultats obtenus par la suite des améliorations apportées. Cette étape est aussi destinée, si l'organisation n'a pas réussi à atteindre ses

global d'urgence, il est cependant l'un de ceux qui doit être établi selon une infrastructure précise, par les plus hauts responsables habilités à prendre des décisions rapides.». Il existe une multitude de risques de différentes sortes que chaque entreprise cherche à résoudre et à maîtriser dans un plan de compréhension de crise, dans un plan d'action de sortie de crise dans laquelle l'organisation ne devra pas oublier un volet communication. Ce volet communication sera le reflet de son action, de sa crédibilité et de son image sur l'opinion publique et les consommateurs.

Face au nouveau contexte de la diffusion et de la recherche d'information par Internet, l'information devient accessible rapidement et par tous, l'information s'amplifie contribuant à ce que la notion de communication de crise dans la démarche d'Intelligence Économique devienne d'une importance capitale. Cependant la communication de crise nécessite une grande prudence au niveau de la perception des masses, car la communication en tant de crise a un rôle d'influence énorme auprès des médias et sur Internet et ce rôle a pour objectif de conserver une perception positive de l'organisation malgré la crise. De plus l'opinion publique a une grande influence sur la communication de crise et est devenue la référence dans toutes les actions de communication.

4.2.6.1 Stratégies de communication de crise

Faute de stratégie de communication précise, faute de préparation et d'analyse de la situation, faute de temps, l'entreprise risque de voir son image de marque se délabrer. "Aujourd'hui on dissout la crise dans la communication au lieu de focaliser sur la gestion de la crise en tant que telle pour la résoudre, explique Patrick Lagadec (1991). L'agitation médiatique va donc à l'encontre des défis qui s'imposent à l'entreprise sur le plan de la gouvernance."

Malgré tout, la communication seule ne suffit pas à sortir une entreprise de la crise. En effet les médias s'étant emparés d'un scoop, ils peuvent utiliser leur pouvoir d'influence pour s'emparer des rumeurs, des fuites et porter un coup fatal à l'organisation. L'entreprise se doit donc d'être réactive afin de limiter les conséquences. Cependant celle-ci doit savoir ce qui se dit, quelles sont les rumeurs, les craintes des consommateurs, la position des médias afin de

mieux répondre aux atteintes et assurer une stratégie de contre-influence. Ce rôle sera dévolu à la composante veille de la cellule de crise mise en place par l'organisation pour la recherche d'information sur les rumeurs et les attentes. La communication de crise est un domaine d'étude sur lequel les certitudes sont faibles. De plus certaines stratégies de communications de crise fonctionnent dans des organisations et pas nécessairement ailleurs, parce que le contexte diffère en fonction du temps, des contingences et des tendances du moment. Une crise pétrolière n'a plus le même impact au 21^{ème} siècle qu'au 20^{ème} siècle. Selon Didier Heiderich, les entreprises disposent de plusieurs stratégies de communication. Elles peuvent reconnaître les faits, nier les faits, c'est-à-dire faire obstruction, ou bien faire une diversion.

La première stratégie qui s'intitule « **la reconnaissance** », consiste à accepter l'existence de la crise le plus rapidement possible. "Dans cette stratégie, explique Didier Heiderich, si la presse dévoile la crise en devançant l'entreprise, c'est que la communication de celle-ci est mauvaise et que la crise ne lui appartient déjà plus. Pour mener l'opération, l'entreprise doit donc aller vite et être en mesure de déterminer rapidement si elle est compétente par rapport au moteur de la crise. Ce moteur peut être interne, par exemple lié aux produits de l'entreprise, ou externe, par exemple lié à un contexte politique. Dans chacun des cas, l'axe de communication ne sera pas le même." Pour être totalement efficace, cette communication nécessite une grande clarté. Elle permet de jouer sur la transparence et d'acquérir une certaine crédibilité auprès de l'opinion publique. Cette stratégie vise à admettre sa responsabilité, à montrer son incompréhension, à délester certains responsables en le désignant comme coupable ou bien à élargir la responsabilité à d'autres acteurs afin de partager les torts.

La deuxième stratégie, **la diversion**, consiste à changer l'angle de vue de la crise auprès des médias et de l'opinion publique. "Mais elle doit pouvoir être fondée sur la réalité et des faits concrets pour réussir à déplacer le lieu de débat", précise Didier Heiderich. L'objectif de cette stratégie est de pouvoir déplacer le débat à l'extérieur de l'entreprise. Cette stratégie vise à riposter en insistant sur ceux qui profitent de la situation, à renvoyer la responsabilité à l'extérieur, ou bien à appuyer sur le fait que le pire a été évité.

La troisième stratégie, **le refus de la crise**, consiste à nier l'évidence et à refuser tout état de crise dans l'organisation. « Le tout va très bien madame la marquise... ». Cette stratégie consiste à minimiser l'effet de la crise, à garder le silence pour ne pas entretenir les rumeurs et ne pas alimenter la crise, ou bien à ne pas communiquer dès le début de la crise. Par contre, si avec le temps qui passe, les nouvelles informations contredisent ou appuient la culpabilité de l'organisation, cette stratégie peut avoir de réels impacts négatifs sur son image et sa réputation. Souvent la firme risque de perdre sa crédibilité face à l'opinion publique et les médias.

4.2.6.2 Plan de communication de crise

Cependant bien avant de définir une stratégie en particulier, la conception du plan de communication en période de crise sera définie sous forme de programme qui guidera la communication de l'entreprise vers les médias. Cette communication nécessite un programme rigoureux, réaliste et efficace. Dans ce programme de communication de crise, toute organisation, pour un meilleur résultat s'appuiera sur des personnes clefs qui seront chargés de diffuser les différentes informations et communiqués. Le programme doit comporter une liste détaillée des différents canaux de distribution de l'information comme les différents médias, l'opinion publique au travers des médias sélectionnés, les agences gouvernementales, les différents canaux de distribution à l'intérieur de l'organisation, et les actionnaires, afin de leur faire renouveler leur confiance dans la firme. Les étapes du programme devront comporter des éléments d'une importance capitale, selon la Présidente et directrice générale Hill & Knowlton – Ducharme Perron, qui sont les suivants :

- Identification du scénario du pire
- Identification des forces et faiblesses de l'entreprise ou de l'organisme, tant au plan technique que communicationnel
- Inventaires des ressources, tant humaines que matérielles
- Choix d'un centre de décision
- Disponibilité de l'information de base
- Identification d'un ou des porte-parole

Les Etudes de Cas avec Corrigées

Étude de Cas : *Gestion des Risques chez "TechPrint"*

TechPrint est une imprimerie numérique spécialisée dans l'impression rapide de documents publicitaires, de brochures, de flyers et de supports pour des événements (salons, conférences, etc.). L'entreprise se distingue par son utilisation des dernières technologies numériques pour répondre à la demande croissante de tirages à faible coût et en délais réduits. Elle utilise des presses numériques de dernière génération pour garantir des impressions de qualité à grande vitesse, avec un système de gestion des commandes et des stocks informatisés.

TechPrint est située dans une zone industrielle d'une grande ville européenne, avec une clientèle diversifiée allant de petites entreprises locales aux grandes sociétés.

Récemment, *TechPrint* a rencontré plusieurs problèmes qui ont perturbé son activité, nécessitant une gestion efficace des risques pour assurer sa pérennité. Ces défis se résument comme suit :

- ✓ *TechPrint* dépend fortement de ses machines pour assurer une production rapide. Récemment, l'entreprise a rencontré des pannes imprévues sur certaines de ses presses numériques. Ces pannes ont entraîné des retards importants dans la production, affectant la satisfaction client et la réputation de l'entreprise. (**Impact: Critique, Probabilité: élevé**)
- ✓ Les opérateurs de machines n'ont pas reçu de formation régulière sur les nouvelles technologies et les mises à jour des logiciels (**I: Moyen , P: Elevé**)
- ✓ L'entreprise a observé une concurrence accrue de la part d'autres imprimeries qui adoptent des modèles d'affaires innovants, comme la personnalisation en ligne et l'impression écoresponsable. Cela met en danger sa position sur le marché. De plus, *TechPrint* peine à diversifier ses services au-delà de l'impression traditionnelle. (**I: élevé, P: élevé**)
- ✓ *TechPrint* n'a pas encore développé d'autres services que l'impression traditionnelle. Cette absence de diversification rend l'entreprise vulnérable aux fluctuations du marché et à la concurrence. (**I : élevé, P : moyen**).
- ✓ Les systèmes informatiques de *TechPrint* sont relativement anciens et vulnérables aux cyberattaques. L'entreprise gère des données sensibles de clients, y compris des informations bancaires et des commandes spécifiques. Bien qu'aucune cyberattaque majeure ne se soit produite jusqu'à présent, le risque demeure élevé, en particulier avec l'augmentation des menaces dans le secteur. (**I: critique, P:moyen**)
- ✓ Les presses numériques, bien qu'efficaces, sont des équipements coûteux et complexes. *TechPrint* a récemment observé une baisse de performance de ces machines, en raison d'une maintenance irrégulière. Les coûts de réparation sont élevés, et la durée de vie des machines semble réduite, ce qui met l'entreprise sous pression financière. (**I: élevé, P: élevé**)
- ✓ Les réglementations environnementales concernant la gestion des déchets de papier et l'utilisation d'encre non toxiques sont de plus en plus strictes. Toutefois, *TechPrint* n'a pas encore pris de mesures concrètes pour réduire son empreinte carbone. Cela pourrait affecter ses relations avec des clients soucieux de l'environnement. (**I: moyen, P: moyen**)

T.A.F: Entant que Risque Manager, on vous demande de :

- 1) a)** Proposez une cartographie des risques (Matrice des risques) adaptée à l'entreprise "*TechPrint*".
b) Expliquez en quoi la cartographie des risques est un outil stratégique pour une entreprise comme "*TechPrint*". Quelle est son utilité dans le processus de gestion des risques ?
- 2)** En vous basant sur la cartographie des risques (Matrice des risques) que vous avez préparé pour "*TechPrint*", hiérarchisez les risques par ordre de priorité en justifiant votre classement selon l'impact et la probabilité.
- 3)** Proposez des actions et des recommandations managériales pour gérer efficacement les risques identifiés chez "*TechPrint*".
- 4)** Selon vous, quels risques pourraient avoir un effet Domino (cascading effect) sur d'autres risques ? Donnez un exemple concret dans le cas de "*TechPrint*".

Corrigé Etude de Cas : *Gestion des Risques chez "TechPrint"*

Nombre pages : 5

Tableau synthétique des risques : Justification Impact/Probabilité

Risques	Impact	Justification Impact	Probabilité	Justification Probabilité
Panne de machines	Critique	Arrêt total de production, coûts très élevés	Élevée	Machines très sollicitées, pannes fréquentes
Manque de formation continue	Moyen	Erreurs réparables, pas d'arrêt total	Élevée	Formation insuffisante, erreurs humaines fréquentes
Concurrence accrue	Élevé	Risque majeur de perte de parts de marché	Élevée	Marché très concurrentiel, pression sur les prix
Mauvaise diversification des services	Élevé	Vulnérabilité à moyen terme, dépendance à un seul service	Moyenne	Marché stable actuellement mais susceptible d'évoluer
Cyberattaque	Critique	Atteinte grave à la réputation, pertes financières	Moyenne	Secteur numérique ciblé, aucune attaque majeure à date
Baisse de performance des machines	Élevé	Production ralentie, coûts de maintenance élevés	Élevée	Machines vieillissantes, maintenance insuffisante
Non-conformité environnementale	Moyen	Sanctions possibles, image affectée	Moyenne	Pas de mesures concrètes prises, risque d'infraction modéré

Réponses aux Questions :

Q1 :

a) On présente ci-dessous une cartographie des risques adaptée au Tech Print :

Famille des Risques	Description des Risques	Impact	Probabilité	Niveau de Risque
Risques Opérationnels	Panne de machines	Critique	Élevée	Très élevé
	Manque de formation continue	Moyen	Élevée	Modéré
Risques Stratégiques	Concurrence accrue	Élevé	Élevée	Très élevé
	Mauvaise diversification	Élevé	Moyenne	Élevé
Risque Informationnel	Cyberattaque	Critique	Moyenne	Élevé
Risque Technique	Baisse performance machines	Élevé	Élevée	Très élevé
Risque Environnemental	Non-conformité environnementale	Moyen	Moyenne	Modéré

b) Pour une entreprise comme "TechPrint", la cartographie des risques présente un outil stratégique et une étape clé dans le processus de gestion des risques. Son utilité se manifeste sur plusieurs niveaux :

- ✓ Elle permet d'identifier les risques selon leur niveau de gravité (impact) et leur probabilité.
 - ✓ Elle aide à hiérarchiser les risques et à prioriser les actions : On se concentre sur les risques les plus critiques ou les plus probables.
 - ✓ Elle facilite la prise des décisions et le pilotage des plans d'actions. (Propositions des solutions et des recommandations).
 - ✓ Elle permet de communiquer efficacement les risques aux dirigeants et aux équipes opérationnelles.
- Dans le cas de Tech Print, cette cartographie des risques permet de se focaliser sur les pannes de machines, la concurrence et les Cyberattaques qui ont un fort potentiel de perturbation.

Q2 :

On vous présente ci-dessous une hiérarchisation des risques par ordre de priorité en justifiant ce classement selon impact et probabilité :

1. Panne de machines (Priorité : Critique)

- Le risque d'une panne majeure des machines est critique, car il entraînerait des arrêts de production qui affecteraient directement la satisfaction client et la rentabilité. La probabilité est élevée, car ces équipements sont utilisés en continu.

2. Concurrence accrue (Priorité : Très Élevée)

- L'augmentation de la concurrence dans le secteur est un risque majeur pour *TechPrint*. La probabilité est élevée, et le risque d'érosion des parts de marché est imminent.

3. Baisse de performance des machines (Priorité : Élevée)

- La dégradation des performances des machines est fréquente avec le temps et l'usage. Cela représente un risque élevé en termes de production et de coûts, d'où la nécessité d'une maintenance préventive.

4. Cyberattaque (Priorité : Élevée)

- Bien que la probabilité soit modérée, l'impact d'une cyberattaque serait critique. Il est impératif de renforcer la cybersécurité de l'entreprise pour protéger les données sensibles.

5. Mauvaise diversification des services (Priorité : Moyenne)

- Bien que l'absence de diversification expose *TechPrint* à un risque stratégique, il peut être géré à moyen terme. Le développement de nouveaux services doit être envisagé pour se maintenir compétitif.

6. Manque de formation continue du personnel (Priorité : Moyenne)

- Le manque de formation peut entraîner des erreurs humaines, mais ce risque reste moins immédiat que d'autres, à moins qu'il ne conduise à des pannes graves ou à des erreurs répétées.

7. Non-conformité environnementale (Priorité : Faible)

- Ce risque est modéré à long terme. Même s'il peut entraîner des amendes, il n'impacte pas immédiatement la production ou la rentabilité de *TechPrint*.

N.B : Toute autre proposition d'hiérarchisation des risques selon un autre ordre de priorité restait possible (acceptée) tant que la justification est objective et convaincante !

Q3 :

Entant que Risque Manager, on pourra proposer quelques recommandations managériales qui permettraient de contrecarrer ces risques et de les gérer de manière efficace :

Risques par ordre de priorité	Recommandations / Solutions
Panne de machines	Mettre en place un Plan de maintenance préventive régulier , formation du personnel pour détection précoce des signes de pannes, Investir dans des équipements de rechange ou un parc machine supplémentaire.
Concurrence accrue	Analyse de marché (les concurrents) pour adapter les prix et les services, diversification des services, amélioration de la relation client via un service personnalisé
Baisse performance machines	Entretien régulier et remplacer les pièces usées, renouvellement du matériel par un autre plus moderne et plus performant , Monitorer la performance en temps réel via des outils connectés
Cyberattaque	Renforcer la sécurité du système d'information (firewalls, antivirus, pare-feu), sensibiliser le personnel aux risques cyber attaques, Mettre en place des pratiques de sauvegardes régulières des données.
Mauvaise diversification	Étudier le marché pour identifier de nouveaux services à proposer (ex : impression 3D, services graphiques) ; Investir dans l'innovation et la R&D. Collaborer avec des partenaires complémentaires
Manque de formation continue	Organiser des sessions de formation régulières sur les nouvelles technologies. Mettre en place un programme de formation continue obligatoire. Encourager le partage de bonnes pratiques entre employés (apprentissage du métier).
Non-conformité environnementale	Réaliser un audit environnemental. Mettre en place des actions pour réduire les déchets et émissions (recyclage, traitement des déchets chimiques). Former le personnel aux normes environnementales.

Q4 :

Dans le cas de "TechPrint", on vous propose ci-dessous deux exemples de risques qui pourraient avoir un effet Domino (cascading effect) sur d'autres risques :

- ❖ **Effet Domino 1** : Une panne majeure des machines pourra entraîner des retards de production et par la suite des retards de livraison. Cela risquerait l'entreprise à perdre des clients face à la concurrence. (*Domino entre risque opérationnel et stratégique*).
- 8. **Effet Domino 2** : Une mauvaise gestion de la cybersécurité peut non seulement causer un piratage de données (notamment informations confidentielles sur les clients) mais elle pourra aussi menacer la confiance des clients, ce qui impacte à son tour la stratégie commerciale. (*Domino entre risque informationnel et stratégique*).

N.B. D'autres risques à effet domino sont aussi envisageables !

Entretien avec Marc Chatelard

(Senior vice-président Transport Asie-Pacifique, Groupe Alstom)

Intelligence économique, patrimoine informationnel de l'entreprise et stratégie internationale

Propos recueillis par Michel-Henry Bouchet

M. H. B. : Quelle définition donnez-vous de l'IE

M. C. : Pour moi l'intelligence économique consiste à évaluer la solidité de mon environnement – mes clients, partenaires, fournisseurs, concurrents –, donc en bref, de tous les acteurs qui peuvent avoir une influence sur nos activités.

M. H. B. : Existe-t-il une structure de l'IE et de la gestion des risques chez Alstom ? Est-elle incorporée dans un département recherche ou un département risque-pays, ou est-elle séparée ?

M. C. : Il existe une structure séparée d'intelligence économique chez Alstom. Elle est intégrée à notre département Stratégie. L'intelligence économique est en effet un élément déterminant de la stratégie de l'entreprise. Cette entité n'est pas intégrée à la structure qui gère les risques-pays qui, elle, dépend de notre direction financière.

M. H. B. : Pensez-vous subir un risque lié à votre système d'information formel ou informel ? Le système d'IE est-il prévisionnel sur le très long terme (quinze-vingt ans ?)

M. C. : Toute activité comporte sa part de risque. Dans une entreprise de biens d'équipements comme la nôtre, le risque est néanmoins plus grand sur les activités industrielles que sur le système d'information qu'il soit formel ou informel. Il faut cependant rester vigilant. Les facteurs économiques que nous gérons sont en général à plus court terme que quinze-vingt ans, les retournements sont fréquents, les bouleversements sont plus rapides. Nous n'avons donc, il faut le reconnaître, que peu de vision à si long terme.

M. H. B. : Comment définissez-vous le patrimoine informationnel de l'entreprise ?

M. C. : L'ensemble de la connaissance accumulée au fil des ans. Dans une entreprise de longue tradition comme la nôtre, nous devons veiller à garder une mémoire. La gestion du patrimoine informationnel est donc importante. Notons cependant que le recours formel au patrimoine ancien est rare. L'action quotidienne est plus basée sur la mémoire récente.

M. H. B. : Que faites-vous pour protéger et sécuriser ce patrimoine ?

M. C. : Nous avons un système de gestion en place basé, lorsqu'il s'agit d'informations sensibles, sur un double archivage. La difficulté réside plus à s'assurer que les nouveaux venus soient avertis de l'existence de ce patrimoine et qu'ils en fassent bon usage.

M. H. B. : Quelle est l'importance de l'intelligence économique dans la stratégie de gestion des risques de la société Alstom ? Est-ce une priorité récente ?

M. C. : C'est une préoccupation quotidienne dans une entreprise comme la nôtre. Elle a pris une importance croissante depuis que nous avons renforcé la gestion des risques, soit depuis trois ans environ.

M. H. B. : Intelligence économique et organisation institutionnelle : comment l'IE est-elle organisée et gérée au sein de la société Alstom ?

M. C. : Chaque secteur (énergie et transport) a son propre système de veille puisque les environnements qui les entourent sont différents. Au niveau de l'information, le recueil est l'affaire de tous, les informations sont remontées à un point de contact unique qui en fait la synthèse.

M. H. B. : L'IE représente l'ensemble des techniques visant à apporter des informations à l'organisation, ainsi qu'à prévenir les menaces directes ou indirectes contre l'organisation : comment s'articulent la veille informationnelle et la stratégie ?

M. C. : Comme je l'ai dit précédemment, la veille informationnelle fait partie de notre département stratégie. C'est la reconnaissance même de son importance dans notre entreprise.

M. H. B. : Au-delà de l'accès à l'information, le défi consiste à élaborer une gestion coordonnée de la recherche, du traitement, de la diffusion et de la protection de l'information. L'intelligence économique est donc au cœur de l'analyse et de la gestion des risques-pays : comment Alstom lie-t-elle IE et stratégie internationale ?

M. C. : L'équipe IE diffuse trimestriellement une synthèse des informations collectées à ses équipes commerciales internationales, qui les prennent en compte dans leur stratégie.

M. H. B. : IE, information et désinformation : Alstom a-t-elle été confrontée à des attaques de désinformation ? Comment a-t-elle procédé pour y faire face ?

M. C. : Une des règles de base de l'information récupérée est de la confirmer par une deuxième source indépendante. Il est fréquent de récupérer des informations erronées, que ce soit intentionnel ou non. Les informations les plus sensibles sont en principe vérifiées. Le tout-venant est classiquement moins stratégique, on prendra alors l'information avec prudence.

Cas n° 2 : manipulation de l'information et motivation économique

La déstabilisation de l'industrie aquacole norvégienne de saumon

Au début de l'année 2005, le cours du saumon d'élevage s'effondre brutalement à la suite d'une étude publiée dans la revue scientifique *Sciences*. Les conclusions des recherches dirigées par le professeur David Carpenter tendent à prouver que la consommation régulière de saumon d'élevage développe les probabilités de cancer chez les populations à risques : femmes enceintes, enfants et personnes âgées. Objet de débat quant à la crédibilité d'une telle étude, « le cas du saumon » est d'abord l'objet d'une manipulation sous forme d'une opération d'information destinée à empêcher la conquête du marché américain par les industriels norvégiens. Le marché du saumon commence à croître à partir de 1982. À cette époque, l'industrie mondiale de la pêche représente 500 000 tonnes par an, celle de l'aquaculture ne s'élève qu'à 100 000 tonnes. En l'an 2000, les volumes de production se sont inversés. L'aquaculture pèse désormais 1,5 million de tonnes par an tandis que la pêche de saumon sauvage ne dépasse pas le million de tonnes. La compétition est devenue mondiale. Elle oppose la confédération des pêcheurs de l'Alaska à la Norvège, leader mondial de la production du saumon d'élevage dont les bénéfices croissent à hauteur de 15 % par an. En 2004, différents facteurs non économiques font chuter le cours du saumon de l'Alaska, au moment où les Norvégiens dévoilent leur ambition de conquête du marché domestique américain. Malgré une taxation de 26 % sur l'importation du saumon scandinave décidée par l'administration fédérale américaine, les cours demeurent en faveur des Européens.

La fondation *Pew Charitable Trust* dont trois membres du conseil d'administration sont directement partie prenante dans les intérêts des pêcheurs du Pacifique Nord est l'acteur central de ce cas, puisqu'elle vote au printemps 2003 le financement de l'étude réalisée par des chercheurs de l'université d'Albany. Ce travail fera l'objet d'un relais médiatique sans commune mesure grâce aux actions d'une grande agence américaine de relations publiques. Toutes les rédactions des grands médias internationaux ont reçu, outre l'étude, un argumentaire contre le saumon d'élevage. Au-delà du débat scientifique et de la crédibilité du travail de recherche, la manipulation de l'information s'est surtout concentrée sur la plausibilité des conclusions. Les démentis argumentés quant à l'intérêt du principe de précaution ont été suivis de peu d'effet à court terme, même si le boycott inconscient des populations européennes n'aura duré qu'un trimestre. L'effet final recherché était autre. Pareillement, la déstabilisation de l'industrie chilienne du saumon d'élevage quelques années auparavant visait à créer des barrières invisibles à l'entrée. L'opération d'intoxication probablement commanditée par les pêcheurs de l'Alaska cherchait également à interdire aux Norvégiens la pénétration de leur marché national. En ce sens, elle fut couronnée de succès.

Acteurs concernés	
Contexte	Interdire l'accès du marché américain aux « éleveurs » norvégiens de saumon
Instigateurs probables	Pêcheurs de l'Alaska ou industrie américaine des biotechnologies
Cibles principales	Toute la filière de l'aquaculture
Date	Janvier 2005
Type de manipulation	Manipulation des conclusions d'un rapport scientifique
Effet final recherché	Degrader la légitimité de l'aquaculture auprès des opinions publiques
Motivation de l'agresseur	Conquête du marché américain par les Norvégiens prévue en 2005
Méthodes utilisées	Production d'un rapport scientifique dénonçant les risques de cancer liés à une trop grande consommation de saumon d'élevage
Caisse de résonance	Revues scientifiques internationales, grands médias
Résultat	Effet de surprise. Pas de contre-communication au niveau de la filière.

Exemple du cours avec Corrigé sur Facteurs Clés de Succès du Lobbying :

L'État lance des licences pour la 5G, mais les coûts sont très élevés. L'entreprise **TelcoPlus** souhaite obtenir des licences 5G moins coûteuses et veut ainsi convaincre le gouvernement de réduire le prix de ces licences afin de pouvoir investir davantage dans la couverture réseau.

Elle réalise une **veille stratégique** et prépare un **argumentaire clair**, expliquant qu'un prix réduit permettra d'investir davantage dans la couverture du réseau. TelcoPlus suit le **processus décisionnel** du ministère des Télécommunications et intervient au bon moment.

Grâce à un **réseau solide** (décideurs, experts, journalistes) et à sa **réputation crédible**, elle parvient à faire entendre ses arguments.

L'entreprise mobilise aussi ses **ressources financières** pour financer des études, des analyses et une petite campagne médiatique.

Enfin, elle agit dans un cadre **éthique et transparent**, ce qui renforce sa légitimité.

Question :

En vous appuyant sur l'exemple, identifiez et expliquez trois facteurs clés de réussite de l'activité du lobbying de TelcoPlus. Pour chacun, indiquez pourquoi il est important et comment l'entreprise l'a mis en œuvre.

Réponse :

1. **Facteurs stratégiques** : TelcoPlus connaît parfaitement le secteur 5G et le processus décisionnel du gouvernement. Elle a préparé un argumentaire clair montrant que des licences moins chères permettraient d'améliorer la couverture réseau. Cela est important car un message précis et bien ciblé augmente les chances d'influencer les décideurs.
2. **Facteurs relationnels** : L'entreprise dispose d'un réseau solide avec des députés, des experts et des journalistes, et bénéficie d'une réputation crédible. Ces relations facilitent l'accès aux décideurs et renforcent la confiance, ce qui est crucial pour que ses arguments soient pris au sérieux.
3. **Facteurs organisationnels et ressources** : TelcoPlus mobilise des ressources financières et humaines pour financer des études, analyses et une petite campagne médiatique. Ces moyens permettent de soutenir le lobbying de manière professionnelle et visible, augmentant ainsi son efficacité.

Conclusion :

La réussite du lobbying de TelcoPlus repose sur la combinaison de ces trois catégories de facteurs clés

- ✓ Stratégique : connaissance du secteur 5G et argumentaire clair pour convaincre les décideurs.
- ✓ Relationnel : réseau solide et réputation crédible auprès des députés et experts.
- ✓ Organisationnel : ressources financières et humaines pour études et communication professionnelle.

Eléments détaillés de réponses

Objectif: Meilleure compréhension des FCS du Lobbysme de TelcoPlus :

1. Facteurs stratégiques

✓ *Connaissance du sujet :*

TelcoPlus maîtrise les aspects techniques : fréquence 5G, investissements nécessaires, risques de saturation du réseau et besoins des utilisateurs.

✓ *Compréhension du processus décisionnel :*

Elle sait que la décision appartient au ministère des Télécommunications et à l'autorité nationale de régulation. Elle intervient **avant la définition des prix** pour avoir plus d'impact.

✓ *Message clair et argumenté :*

TelcoPlus formule un argument simple :

Si les licences sont moins chères, l'entreprise peut investir plus dans les antennes et offrir une meilleure couverture nationale.

✓ *Stratégie structurée :*

- Publication d'un rapport économique
- Rencontres avec les conseillers ministériels
- Étude comparative sur les prix 5G dans d'autres pays
- Participation aux consultations publiques

✓ *Veille stratégique :*

L'entreprise suit les annonces de l'Europe, les décisions des autres régulateurs et les tendances du marché pour ajuster son discours.

✓ *Influence de l'opinion publique :*

Elle lance une campagne médiatique :

“Une 5G accessible pour tous”. Cela crée une pression positive sur les décideurs.

2. Facteurs relationnels :

✓ *Qualité du réseau (network) :*

TelcoPlus entretient des liens avec :

- Des députés spécialisés dans l'économie numérique,
- Des journalistes high-techs,
- Des experts en cybersécurité.

✓ *Crédibilité et confiance :*

L'entreprise est connue pour son sérieux et ses investissements massifs dans l'innovation (les décideurs lui font confiance.)

✓ **Relations institutionnelles et médiatiques :**

Participation active aux conférences, forums sur la transformation digitale, interviews dans les médias.

✓ **Éthique et conformité :**

TelcoPlus déclare ses actions de lobbying et publie ses données financières de manière transparente.

3. Facteurs organisationnels et ressources :

✓ **Ressources financières :**

TelcoPlus finance des études économiques, des campagnes de communication et des consultants experts en réglementation.

✓ **Capacités internes :**

Ses équipes préparent des dossiers techniques sur la 5G, analysent l'impact économique et argumentent de manière professionnelle.

✓ **Moyens logistiques et opérationnels :**

Organisation de tables rondes, démonstrations technologiques, visites de centres de données pour les décideurs publics.

Conclusion :

⇒ *Cet exemple montre que **la réussite du lobbying** dépend de trois dimensions :*

- Stratégique (arguments, timing, analyses),
- Relationnelle (réseau, crédibilité),
- Organisationnelle (financement, moyens internes).

Il illustre comment une entreprise utilise le lobbying comme outil de management stratégique pour influencer un environnement réglementaire.

Sujets Examens 23-24-25

UNIVERSITÉ DE SOUSSE
INSTITUT SUPÉRIEUR DE GESTION DE SOUSSE

SESSION PRINCIPALE
Janvier 2023

NIVEAU	3LSMGT
ÉPREUVE	Management des risques et Intelligence économique
DURÉE	2h
NB. PAGE	2
ENSEIGNANT	Dr.Karima Mnasser

Exercice 1 : (6 points)

- 1) Citer les différents attributs d'un risque. (1)
- 2) La mesure du risque selon l'approche sociale fait appel à trois niveaux de Zones. Quelles sont ces trois zones ? (1.25)
- 3) Indiquer et expliquer les différentes caractéristiques d'un risque qu'un manager doit en tenir compte lors de son traçage d'un bon profil du risque. (2)
- 4) a) Quelle est l'utilité d'une cartographie des risques ? (0.25)
 b) Dresser un exemple d'une cartographie générique des risques. (*Donner 3 rubriques de familles de risques et pour chaque famille un exemple de risques*). (1.5)

Exercice 2 : (6 points)

- 1) Définir le concept de « l'intelligence économique (IE) » tout en montrant son rôle au service de la gestion des risques. (1)
- 2) Les finalités de l'intelligence économique sont largement reliées aux risques encourus par les entreprises. Expliquer cette interaction par trois exemples. (1.5)
- 3) Quelles sont les étapes du processus d'intelligence économique (IE) ? (2)
- 4) Actuellement, les entreprises se trouvent face à une réalité économique de plus en plus complexe et immatérielle. Expliquer cette idée tout en montrant l'impact de cette nouvelle réalité sur l'évolution de la culture managériale de l'entreprise et de sa compétence (capacité) en particulier. (1.5)

Exercice 3 : (8 points)

L'entreprise ABC possède une structure séparée d'intelligence économique (**IE**). Elle est intégrée au département Stratégie. Les actionnaires décident de vous nommer « Risk manager » responsable sur la prévention et la gestion des risques et appelé à collaborer étroitement avec la direction générale (**D.G**) et aussi avec les différents services de la société. Votre mission commence.....

T.A.F :

- 1) Entant que « Risk manager », vous avez choisi « **la gestion intégrée des risques** » comme outil pour une bonne prévention des crises. Présenter la méthodologie de cette gestion intégrée des risques en décrivant brièvement ses quatre étapes.
- 2) Afin de mesurer les risques, vous avez proposé aux membres de votre équipe d'utiliser le modèle *mini-max* de hiérarchisation des risques.
 - ✓ Présenter et Interpréter ce modèle tout en montrant son utilité pour une bonne analyse de gestion préventive des risques.

Dans le cadre de l'entreprise ABC, l'**IE** présente un mode de management stratégique de l'information en vertu desquels, les trois fonctions de l'**IE** à savoir renseignement, influence et protection, devraient être toutes assurées.

- 3) a) Quel est l'outil d'**IE** que l'entreprise ABC pourrait utiliser pour assurer sa première fonction de renseignement. Présenter cet outil à travers ses quatre étapes.
 - b) Dans le même cadre de sa fonction de renseignement, présenter deux principaux types de « Veille » que ABC pourra les mobiliser pour tirer un avantage concurrentiel.
- 4) a) En recherchant et en partageant ses informations, l'entreprise ABC accroît potentiellement sa vulnérabilité. Citer quelques risques informationnels potentiels liés à cet actif (patrimoine) immatériel.
 - b) Dans le cadre de sa fonction d'influence et de protection, présenter les stratégies qui pourraient être mises en œuvre par l'**IE** pour gérer ces risques informationnels et protéger le système d'information SI de l'entreprise. (*N'oubliez pas de faire référence dans votre réponse aux outils d'IE à utiliser dans ce cadre*).

BON COURAGE

UNIVERSITÉ DE SOUSSE
INSTITUT SUPÉRIEUR DE GESTION DE SOUSSE

SESSION PRINCIPALE

Janvier 2024

NIVEAU	3LSMGT
ÉPREUVE	Management des risques et Intelligence Économique
DURÉE	2h
NB. PAGE	3
ENSEIGNANT	Dr. Karima Mnasser

Exercice 1 : (5 points)

Répondez aux questions suivantes :

- 1) Définir le concept de « l'intelligence économique » IE tout en montrant son rôle au service de la gestion des risques. (1)
- 2) Citez les trois fonctions de l'IE et donnez un exemple d'outil d'IE approprié pour chaque fonction. (1.5)
- 3) Distinguer entre « benchmarking concurrentiel » et « benchmarking générique ». (1)
- 4) La protection du patrimoine informationnel requiert la définition et la mise en œuvre d'une politique optimale de sécurité du système d'information. Nommez les membres (personnels) impliqués dans la définition et le pilotage de cette politique de sécurité. (1.5)

Exercice 2 : (5 points)

Un lobbyiste-conseil fait des démarches auprès du ministère de la santé et des services sociaux pour le compte d'un client distributeur de produits pharmaceutiques afin de faire modifier la loi, ici *la loi visant à réduire le coût de certains médicaments couverts par le régime d'assurance médicaments en permettant le recours à une procédure d'appel d'offre.*

- 1)** Donner une définition claire du concept « lobbying » comme un outil de l'IE. **(1)**
- 2)** Présenter clairement les différents acteurs clés intervenant dans cette activité du lobbyisme décrite dans l'exemple. **(2)**
- 3)** Quel est le type de lobbying approprié à cet exemple ? Justifier. **(1)**
- 4)** Quels sont les facteurs que doit maîtriser ce « lobbyiste-conseil » afin de pouvoir réussir son activité de lobbyisme. **(1)**

Exercice 3 : (10 points)

« Alstom » est une multinationale française spécialisée dans le secteur des transports, principalement ferroviaires (trains, tramways et métros). Le 29 Janvier 2021, « Alstom » finalise le rachat et l'absorption de son concurrent canadien « Bombardier Transport ». Cette acquisition donne naissance à un géant industriel, numéro deux mondial du ferroviaire.

Marc Chatelard, senior vice-président du groupe déclare : *« Il existe une structure séparée d'intelligence économique (IE) Chez « Alstom ». Elle est intégrée au département Stratégie. Toute activité comporte sa part de risque. Dans une entreprise de biens d'équipements comme la nôtre, le risque est néanmoins plus grand sur les activités industrielles que sur le système d'information qu'il soit formel ou informel. Il faut cependant rester vigilant dans notre politique de gestion des risques.*

Chaque secteur (énergie et transport) a son propre système de veille. La dynamique de marché reste très positive avec des perspectives de prises de commandes et de croissance convaincantes dans toutes les régions, soutenues par un environnement politique favorable axé sur la décarbonation du transport ».

Les actionnaires décident de vous nommer « Risk manager » responsable sur la prévention (anticipation) et la gestion des risques dans « Alstom ». Vous êtes appelé à collaborer étroitement avec la direction générale (**D.G**) et aussi avec les différents services de la société. La démarche de la gestion des risques vous a toujours passionné. Vous acceptez donc cette proposition, ravie de ce nouveau challenge. Votre mission commence.....

T.A.F :

- 1) a)** Selon vous, est-ce qu'il y a une cartographie des risques standard à appliquer pour toutes les entreprises ? Justifier votre réponse. **(0.5)**

- b)** Dresser un exemple d'une cartographie des risques potentiels spécifique à l'activité « Alstom » (2).
- c)** Proposer une cartographie de risques adapté à un business plan. (Il suffit de donner trois exemples) (0.75)
- 2)** **a)** Entant que « risk manager », quelles sont les deux approches que vous recommandez pour mesurer les risques ? (2)
- b)** Selon vous, est-ce qu'il y a une approche qui est plus efficace que l'autre ? Pourquoi ? (0.5)
- 3)** Proposer trois types de « Veille » les plus adaptées à la société « Alstom » dans son processus d'analyse et de gestion des risques tout en expliquant brièvement leurs objectifs. (1.5).
- 4)** Dans le cas où « Alstom » échouera dans sa politique de gestion de risques et se trouvera dans une situation de crise ; la société devra passer automatiquement à l'outil « communication de crise ».
- a)** Quelle est l'utilité de « la communication de crise » et pourquoi elle revêt une importance cruciale dans cette démarche d'IE de la société ? (0.5)
- b)** Quelles sont les stratégies qui pourraient être adoptées dans cette « communication de crise ». (0.75)
- c)** Quelle stratégie vous recommandez le plus et pourquoi ? (0.5)
- 5)** Si « Alstom » est confrontée à des attaques de désinformation, à des problèmes de déstabilisation ou à des rumeurs qui nuisent à son image de marque. Selon vous, comment pourra-t-elle procéder pour y faire face et résister à ces attaques ? (1)

BON COURAGE

UNIVERSITÉ DE SOUSSE
INSTITUT SUPÉRIEUR DE GESTION DE SOUSSE

SESSION PRINCIPALE

Janvier 2025

NIVEAU	3LSMGT
ÉPREUVE	Management des risques et Intelligence économique
DURÉE	2h
NB. PAGE	4
ENSEIGNANT	Dr. Karima Mnasser

Exercice 1 : (3.5 points)

- 1) Indiquer et expliquer les différentes caractéristiques d'un risque qu'un manager doit en tenir compte lors de son traçage d'un bon profil du risque. **(1.5)**
- 2) a) Quelles sont les stratégies qui pourraient être adoptées dans « **la communication de crise** » ? **(1.5)**

b) Selon vous, quelle est la meilleure stratégie de communication de crise ? Justifier votre réponse. **(0.5)**

Exercice 2 : (4.5 points)

Au début de l'année 2005, le cours du saumon d'élevage s'effondre brutalement à la suite d'une étude publiée dans la revue scientifique *Sciences*. Les conclusions de recherches tendent à prouver que la consommation régulière de saumon d'élevage développe les probabilités de cancer chez les personnes âgées, les femme enceintes et les enfants. L'objectif de cette étude « non crédible » était d'empêcher la conquête du marché américain par les industriels Norvégiens. En effet, la fondation *Pew Charitable Trust* dont trois membres du conseil d'administration directement parties prenantes dans le marché des pêcheurs américains, est l'acteur principal dans ce cas puisqu'elle a voté au printemps 2003 le financement de cette étude réalisée par des chercheurs d'une université américaine. En plus ce travail a fait l'objet d'un relais médiatique sans commune mesure grâce aux actions d'une grande agence américaine de relations publiques. L'opération d'intoxication commanditée par les pêcheurs d'Alaska (pêcheurs du marché américain) cherchait donc à interdire aux Norvégiens la pénétration de leur marché national.

- 1) Donner une définition claire du concept « lobbying » comme un outil de l'IE. (1)
- 2) Présenter clairement les différents acteurs clés intervenant dans cette activité du lobbysme décrite dans l'exemple. (2)
- 3) Quel est le type de lobbying approprié à cet exemple ? Justifier. (0.5)
- 4) Dans l'exemple, quels sont les deux facteurs clés qui ont contribué à la réussite de cette activité de lobbysme ? (1)

Exercice 3 : (12 points)

Air France est une compagnie aérienne dont la gestion du risque repose principalement sur l'anticipation des crises et, ensuite sur leur gestion.

Chez Air France et, plus largement dans les compagnies aériennes, les risques sont suivis et analysés par un service central à la direction de l'audit interne qui les catégorise selon deux niveaux : les risques opérationnels et les risques stratégiques. Cette cartographie des risques est élaborée avec chaque direction et mise à jour trimestriellement pour les risques opérationnels, et annuellement pour les risques stratégiques.

Pour autant et en plus de ce dispositif global, il existe au quotidien une pratique systématique de l'intelligence économique (IE) qui vise à anticiper les risques concurrentiels.

Cette cellule d'IE procède à l'analyse des risques concurrentiels à partir d'une batterie d'indicateurs clés qui sont systématiquement suivis avec des fréquences quotidiennes. Elle est composée de 10 personnes spécialisées dans l'étude et l'analyse des indicateurs de tendance dont l'acteur principal est « *le risque Manager* ». Ainsi, l'évaluation des risques se fait en fonction de la fréquence d'occurrence et de la gravité des conséquences.

De son côté, la direction de sûreté assure l'anticipation et la gestion des risques terroristes ou géopolitiques.

Le groupe Air France structure finement et efficacement sa pratique de l'IE dans des processus transparents basés sur l'analyse informationnelle par des experts qualifiés dans le domaine concerné (économique, financier, concurrence, commercial, etc.). Chaque indicateur, par pays, par compagnie, collecté selon différentes sources, est étudié ensuite lors des réunions

systématiques entre services. A la suite, ces évènements informationnels sont classés en fonction de la priorité stratégique qu'ils représentent.

L'efficacité du « modèle Air France » repose sur la fiabilité des données brutes et sur la valeur ajoutée du traitement et de l'analyse de ces données. Bien entendu la collecte et l'analyse d'un grand nombre d'informations sont facilitées par l'utilisation d'un système d'information (**SI**) adapté et surtout d'une politique optimale de sécurité du SI qui est définie et pilotée par une structure spécifique du personnel.

Le risque informationnel existe donc peu. En revanche, le risque commercial demeure important pour les compagnies aériennes qui trouvent une source évidente d'avantages concurrentiels dans les améliorations des servies et de la qualité.

Source : Entretien avec Gilles Bordes-Pages (Directeur stratégie et planification, Groupe Air France)

T.A.F :

- 1) a) L'intelligence économique (**IE**) est un mode de management stratégique de l'asymétrie informationnelle. Expliquer cette idée. **(0.75)**
 - b) En évoquant les trois fonctions de l'IE, expliquer clairement comment le groupe « Air France » a appliqué et réussi ce mode de gestion de l'asymétrie informationnelle. **(2.5)**
- 2) a) Quelle est l'approche de mesure de risque utilisée par le groupe « Air France » ? Justifier votre réponse à partir du cas. **(0.5)**
 - b) Présenter et interpréter cette approche tout en montrant son objectif et utilité. **(1.5)**
 - c) Selon vous, est-ce qu'il y a une approche de mesure de risque qui est plus efficace que celle utilisée par la cellule IE de Air France ? Justifier votre réponse. **(0.5)**
- 3) a) Afin d'assurer sa première fonction de l'IE, la cellule responsable au sein du groupe « Air France » a utilisé l'outil « veille ». Quelles sont les deux types de veille implicitement indiquées dans le cas ? Justifier votre réponse. **(1.5)**
 - b) Citer un autre outil approprié que la cellule IE pourrait l'utiliser pour assurer sa première fonction informationnelle de l'IE. **(0.5).**

- 4) a)** Quelle est l'utilité d'une cartographie des risques ? **(0.5.)**
- b)** En se basant sur le cas, dresser un exemple d'une cartographie des risques potentiels adaptée au groupe « Air France ». **(1.5)**
- 5)** Selon le témoignage du « *Gilles Bordes* », le système information (**SI**) du groupe « Air France » est défini et piloté par une structure spécifique du personnel. Préciser les acteurs clés intervenant dans cette composition. **(1)**
- 6)** Selon le cas, le risque informationnel existe peu. Néanmoins, en recherchant et en partageant ses informations, « Air France » accroît potentiellement sa vulnérabilité.
- ✓ Présenter deux types de risques informationnels potentiels différents et proposer pour chaque risque informationnel une stratégie convenable pour le gérer et protéger le SI. **(1.25)**

BON COURAGE!